CYBERSECURITY 2022

In association with
Simmons & Simmons

LEXOLOGY
Getting the Deal Through

simmons+simmons

simmons+simmons

Our team provides a business-focused and pragmatic approach.

Our international data, privacy and cybersecurity practice spans the globe advising within the Asset Management & Investment Funds, Financial Institutions, TMT and Healthcare & Life Sciences sectors.

Our lawyers advise on the full suite of data and cybersecurity issues – from implementing preventative measures and regulatory requirements through to data breach response and full-scale litigation.

simmons-simmons.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2015
Seventh edition
ISBN 978-1-83862-941-0

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CYBERSECURITY 2022

Contributing editors
Edward R McNicholas and Fran Faircloth
Ropes & Gray LLP

Lexology Getting The Deal Through is delighted to publish the seventh edition of *Cybersecurity*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Edward R McNicholas and Fran Faircloth of Ropes & Gray LLP, for their continued assistance with this volume.

LEXOLOGY
Getting the Deal Through

London
February 2022

Contents

Global overview

Edward R McNicholas and Fran Faircloth

Ropes & Gray LLP

The law of cybersecurity continues to evolve rapidly across the globe in an effort to keep pace with the swiftly developing threat environment, the significant harms suffered as a result of cybersecurity incidents, and the efforts of regulators and law enforcement to protect consumers, investors and companies. At the most basic level, the law of cybersecurity is developing along a path defined by the exponential growth in the internet – and the internet of things – technologies that have created virtual social gatherings, information pools and even whole worlds, while augmenting and enhancing our real-world lives. These technologies are quickly becoming an indispensable mainstay of everyday life, and technology-enabled critical infrastructure is always running behind the scenes making this life function. Coupled with widespread movement to cloud computing, technological developments have enabled numerous revolutionary innovations and benefits to society. From a risk perspective, however, our growing dependence on technology and its constant development has also significantly increased our exposure to cyberthreats, which has only expanded as hackers exploit vulnerable targets. It would be virtually impossible to stop or even slow the speed of cyber developments, and we expect the law of cybersecurity to continue to develop in a responsive effort to manage these new risks.

Many countries have pursued a whole-of-government response to cybersecurity risk by pushing forward with aggressive criminal investigations, both domestically and internationally where possible. This has been combined with general and sector-specific regulation; trade and export sanctions and restrictions; and both defensive and offensive military and intelligence operations. On any given day, criminals, hacktivists, disloyal employees, spies and militaries launch a series of attacks at their victims over the same networks that carry infrastructure, social interactions and culture, simultaneously bringing the globe closer together than ever before while leaving companies both bereft of enforceable global legal norms and subject to a complex array of cybersecurity regulations.

Thanks to the rapid development of technological growth and the law's attempt to stay ahead of new risks as they arise, the private sector is now subject to a complex and often conflicting set of laws and regulations that both impose cybersecurity obligations and prohibit certain cybersecurity practices. In the United States, the approach to cybersecurity regulation and governance is largely sectoral, with different sets of requirements for healthcare, financial services, communications, defence, energy and other sectors, which can result in siloed approaches to managing cyber risk that vary dramatically by sector. These variations are only compounded for global businesses balancing multiple conflicting national approaches to cybersecurity law. Companies must balance the sectoral US cybersecurity standards, many of which spring from consumer protection laws, with the substantive security requirements and strict data breach reporting requirements in the European Union's human rights-based General Data Protection Regulation as well as with new laws like China's Data Security Law and Personal Information Protection Law, which represents a robust assertion of national sovereignty over the data within China and against foreign governments and global companies.

These various laws can leave companies unsure of how to interact with government agencies following a cyber incident. Companies are rightly worried that even while certain government entities view companies as the victims of criminal attacks or even hostile military actions, other agencies can simultaneously view these same companies as potential perpetrators of wrongdoing for neglecting their obligations to protect their networks and the personal and other data they hold.

In response, the private sector has taken concerted steps to organise its own cyber risk standards, such as the private sector Payment Card Industry Data Security Standard, and enhance contractual protections in vendor relationships, which now impose increasingly complex affirmative cybersecurity requirements. These vendor-client relationships naturally span both sector and geographic boundaries, requiring the applicable laws and regulations to address the complexity of cross-sector and international interdependence that characterises modern economic realities.

In the United States, companies confront an array of federal and state regulators and government agencies addressing cybersecurity issues. The Federal Trade Commission (FTC), state attorneys general, and other agencies empowered by specific statutory mandates have set the primary data security requirements for entities that are not in critical infrastructure sectors – healthcare, energy, defence, telecommunications or other regulated industries – which are subject to more specific regulatory requirements. The FTC's assertion of authority over information security, however, is limited by its statutory powers under section 5 of the FTC Act to prohibit 'unfair or deceptive acts or practices' that injure consumers – and its expansion of authority has recently received repeated judicial challenges.

The FTC's consumer protection mission, however, does little to address the cyber risks that are companies' top concerns: attacks that target their operations, bank accounts, supply chain, intellectual property and trade secrets. These threats pose an existential risk to companies and are expected to continue to be central in 2022, following attacks in recent years that had significant impact across the public and private sectors, such as the exploitation of Microsoft Exchange server vulnerabilities (attributed to China) and the potential for cyber conflicts erupting from international trouble spots, such as North Korea.

The Securities and Exchange Commission (SEC) has attempted to create new rules for disclosure of such cybersecurity risks, and perhaps even mere vulnerabilities, for all public companies. Through its regulation of these markets, the SEC has pushed companies to develop enhanced governance of cybersecurity risks to protect information assets, even while choosing not to issue specific regulatory guidance.

Despite these efforts of the FTC and SEC, the field of cybersecurity law continues to confront the challenge of developing a comprehensive, publicly transparent knowledge base regarding malicious cyberspace

actors and their capabilities. At present, the extent of attacks, the methods of the attackers and the true cost to companies remain veiled, leading to a dearth of information in the markets and a failure of the security and insurance markets to value cybersecurity risk efficiently. Only with further information will markets gain the ability to assess and price these risks.

Certain jurisdictions and regulators are increasingly requiring nearly instantaneous sharing of information from companies that have been the victims of cyber attacks in an attempt to encourage better information distribution and remedy the lack of public transparency over the scope and impact of such cyber incidents, including compromises impacting personal information. In the EU, data protection authorities have levied significant fines against companies, including Booking.com and Twitter, for failure to fulfil data breach notification obligations. Meanwhile, in the United States, the SEC has taken aggressive actions to investigate, enforce and settle with companies on cybersecurity-related matters, including failures to adequately disclose material cyber risks and adverse cyber incidents.

The Cybersecurity and Infrastructure Security Agency (CISA) has recently joined the host of similar bodies across the globe that are attempting to gather comprehensive databases of attacks, defences and techniques. Through CISA and other similar agencies, US federal legislators and executive agencies are also attempting to encourage the sharing of information about cybersecurity incidents, particularly since the passage of the Cybersecurity Act of 2015, which authorises monitoring, use of so-called 'defensive measures' and sharing of 'cyber threat indicators' (with private and governmental entities) with limited liability protections for such monitoring and information sharing. In 2021, building on the work of the seminal Cyberspace Solarium Commission, President Biden issued an Executive Order and convened leaders of key commercial enterprises to work in concert with the government to advance shared cybersecurity norms and expand information sharing from the private sector to the federal government. While the full impact of these activities undertaken to mitigate cyber risks is yet to be seen, they are important steps toward enabling the private sector and government to conduct necessary activities more easily and with reduced legal risk.

Finally, we should note that while 'privacy laws' and 'cybersecurity laws' are sometimes discussed separately, few would doubt that the law's approach to the protection of privacy and cybersecurity are interdependent. Many data protection and information security statutes can be classified as both 'privacy laws' and 'cybersecurity laws' because these concerns go hand in hand. Personal privacy should always be a chief consideration when developing cybersecurity measures; an effective privacy programme enhances security, and security against unauthorised intrusions is essential for protecting the privacy of data. As laws expand to protect cyberspace, they should not advance at the expense of personal freedom or rights to privacy, and they should take into consideration the potentially differential impact that evolving cybersecurity technologies might have on the civil liberties and human rights of the most vulnerable members of our society.

In this vein, the conflict between cybersecurity and surveillance issues is likely to continue to be a sticking point, especially between the United States and its European counterparts, despite the prevalence of state surveillance in both lands. The growth of cloud data centres and the need to protect them is similarly likely to continue to be a point of tension. Conflicting approaches to the law of data protection in the United States, Europe and Asia may also inhibit the development of the sort of globally interoperable cybersecurity solutions that are necessary to protect global information systems. Even as the Internet may appear to bridge geographies seamlessly and instantaneously, making globalisation a part of our everyday lives, some countries are not committed to the unambiguous goal of a globally interoperable internet.

While the broader outlook for cybersecurity is uncertain, it is clear that advances in factual knowledge, technological developments and the threat environment will continue to propel this field to the front of the global consciousness. Data is a valuable asset, and failure to protect a company's data or systems can create substantial risk. Companies are expected to maintain a secure environment and appropriate information governance. We anticipate that cybersecurity will remain a top priority for companies in the years to come as the law continues to fashion new legal requirements that compel the development of further governance of cybersecurity risks.

Austria

Árpád Geréd

MGLP Rechtsanwälte | Attorneys-at-Law

LEGAL FRAMEWORK

Legislation

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Even though cybersecurity and, as a related topic, cybercrime have a long history in Austrian law, efforts to establish dedicated and detailed rules on cybersecurity that are binding, not only for governmental agencies and (partially) state-owned companies but also the private sector, are fairly recent.

The first legal provision on cybersecurity in its widest sense was article 10 of the (then new) Austrian Data Protection Act (DSG 1978), which entered into force in 1980. In this provision, data processors were obliged to set up work rules regarding data security, such as measures for access security or software testing. While the provision did not contain any details on the required rules and, further, took economic and technical feasibility into account, it required these internal rules to be approved by the Austrian Data Protection Commission (now the Data Protection Authority, or DSB), thus granting at least a minimum level of homogeneity.

In hindsight, article 10, despite its lack of detail, provided a solid basis for a unified understanding of required data security measures. But in 1987 this provision was amended with far-reaching consequences: first, the new article 10 no longer required data security measures to be compiled in a set of work rules; and second, the requirement for approval by the now DSB was removed. However, the modified provision still took into account the economic and technical feasibility of the measures as well as their adequacy related to the processed data.

In Austria, a country dominated by small and medium-sized enterprises, the flexibility of article 10 DSG 1978, coupled with a legal and factual lack of control of the security measures taken, has led to wide variation of levels of cybersecurity and has, in extreme cases, led to very small enterprises not taking any relevant security measures at all, arguing that they were neither economically feasible nor required by the type of processed data. Unfortunately, this relatively toothless rule has found its way into article 14 of the Austrian Data Protection Act (DSG 2000) in mostly unmodified form. While article 14 DSG 2000 applies to data controllers and data processors alike and corresponds in essence to article 17 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the EU Data Protection Directive), it is, nevertheless, a step backward from its predecessor, article 10 DSG 1978. As of 25 May 2018, however, the DSG 2000 was replaced by Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation), which provides for slightly more detailed rules on data security in its article 32.

The first cybercrime-related rules were established in 1987 with articles 126a and 148a of the Austrian Criminal Code (StGB). These provisions penalised the damaging of data and the abuse of automated data processing (including the modification of processed data as well as the processing software), respectively. Depending on the damage caused, these actions were punishable by imprisonment for up to five or 10 years respectively.

In 2002, Austria adopted the Council of Europe's Convention on Cybercrime, modifying the StGB to also penalise acts such as illegitimate access to a computer system (article 118a) or the abusive interception of data (article 119a). In the meantime, more and more cybercrime-related rules were adopted by the Austrian Criminal Code: for example, disruption of the functioning of a computer system (article 126b), abusive use of computer programs or access data (article 126c) and spying on data from cashless payment instruments (article 241h). Also, in 2021, the existing article 107c of the Austrian Criminal Code was tightened in the areas of cyber-crime and protection of likeness, so that (for example) cyber bullying is now already punishable from the first post.

With these provisions of the DSG 2000 and the StGB, a first basic set of cybersecurity rules was in place, obliging enterprises to take protective measures while at the same time protecting their efforts and systems by means of the Criminal Code.

While it was not until 2014 that new legal rules on cybersecurity were announced, Austrian private entities, as well as the federal government, were far from inactive in the meantime.

The first industry-wide initiative to centrally collect and manage cybersecurity incidents from the private as well as the public sector was the Computer Incident Response Coordination Austria (CIRCA), established by the Internet Service Providers Association in cooperation with the Austrian Federal Chancellery. In 2008, CIRCA was incorporated into the newly created Austrian Computer Emergency Response Team (CERT) as well as the Austrian Government Computer Emergency Response Team (GovCERT), with the former being primarily operated by NIC.at, the Austrian domain registry, and the latter by the Federal Chancellery. Though factually important and well-recognised, the main purpose of both CERT institutions lies in the collection of information on incidents and the coordination of the incident response. As such, both institutions may only advise on prevention measures but have no authority to demand certain actions.

Apart from these two most important CERTs, there are others established at authorities or formerly state-owned enterprises, such as the City of Vienna, A1 (the former state-owned telephone operator) or the Austrian Federal Computing Centre (BRZ), which is the former federal data centre and now e-government partner of the federal administration in Austria. These are all organised in the Austrian CERT-network, which was established in 2011.

The most recent addition to the Austrian organisations active in the field of cybercrime is the Cyber Crime Competence Centre (C4), which was established in 2012. In contrast to the CERTs, the C4's aim is to actively combat cybercrime. Therefore, its personnel consists of members of the Austrian Federal Police as well as the Austrian Federal Ministry for Internal Affairs.

In May 2014, the Austrian government announced the introduction of a dedicated Austrian Cybersecurity Act. This announcement came in the wake of similar efforts in Europe, most notably the presentation of the draft version of a Network and Information Security Directive by the European Commission in February 2012, in the meantime published as Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, and of a German law on cybersecurity (the IT Security Act) in March 2013. In June 2016, a White Paper was published that contains recommendations for the planned Austrian Cybersecurity Act. Following these recommendations, the new Act will be a transposition of the Network and Information Security Directive into Austrian law, taking into account Austria's experiences in combatting cybercrime so far, as well as the government's Austrian Strategy for Cybersecurity, which is based not only on general experience but also on the results of larger-scale cybersecurity exercises held for the purpose of evaluating and improving cyber defence readiness.

While the promised draft of the Austrian Cybersecurity Act was still outstanding, another law has in fact established itself as the first legal act to require Austrian companies to ascertain an appropriate level of cybersecurity: Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, better known as the General Data Protection Regulation (GDPR). This Regulation, which entered into force on 25 May 2018, first and foremost aims at protecting personal data (ie, data by which a natural person can be identified). However, in contrast to the existing rules on data protection back then, the GDPR is no longer satisfied with requiring companies to have appropriate contractual provisions in place but explicitly also requires appropriate technical and organisational measures – thus, in essence, cybersecurity measures.

In the meantime, the Austrian government has revived the Cybersecurity Act as the Network and Information Systems Security Act (NISG), which entered into force on 29 December 2018. Furthermore, on 18 July 2019 the Network and Information Systems Security Ordinance (NISV), which determines the businesses to be considered providers of critical infrastructure, defines security precautions and regulates the sectors and security incidents according to the NISG in more detail, entered into force.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The NISG established measures to ensure a high level of security of network and information systems of providers of critical infrastructure in the following sectors: energy; transportation; banking; financial market infrastructures; healthcare; drinking water supply; and digital infrastructure, plus digital services and public administration institutions. The details regarding which businesses active in the mentioned industry fields actually fall within the scope of the NISG have been determined in the NISV (eg, by the megawatts of energy generated in power plants).

The Austrian communication industry, including internet service providers, already has a head start in the field of cybersecurity. This is not only because IT forms the core (or at least a substantial part) of its business, but also owing to the involvement of the Austrian communication industry in the CIRCA and now CERT. The same applies to a few public authorities, most notably the Austrian Federal Chancellery and the BRZ. These entities are also those that have made the most progress towards promoting cybersecurity.

Other industries, however, still need to improve to varying degrees. For instance, the financial sector in Austria features some leading as well as, unfortunately, some less stellar examples. The Austrian energy sector has in the past mostly focused on downplaying the potential risks of networked power grids and smart metering in the media. The transportation sector has also appeared unevenly prepared to face cybersecurity challenges, with, for example, the Austrian Federal Railway (ÖBB) being one of the positive examples.

In 2014, the initiative Trust in Cloud (www.trustincloud.org) was launched by EuroCloud Austria, the Austrian association of EuroCloud Europe, an independent non-profit organisation. Participants include national and international enterprises from the IT sector, but also public and private entities from other sectors, such as the Austrian Federal Chancellery, the ÖBB, an international supermarket chain and an international producer of skiing equipment. While the aim of the initiative is to promote cloud computing in general, cybersecurity is one of the major focal points.

In any case, since the entry into force of the GDPR on 25 May 2018, binding rules on cybersecurity apply to any and all companies for the first time.

In general, the discussion around cybersecurity in recent years, fueled again by the accelerated digitalisation during the covid-19 pandemic and lockdowns, has benefited Austrian businesses, turning a problem most would refuse to talk about for fear of gaining a reputation for not being secure enough into something that could affect anyone, no matter how well prepared. A significant degree of improvement of awareness, as well as of readiness, could be noted in the course of the many expert discussions during the conception of the Cybersecurity Act, as well as during the cybersecurity exercises held for the same purpose. The Austrian government today claims that Austria is a model example of cyberthreat readiness. While this evaluation may need to be taken with a grain of salt, it is nevertheless true that Austria is among the better-prepared member states of the European Union.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The Austrian Standards Institute, which is the Austrian member of the European Committee for Standardization and the International Organization for Standardization, has adopted all relevant international standards related to cybersecurity, most notably, ISO/IEC 27001:2013 (currently ÖVE/ÖNORM EN ISO/IEC 27001: 2017 07 01 in Austria). The adoption of the (quite) recently published (16 February 2021) cybersecurity framework development guidelines ISO/IEC TS 27110:2021 is still pending.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

While Austrian law knows the concept of responsible persons (ie, employees responsible for certain areas of business within their company) this concept does not extend to cybersecurity or (unlike, for example, Germany) even data protection. Thus, managerial employees or directors in Austria are liable only according to the general legal rules, which essentially means that they need to act with due diligence

and with the care of a prudent businessperson, as set forth by Austrian law and further detailed by rulings of Austrian courts.

The GDPR requires any company or organisation to periodically verify the effectiveness of the technical and organisational measures it has taken and document the results. This obligation exists regardless of whether the company or organisation in question is required to have a dedicated data protection officer. However, as was the case before the GDPR entered into validity, the consequences of default are generally borne by the company rather than any internally responsible employee or the director.

5 How does your jurisdiction define cybersecurity and cybercrime?

The NISG defines cybersecurity (actually network and information system security) as the ability to prevent, detect, defend against and remediate security incidents. Apart from that, Austrian law knows no definition of cybersecurity or cybercrime. While article 32 GDPR does stipulate data security measures, it does not define data security, much less cybersecurity. Also, the StGB penalises and defines certain acts of cybercrime, though it lacks a general definition of cybercrime as a whole.

In any case, cybersecurity in Austria is distinct from data privacy. Even though neither term is really defined in Austrian law, from the provisions of the laws containing relevant provisions, above all the GDPR and the StGB, it becomes apparent that data privacy in Austria primarily deals with the rights and obligations related to the usage of data obtained legitimately, while the aim of data security as an aspect of cybersecurity is to prevent illegitimate access to and use or abuse of data.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Article 32 GDPR requires any controller or processor of personal data to implement measures to ensure data security. However, such measures need to take into account the type, extent and purpose of the processed data, the state of the art and the economic feasibility.

Therefore, even though this provision does stipulate minimum protective measures, it is not clear what the minimum requirements in each case may be. Further, this provision only applies to personal data rather than any type of data.

As a result, in the field of cybersecurity, industry standards and the recommendations of the CERT and GovCERT are more important in Austria than legal rules. This is especially true for relatively new technology such as cloud computing or the issues associated with various forms of 'bring your own device'.

Of course, the GDPR explicitly mentions that the European Commission, national data protection authorities and industry-specific organisations should define recommendations and standards for appropriate technological and organisational measures. These will, in the end, set forth the minimum requirements for cybersecurity that any company will need to meet. Currently, however, except for individual rulings, the only binding rules and guidelines issued by the Austrian Data Protection Authority are two regulations on privacy impact assessments (PIA), one listing processing operations that do not require a PIA to be performed (DSFA-AV, published on 25 May 2018) and one listing processing operations that in any case require a PIA to be performed (DSFA-V, published on 9 November 2018).

However, providers of critical infrastructure and federal institutions do have to take measures to ensure a high level of security of network and information systems according to the NISG. For this purpose, according to articles 17, 21 and 22 NISG, appropriate measures need to take into account the state of the art and be appropriate to any risk that can be determined with reasonable effort. Therefore, providers of critical infrastructure must take into account the following: safety of systems and facilities; management of security incidents; business continuity management; monitoring; verification and testing; and compliance with international rules. To enable the verification of the measures taken, providers of critical infrastructure must submit a list of the security measures they have carried out, including evidence of certification or inspections – and, if applicable, security deficiencies discovered – to the Federal Minister of Internal Affairs at least every three years. The Federal Minister is also authorised to issue recommendations regarding measures providers will have to take.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Articles 40(e) and 40(f) of the Austrian Intellectual Property Act stipulate rules on the decompiling of software and the use of databases, respectively. While these rules do not address cyberthreats specifically, they are the only ones addressing this subject explicitly within the context of intellectual property.

Where cyberthreats to intellectual property involve acts of cybercrime, the rules of the StGB apply.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

In Austria, cyberthreats to critical infrastructure are specifically addressed by the NISG and NISV, which are in effect transpositions of the EU NIS Directive into Austrian law. With the entry into force of the NISG on 29 December 2018 and the NISV on 18 July 2019, the new EU standards have therefore been belatedly introduced to Austria.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation on providers of digital services to report a security incident only applies if they have access to the information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability, or failure, of the service operated with significant impact. To assess whether the impact is significant or not, the anticipated number of users affected, duration and geographical spread, as well as the expected impact on economic and social activities, must be taken into account.

The GDPR also sets forth data breach notification requirements. However, according to the GDPR, the national data protection authorities only need to be informed if the breach may result in a risk to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical and organisational measures (eg, pseudonymisation, encryption).

In addition, article 165 of the Austrian Telecommunications Act 2021 stipulates that master data, traffic data, location data and also content data may only be collected or processed for the purpose of providing a communications service, whereby article 160 para. 3 lit 8 defines content data as the contents of transmitted messages. However, there are exceptions, in particular with regard to criminal justice.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal acts of cybercrime, relevant to businesses, which are penalised by the StGB depending on the amount of damage caused, are:

- 'cyber bullying' in the broadest sense (tightened article 107c);
- illegitimate access to a computer system (article 118a);
- breach of telecommunication secrecy (article 119);
- abusive interception of data (article 119a);
- abuse of audio recording or listening devices (article 120, para 2a);
- damaging of data (article 126a);
- disruption of the functionality of a computer system (article 126b);
- abuse of software or access data (article 126c);
- fraudulent abuse of data processing (article 148a);
- forgery of data (article 225a); and
- spying out data of cashless payment instruments (article 241h).

The fines are determined by the income of the culprit. Therefore, neither a minimum nor a maximum amount is stipulated by Austrian law. In principle, the Austrian Criminal Code also provides terms of imprisonment for cybercrimes.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

For the time being, the Austrian government, on the one hand, has not specifically addressed any of the challenges associated with cloud computing. On the other hand, private and non-profit organisations, such as EuroCloud Austria and the Austrian Chamber of Commerce, have made significant efforts to educate providers and especially (private and business) users of cloud computing solutions by means of events or publications, such as White Papers or even a recommendation catalogue relating to cloud contracts (some of these publications are available in English and can be obtained from the website of EuroCloud Austria: www.eurocloud.at).

Currently, the most important Austrian initiative regarding cloud computing is Trust in Cloud (www.trustincloud.org), which has formulated recommendations to the Austrian government, among others, in the field of cybersecurity. As the Austrian Federal Chancellery takes part in this initiative, it is realistic that those recommendations will be taken into account in the future.

In the NISG, cloud computing is defined as a type of 'digital service'; therefore the regulations of the NISG for providers of digital services also apply to cloud computing offerings.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The NISG regulates the obligations of providers of critical infrastructure and digital services as well as public administration institutions. It defines them as institutions with a branch office in Austria that provide an essential service, respectively legal entities or registered partnerships with a main office in Austria that provide a digital service in Austria and are not defined as 'micro' or 'small enterprises'. However, providers of digital services without a main office in the European Union that have appointed a representative are treated in the same way. Therefore, foreign companies without a branch office in Austria, and which have not appointed a representative, are not subject to the NISG.

Concerning the regulations of the GDPR, they are, according to article 3, para 1 GDPR, applicable to the processing of personal data, insofar as it is related to the activities of an establishment of a person responsible for it or a processor established in the European Union, whether or not the processing takes place in the Union.

With regard to the processing of personal data relating to data subjects in the European Union by a controller or a processor not established in the European Union, article 3, para 2 GDPR applies. The GDPR is therefore applicable if the processing is carried out to:

- offer goods or services to persons in the European Union, irrespective of any obligation to pay; or
- monitor the behaviour of persons within the European Union.

The GDPR also applies to responsible persons and processors not established in the European Union but in a place that is subject to the law of a member state by virtue of international law, such as diplomatic or consular representations of a member state. Thus the GDPR applies to all organisations participating in the EU market, which also includes foreign companies.

In any case, the rules of the European Union regarding the free movement of goods and services will need to be observed. In principle, this would mean that businesses already established in the European Union, be it with a seat or a representative, should fall under the jurisdiction of the member state in which they are established.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As there are currently no substantial laws on cybersecurity in Austria nor binding guidelines or best practices established on the grounds of the data security requirements set forth in the General Data Protection Regulation (GDPR), enterprises need to rely on industry standards and recommendations by various organisations and authorities.

The first contact in the field of cybersecurity in Austria is the Austrian Computer Emergency Response Team (CERT) for private entities and the Austrian Government Computer Emergency Response Team (GovCERT) for the public sector. Both institutions not only coordinate responses to cyberthreats but also advise on prevention measures. Thus, they constitute the most important contributors to a harmonised understanding of required and recommended cybersecurity measures. To facilitate intra-sectoral exchange of information, sector-specific CERTs are planned with the Austrian Energy CERT for the energy sector already being established. Additionally, sector-specific cybersecurity exchanges for providers of various critical infrastructures have been established in the form of the Austrian Trust Circles.

Further, interested parties can find a multitude of freely available publications on this topic; for example, from the Federal Ministry for Internal Affairs, the Chamber of Commerce or associations specialised in IT topics.

In addition, a coordination committee was established with the introduction of the Network and Information Systems Security Act (NISG) which advises the Federal Minister of Internal Affairs and the Federal Government on the decision whether a 'cyber crisis' is occurring or not as well as the operative measures required to cope with such a crisis and the coordination of public relations.

14 How does the government incentivise organisations to improve their cybersecurity?

While the Austrian government is very active in promoting cybersecurity directly as well as indirectly (eg, by means of GovCERT), there are currently no incentives in this context.

The NISG also follows the 'classical' approach and penalises inadequate cybersecurity measures, but otherwise does not provide any incentives for compliance.

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In Austria, ÖNORM ISO/IEC 27001: 2017 07 01 (which can be obtained from the ASI against payment) as well as the recommendations of the CERT (available from their homepage: www.cert.at) can be regarded as the main industry standards and codes of practice in the field of cybersecurity.

Comprehensive guidelines summarising the relevant rules and recommendations, as well as a checklist created specifically for very small enterprises, have been created by the Austrian Chamber of Commerce and can be obtained from www.it-safe.at.

16 | Are there generally recommended best practices and procedures for responding to breaches?

Best practices and procedures can be derived from industry standards or recommendations of the CERT. They may vary depending on the type, severity and potential danger of a breach. Thus, there are no general rules apart from containing the breach and saving any information for later analysis.

After the incident, it is considered best practice to have the existing data analysed by a trustworthy and independent third party to determine the methods by, and reasons for, which the system could be breached and to take measures to prevent such occurrences in the future.

While the various decisions and recommendations of the data protection authorities, both in Austria and abroad, have provided some guidance in regard to cybersecurity, it is still either rather general or very case-specific. In the latter cases, best practices can be seen slowly developing based on the decisions and recommendations.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Voluntary information on cyberthreats should be addressed to the CERT (or the GovCERT, in the case of a public entity) by means of an email containing:

- details of where the incident has occurred (eg, IP address, website);
- details of the nature of the incident (eg, a virus, a DoS attack);
- details of how the incident has been noticed (eg, log files);
- a request for feedback; and
- an electronic signature.

As there are no recommended standard procedures that the notifying entity can follow in the meantime, it will need to wait for a response from the CERT. In any case, records of the incident should be saved in case they are destroyed or modified during the incident. For providers of critical infrastructure and digital services, the NISG stipulates that these voluntary reports are forwarded to the Federal Ministry for Internal Affairs by the CERT.

Unfortunately, there are currently no incentives to voluntarily disclose information on cyberthreats, apart from peer pressure within the industry.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In the field of cybersecurity, cooperation between the private and public sectors has a long tradition in Austria, its first highly visible project being the Computer Incident Response Coordination Austria, established in 2003 by the Internet Service Providers Association and the Federal Chancellery.

Nowadays, cooperation continues mainly within the Austrian CERT network, where the most important stakeholders from the private and public sectors are united either directly or indirectly through the participating CERTs. Within this network, not only is the collected information on incidents or threats exchanged but the incident response and the advice on prevention measures are also coordinated.

The results are then propagated by the participants to other organisations, such as the Chamber of Commerce, which issue recommendations to their members, usually in the form of publications. Of course, the flow of information works both ways.

In December 2014, Curatorship Safe Austria, an independent association focused on issues related to internal security, organised a large-scale cybersecurity exercise focused on threats to critical infrastructures, in which, among others, the CERTs, the Federal Ministry for Internal Affairs and various private enterprises participated. The aim of the exercise was to optimise communication between the participants, especially the stakeholders as well as the organisations serving as information hubs for their respective sectors. Smaller exercises were conducted annually in the following years. The results and experience gained during those exercises were taken into consideration in White Papers on cybersecurity published by Curatorship Safe Austria in early summer of the following year, containing recommendations for the planned Austrian Cybersecurity Act, now the NISG.

Further cooperation is expected in the issuing of industry-specific recommendations according to the GDPR.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance against cybersecurity incidents, covering the costs of, for example, data recovery or downtime, are offered by every major insurer active in Austria. In detail, the covered risks of course vary from offer to offer, with some providing cover even in the case of negligence or fault.

Despite its availability, cybersecurity insurance is as yet far from common. This has not changed with the introduction of the NISG.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Concerning the provisions of the General Data Protection Regulation (GDPR), the Data Protection Authority (DSB) is responsible for enforcing data security rules and penalising non-compliance in Austria.

According to article 83, para 4 GDPR, the DSB may impose a fine of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, on any business that has failed to implement the data security measures set forth in article 32 GDPR.

The prosecution of cybercrime is handled by the Cyber Crime Competence Centre (C4), which acts as a special unit of the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs, as

the case may be. Therefore, the powers of the C4 equal those of the authority they represent.

It should be noted that breaches of the GDPR (thus, also a breach of the provision on data security measures) constitute an act of unfair competition under Austrian law. As a consequence, enterprises may call upon the courts if they accuse a competitor of breaching data privacy or data security provisions. In practice, owing to the very low fines the DSB has imposed in the few months since the GDPR has entered into validity, despite much higher ones being possible by law, this poses the most relevant risk of litigation in the context of the GDPR.

The enforcement of the Network and Information Systems Security Act (NISG) is incumbent upon the Federal Government, the Federal Chancellor, the Federal Minister of Internal Affairs, the Federal Minister of National Defence and the Federal Minister for Europe, Integration and Foreign Affairs within the scope of their respective areas of responsibility. The regional administrative authorities are responsible for the prosecution of infringements of the NISG. They may impose a fine of up to €50,000 for each infringement (€100,000 in the case of recurrence).

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

In the case of a data breach notification according to article 33 GDPR or an alleged breach of data security provisions, the DSB initiates formal proceedings in which it can request statements and documents from any company concerned. Should the DSB find that the company has failed to comply with or document the data security rules set forth in article 32 GDPR, the DSB, similar to Austrian courts, is entitled to base its decision on the facts at hand but it cannot force the company to disclose any further information.

The C4, on the other hand, has access to all measures available to the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs. Thus, they are, for instance, even able to have documents confiscated. Since they are limited to the prosecution of cybercrime, however, they may not use their powers to merely monitor compliance with or prosecute infringements of data security rules.

Regarding providers of critical infrastructure or digital services, article 17, paras 4 and 5 and article 21, para 4 NISG provide that, in the case that the Federal Minister of Internal Affairs becomes aware that providers of critical infrastructure or digital services have failed to meet their obligation to take suitable and adequate security measures, he or she is authorised to demand providers to submit evidence of the security measures taken, including evidence of certification or inspections and, if applicable, security deficiencies discovered. The Federal Minister of Internal Affairs is also authorised to ensure inspection of the network and information systems used for the provision of critical infrastructure or digital services as well as any relevant documents. For this purpose, he or she is entitled to authorise the entry for inspection of locations where network and information systems are located, after prior notification. However, such inspection shall only be carried out to the extent absolutely necessary and with the greatest possible protection of the rights of the affected provider and third parties.

In addition, the Federal Minister of Internal Affairs is authorised to issue recommendations regarding the measures that providers will have to take within a reasonable period of time; otherwise they will be ordered by notice.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

Because of the current state of cybersecurity rules in Austria, no enforcement actions have yet been brought against the concerned companies by the Austrian authorities (namely the responsible CERTs or the DSB). While the DSB has already fined companies for lacking technical and organisational measures, no decisions have yet been published in which companies have been fined after cybersecurity incidents. In the publicly known cybercrime cases, the Austrian police have prosecuted the participating persons with varying degrees of success. However, no enforcement measures have been taken against the companies and institutions whose IT systems have been breached. Rather, they have received support from cybersecurity organisations to better secure their systems for the future.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

Apart from industry standards and recommendations, the NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation on providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability or failure of the service operated with significant impact. To assess whether the impact is significant or not, the anticipated number of users affected, the duration and the geographical spread, as well as the expected impact on economic and social activities must be taken into account.

The GDPR also sets forth data breach notification requirements. According to the GDPR, the national data protection authorities must be informed if the breach may result in a risk, no matter how small, to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical and organisational measures (eg, pseudonymisation, encryption).

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Apart from court actions by competitors (a breach of the GDPR constitutes an act of unfair competition under Austrian law), according to article 83, para 4 GDPR the DSB may impose fines of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements of the GDPR.

Concerning violations of the NISG, the regional administrative authorities may impose fines of up to €50,000 (€100,000 in the case of recurrence).

The prosecution of cybercrime is handled by the C4, which acts as a special unit of the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs, as the case may be. Therefore, the powers of the C4 equal those of the authority they represent.

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

The two data breach provisions in Austrian law are articles 33 and 34 GDPR.

According to article 33, the controller must notify the DSB without undue delay and not later than 72 hours after having become aware of a personal data breach. A notification may only be omitted if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where a breach has occurred at a processor, he or she must notify the controller, who will then notify the DSB.

Irrespective of whether or not personal data breaches may result in a risk to the rights and freedoms of natural persons, and thus require notification to the DSB, a controller is obliged to document each breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation must be presented to the DSB upon request to enable the DSB to verify compliance with article 33.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is furthermore obliged to notify the affected data subjects (ie, the natural persons) without undue delay. However, appropriate remedial or technological measures (eg, secure encryption of the personal data) may be considered to lower the risk sufficiently to relieve controllers of the notification duty of article 34 GDPR. Unlike the former Austrian notification rule of the Austrian Data Protection Act 2000, the controllers may not omit notification of the data subjects in the case that individual notifications would be considered disproportionate. Rather, they are now obliged to publicly communicate the personal data breach.

The DSB may review the controller's interpretation of the severity and possible consequences of an incident and oblige him or her to inform the data subjects or confirm that the level of risk is sufficiently low for such notification to be omitted.

These provisions, however, only apply to breaches where personal data is affected. As a result, no notification requirement exists for cyberthreats or breaches where no personal data is involved (though the latter is statistically quite unlikely).

Article 83, para 4 of the GDPR allows the DSB to impose fines of up to €10 million or 2 per cent of the total worldwide annual turnover of the preceding financial year if the data breach notification and documentation requirements are not met.

The NISG introduced data breach notification requirements for providers of critical infrastructure and digital services that go beyond the scope of articles 33 and 34 GDPR. If these requirements are not met, fines of up to €50,000 pre-infringement (€100,000 in the case of recurrence) may be imposed.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

As a result of the lack of any specific rules on cybersecurity and the consequences of non-compliance, private redress can only be sought before civil courts following general tort rules. This means that any person seeking redress would need to claim a concrete amount for damages and also prove that the damages in the desired amount have actually been caused by the defendant.

Even in the case of a breach of data protection rules, parties would need to call upon civil courts for any redress, as the DSB and the regional administrative authorities may only impose fines. Nevertheless, the decision of the DSB or a regional administrative authority would be required in such a case to determine whether a breach of data protection rules has occurred in the first place.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Apart from industry standards and recommendations, article 32 of the General Data Protection Regulation (GDPR) requires any controller or processor of personal data to implement measures to ensure data security. However, such measures need to take into account the type, extent and purpose of the processed data, the state of the art and the economic feasibility. Therefore, even though this provision does stipulate minimum protective measures, it is not clear what the minimum requirements in each case may be. Further, this provision only applies to personal data rather than any type of data. As a result, in the field of cybersecurity, industry standards and the recommendations of the Austrian Computer Emergency Response Team (CERT) and Austrian Government Computer Emergency Response Team (GovCERT) are more important in Austria than legal rules. This is especially true for relatively new technology such as cloud computing, the internet of things or the issues associated with various forms of 'bring your own device'.

Also, recommendations and standards for appropriate technological and organisational measures defined by the European Commission, national data protection authorities and industry-specific organisations will, in the end, set forth the minimum requirements for cybersecurity any company will need to meet. Currently, however, except for individual rulings, the only binding rules and guidelines issued by the Austrian Data Protection Authority are two regulations on privacy impact assessments (PIA), one listing processing operations that do not require a PIA to be performed (Exceptions from the PIA, DSFA-AV, published 25 May 2018) and one listing processing operations that in any case require a PIA to be performed (DSFA-V, published 9 November 2018).

Furthermore, providers of critical infrastructure must take measures to ensure a high level of security of network and information systems according to articles 17, 21 and 22 of the Network and Information Systems Security Act (NISG).

According to articles 17, 21 and 22 NISG, appropriate measures need to take into account the state of the art and be appropriate to any risk that can be determined with reasonable effort. Therefore, providers of critical infrastructure must take into account the following: safety of systems and facilities; management of security incidents; business continuity management; monitoring; verification and testing; and compliance with international rules. The security measures should include: governance and risk management; dealing with service providers, suppliers and third parties; security structure; system administration; identity and access management; system maintenance and operation; physical security; detection and handling of security incidents; business continuity; and crisis management. These security measures are regulated in more detail in Appendix 1 to the Network and Information Systems Security Ordinance.

To enable verification of the measures taken, providers of critical infrastructure must submit a list of the security measures they have carried out, including evidence of certification or inspections and, if applicable, security deficiencies discovered, to the Federal Minister of Internal Affairs at least every three years. The Federal Minister is also authorised to issue recommendations regarding the measures that providers will have to take.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

As such records do not fall within the scope of Austrian legal rules on the keeping of documents (eg, contracts, invoices), the only applicable rules are article 32 GDPR and those determined by industry standards or recommendations, such as ISO/IEC 27001 (which can be obtained from the ISO or ASI against payment), the recommendations of the German Federal Office for Information Security and the recommendations of the CERT (available from their respective websites: www.bsi.bund.de and www.cert.at). These three can be regarded as the main industry standards and codes of practice in the field of cybersecurity.

In addition, comprehensive guidelines summarising the relevant rules and recommendations, as well as a checklist created specifically

for very small enterprises, have been created by the Austrian Chamber of Commerce and can be obtained from www.it-safe.at.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Apart from industry standards and recommendations, the NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation of providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability or a failure of the service operated with significant impact. To assess whether the impact is significant or not, the anticipated number of users affected, duration, geographical spread and expected impact on economic and social activities must be taken into account.

The GDPR also sets forth data breach notification requirements. However, according to the GDPR the national data protection authorities only need to be informed if the breach may result in a risk to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical or organisational measures (eg, pseudonymisation, encryption).

Time frames

30 | What is the timeline for reporting to the authorities?

As of 25 May 2018, the date the GDPR entered into validity, companies must notify the national data protection authority in case of any risk to the rights and freedoms of a natural person without undue delay and as far as possible within 72 hours after the person responsible has become aware of the breach; any delay must be justified. If said risk is high, the natural person will also need to be notified. In addition, according to the NISG, providers of critical infrastructure and digital services are obliged to report security incidents without undue delay to the national computer emergency team, or if none has been set up or the incident occurred in a federal institution, to the GovCERT, which will immediately forward the report to the Federal Minister of Internal Affairs.

However, the obligation of providers of digital services to report a security incident only applies if they have access to the information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability or a failure of the service operated with significant impact. To assess whether the impact is significant or not, the anticipated number of users affected, duration, geographical spread and expected impact on economic and social activities must be taken into account.

If a security incident involving a provider of digital services affects one or more EU members, the Federal Minister of Internal Affairs or the competent computer emergency team must inform the single point of contact (SPOC) in the affected state.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

According to article 34 GDPR, providers are obliged to notify the affected data subjects (ie, natural persons) in the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons without undue delay. However, appropriate remedial or technological measures (eg, secure encryption of the personal data) may be considered to lower the risk enough to relieve providers of this notification duty. Unlike the former Austrian notification rule of the Austrian Data Protection Act 2000, the controllers may not omit notification of the data subjects in the case that individual notifications would be considered disproportionate. Rather, they are now obliged to publicly communicate the personal data breach. The Data Protection Authority may review the controller's interpretation of the severity and possible consequences of an incident and oblige him or her to inform the data subjects or confirm that level of risk is sufficiently low for such notification to be omitted.

These provisions, however, only apply to breaches where personal data is affected. As a result, no notification requirement exists for cyberthreats or breaches where no personal data is involved (though the latter is statistically quite unlikely).

The NISG, on the other hand, does not provide any reporting obligations to others in the industry, customers or the general public.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

After the entry into effect of the General Data Protection Regulation (GDPR), currently the biggest legal challenge businesses are facing is the increased focus of the data protection authorities on accountability for the technical and organisational measures implemented. Thus, where the lenient treatment of infringements and lax cybersecurity in 2018 led many companies to consider their implementation of the GDPR rules as future-proof, a sharp increase in fines in 2019 caused a trend in re-evaluating the existing measures. The sometimes forced and hurried implementation of conferencing and collaboration solutions by many Austrian companies to enable work to continue during the covid-19 related lockdowns created another potential problem, not only in regard to data protection, but also in regard to IT security.

A further open question is the impact of the relatively recent NIS Act (the Austrian transposition of the EU Directive on Security of Network and Information Systems (NIS Directive)) on cybersecurity best practices solutions. While, in principle, it is only binding for providers

MGLP
RECHTSANWÄLTE | ATTORNEYS-AT-LAW

Árpád Geréd
a.gered@mglp.eu

Museumstraße 5
1070 Vienna
Austria
Tel: +43 1 997 19 66
www.mglp.eu

of critical infrastructure, decisions and recommendations on best practices are also expected to influence measures taken by other, non-critical businesses. Such decisions and recommendations are, however, slow in coming.

Also, covid-19 has posed, and still does pose, a significant challenge for companies. One of the main issues they have faced was keeping their offices and businesses operational, first during lockdown and afterwards with strict distancing rules in force. As a solution, many companies have, sometimes hurriedly, implemented software solutions for tele- and collaborative working, enabling their employees to (also) work from home. However, even after the entering into force of the Austrian Homeoffice-Act, there are still no rules on technology, data protection and cybersecurity for working from home. The only 'guidelines' for data protection and cybersecurity in home office can be found in the information sheet of the Austrian data protection authority.

A programme that was not created as a result of covid-19, but has proved quite important due to it, is the 'Vienna digital' programme of the city of Vienna. Within the scope of the programme, small and medium-sized enterprises with an establishment in Vienna can – if certain conditions are met – receive funding of 30 per cent of their investments (to a maximum of €40.000) in digitalisation projects, including cybersecurity measures.

Last, but not least, it should also be mentioned that at the end of 2021, the EU Council of Ministers presented a draft for the amendment of the NIS Directive (NIS2), which became necessary because the provisions relating to reporting obligations for serious cyber incidents in particular did not work out as planned. Thus, the provisions of the amended directive will also have to be observed in the future, although the concrete consequences of the amendment remain to be seen. However, no major direct impacts are to be expected for Austria.

Belgium

Camille De Munter*
NautaDutilh

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

While there are no dedicated cybersecurity laws, some laws contain provisions relating to cybersecurity.

First, there are general regulations such as the Belgian Criminal Code (BCC, which notably implements the Cybercrime Convention and includes provisions on professional secrecy), the General Data Protection Regulation 2016/679 (GDPR) and the Belgian Act of 30 July 2018, which supplements the GDPR. Second, there are more sector- or activity-specific rules, such as:

- in respect of essential services, the Belgian Act of 7 April 2019 (Belgian NIS Act) and the Act of 1 July 2011 (Belgian Critical Infrastructures Act), which implement respectively the NIS Directive and the Directive on European Critical Infrastructures;
- in the telecommunications sector, Commission Regulation No. 611/2013 and the Belgian Act of 13 June 2005 (BAEC), implementing the ePrivacy Directive and modified in December 2021 to implement the European Electronic Communications Code;
- in relation to trust service providers (TSPs), the eIDAS Regulation (EU Regulation 910/2014); and
- in relation to payment service providers (PSPs), the PSD2 Act of 11 March 2018 (implementing PSD2).

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The sectors of essential services and critical infrastructure are the most affected by cybersecurity laws. Such sectors are:

- the energy sector (electricity, petroleum and gas);
- the transport sector (air, rail, water and road transport);
- financial operators (financial institutions, financial trading platforms and PSPs);
- the health sector (healthcare facilities, including hospitals and private clinics);
- the sector dealing with clean water;
- the telecommunications sector;
- TSPs; and
- digital infrastructures (including digital service providers).

In light of the covid-19 pandemic, cloud service providers and providers of solutions allowing homeworking have improved the cybersecurity of their networks. Moreover, high-profile enterprises such as Microsoft, Google and Tesla have issued bug bounty programmes, where anyone can obtain a monetary reward when pointing out one of their security flaws. The automotive sector has also made cybersecurity improvements, notably after the adoption of UN Regulations No. 155 (Cyber security and cyber security management system) and No. 156 (Software update and software update management system), which apply in the European Union from July 2022.

With regard to sectors clearly needing to improve, internet of things devices in general have often been shown to be vulnerable. The same applies to the public sector (schools, government agencies, etc) and healthcare institutions. The tragic death in September 2020 of a patient in Germany as a result of a ransomware attack on a hospital was reported in the Belgian press, but it did not lead to any visible movement on the part of the Belgian healthcare sector.

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

Operators of essential services (OES) must have a security policy in relation to information systems and networks, and the Belgian NIS Act includes the very first recognition of ISO/IEC 27001 in this respect, stating that the required security policy is presumed compliant with the relevant requirements of the Belgian NIS Act if an organisation has ISO/IEC 27001 certification. In addition, the former Belgian Privacy Commission (now replaced by the Belgian Data Protection Authority (BDPA)) had issued guidelines on information security based on ISO 27002:2013, ISO 27005:2011 and ISO 27018:2014. Unfortunately, those guidelines are no longer available and the BDPA has not issued anything referring to such international standards yet (though its case law refers to certain best practices).

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

In principle, an employer is liable for the behaviour of its personnel and directors (with certain exceptions). Therefore, in the case of inadequate cybersecurity, the employer will be liable towards a third party for any damage caused provided the party claiming compensation can prove a clear link of subordination between the employer and its personnel; a 'fault' (eg, negligence) made by its personnel; damage or loss arising from such fault; and the link between the fault and the function exercised by the personnel (article 1384 Belgian Civil Code).

For the same reasons, it is likely that any fines will be imposed on the employer, not the personnel or directors individually.

However, the personnel's (in)action and 'fault' could be considered as gross negligence or be constitutive of an infringement of an internal security policy, leading to the person's dismissal. Moreover, the responsible individual can be held criminally liable in front of criminal jurisdictions.

5 How does your jurisdiction define cybersecurity and cybercrime?

Cybercrime, on the one hand, encompasses the crimes of internal and external hacking, which are respectively defined as a person exceeding his or her access rights with fraudulent intent and a person granting to him or herself, knowingly, unauthorised access to an IT system (articles 550-bis sections 1 and 2 BCC). Internal hacking does not cover the reuse of authorised access, but that can be considered as a breach of trust, a more general criminal offence (Cass., 24 January 2017, P.16.0048.N). The criminal handling of hacked data also constitutes a criminal offence (article 505, section 1, 1° BCC). Another cybercrime is that of 'data manipulation', which occurs when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of such data. Furthermore, 'system interference' is the cybercrime of data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter BCC). When such an act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater BCC).

Cybersecurity, on the other hand, is to be distinguished from data privacy and data protection, as cybersecurity is about protecting information, whether it is personal data or non-personal data, and cybersecurity in relation to personal data is merely one component of data protection (which also encompasses various other aspects, such as storage limitation and data minimisation).

The EU Cybersecurity Act (Regulation 2019/881) further defines cybersecurity as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' (article 2(1)).

Information system security is to be distinguished from cybercrime enforcement in practice, due to the involvement of regulatory authorities (and, in particular, specialised police units) in the latter, while the former is more general.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The general rules of Belgian law do not specify any specific minimum measures, such as requirements to use encryption or to have a strong password policy. Instead, these rules provide for a general requirement to implement appropriate technical and organisational measures.

For instance:

- Under data protection rules, this principle applies (see article 32, GDPR), with illustrations such as pseudonymisation and encryption of personal data.
- Regarding trade secrets, organisations must take reasonable steps, considering the circumstances, to keep them a secret and thus benefit from legal protection.
- In the telecommunications sector, providers of public electronic communications networks and of publicly available electronic communications services (ECSP) must take appropriate technical and organisational measures, taking into account the potential risks and the technical state of the art (article 107/2, BAEC). Data relating to user identification must be subject to the same security requirements during storage as when it is on the network. Such data must be unreadable and useless for anyone who is not authorised to have access to it (article 126(4), BAEC).
- In the realm of essential services, OES must ensure a level of physical and logical security, having regard to the technical state of the art, with appropriate and proportionate technical and organisational measures (article 20, Belgian NIS Act):
  - in addition, digital service providers (DSPs) must take appropriate and proportionate technical and organisational measures, with regard to the technical state of the art, to manage the risks of security of network and information systems (article 33, Belgian NIS Act); and
  - critical infrastructure operators are also required to identify in a security policy the measures taken to prevent, mitigate and neutralise interruption or destruction risks.
- In the financial sector, PSPs must ensure a high level of technical security and data protection (article 51, PSD2).
- Finally, TSPs must, having regard to the latest technological developments, take appropriate technical and organisational measures to manage the risks posed to the security of the trust service they provide (article 19, eIDAS regulation).

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

First, the rules on professional secrecy prohibit certain professions from disclosing their clients' secrets, except where foreseen by law (article 458, BCC). Moreover, employees are prohibited from disclosing manufacturing secrets (article 309, BCC) and no one is permitted to unlawfully acquire, use or disclose trade secrets.

On the side of more traditional, 'hard' intellectual property rights, patentable inventions must be 'novel' to benefit from protection by way of a patent; secrecy is therefore crucial to benefit from protection (lack of secrecy prior to filing means that the patent application is not novel). However, a clear misuse of rights leading to a breach of secrecy does not prevent the obtaining of a patent (article XI.6, section 6 Belgian Code of Economic Law).

Finally, in the event of 'theft' of a potential trademark, any trademark registration following such breach of secrecy will be made in bad faith and can thus be invalidated (article 2.2-bis section 2, Benelux Convention on Intellectual Property; article 59(1), EU Trade Mark Regulation).

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

First, the Belgian NIS Act implements the NIS Directive and contains provisions on cybersecurity for essential services, such as:

- the energy sector (electricity, petroleum and gas);
- the transport sector (air, rail, water and road transport);
- financial operators (financial institutions and financial trading platforms);
- the health sector (healthcare facilities, including hospitals and private clinics);
- the sector dealing with clean water; and
- digital infrastructures.

The Belgian Critical Infrastructures Act also includes specific rules for critical infrastructure operators, such as the obligation to have a security policy identifying measures to handle certain risks.

Secondly, provisions regarding telecommunications are described in the BAEC, implementing the ePrivacy Directive.

Finally, Belgium has adopted the PSD2 Act of 11 March 2011 about payment services.

9 | Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Belgian law prohibits various kinds of use of electronic communications without the consent of each person directly or indirectly involved in the communication (article 124, BAEC). This prohibition covers both the content of the communication and its metadata, and it includes intentionally becoming aware of the existence of information not intended for the person in question; intentionally identifying the persons involved in the transmission and its content; intentionally obtaining electronic communications data relating to another person; and making any use whatsoever of the aforementioned information, identification or data obtained.

However, there are exceptions to this rule, such as acts performed to verify the proper functioning of the network and the electronic communication service, and the prevention of unwanted electronic communications providing the end-user has given his or her authorisation, as well as combating fraud committed by means of messages using telephone numbers under certain conditions (articles 125, 2°, 6° and 7°, BAEC).

Telecommunications operators are subject to additional rules in relation, for example, to the use of metadata (notably with reference to the obligation to cooperate with competent authorities in the investigation and prosecution of criminal offences, as well as the possibility to use metadata for fraud detection (article 122, sections 1 and 4, BAEC)0. Location data is subject to even stricter rules and can as a rule only be processed if rendered anonymous or when the processing of location data is part of a location data service (article 123, BAEC).

10 | What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

First, external hacking and internal hacking are both criminalised (article 550-bis sections 1 and 2, BCC). External hacking occurs when a person knowingly grants him or herself unauthorised access to an IT system, while internal hacking occurs when a person exceeds his or her access rights with fraudulent intent. Internal hacking does not cover the reuse of authorised access, but that can be considered as a breach of trust, a more general criminal offence (Cass., 24 January 2017, P.16.0048.N). The criminal handling of hacked data also constitutes a criminal offence (article 505, section 1, 1°, BCC).

Another cybercrime is that of 'data manipulation', which occurs when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of such data. Furthermore, 'system interference' is the cybercrime of data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter, BCC). When such an act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater, BCC).

Secondly, when a person knowingly (directly or indirectly) enters, modifies or deletes data into or from an IT system or modifies the normal use of this data, this is a criminal offence called 'data manipulation'. The offence of 'system interference' is data manipulation that fully or partly hinders the functioning of an IT system (article 550-ter, BCC). When such act occurs with fraudulent intent to acquire an unlawful economic advantage, it is an 'information technology fraud' (article 504-quater, BCC).

11 | How has your jurisdiction addressed information security challenges associated with cloud computing?

Cloud computing service providers are considered as DSPs under the Belgian NIS Act and must therefore identify risks to the security of network and information systems that they use. Moreover, they must take appropriate and proportionate technical and organisational measures to manage such risks (article 33, Belgian NIS Act). Having regard to the technical state of the art, those measures must take into account the security of systems and facilities; how DSPs handle incidents; the business continuity management; and the monitoring, auditing and testing of security. While there is no legal requirement to do so, compliance with international standards, such as those embedded in the Standards Supporting Certification report from ENISA, can be a useful means of evidence of such measures.

12 | How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

This varies from one cybersecurity law to another. Cybersecurity legislation only applies to foreign organisations when it mentions it expressly. Most cybersecurity laws have no extraterritorial scope.

The GDPR affects foreign organisations when they process personal data from citizens of the European Union. The Belgian NIS Act applies to any OES having at least an establishment on Belgian territory and effectively exercising an activity linked to the provision of at least one essential service on Belgian territory. This Act also applies to DSPs having their registered office in Belgium, as well as to DSPs without an establishment in the EU but that provide services in Belgium and have a representative in Belgium. The BAEC applies to foreign organisations only where they conduct relevant activities in Belgium. The PDS2 Act only applies to European organisations conducting activities in Belgium or organisations that are established in Belgium.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Belgian Privacy Commission, predecessor of the Belgian Data Protection Authority (BDPA), had issued guidelines on information security. Unfortunately, those guidelines are no longer available and the BDPA has not issued any guidance of its own. The BDPA's own case law suggests best practices for compliance with the General Data Protection Regulation's (GDPR) general obligation regarding cybersecurity (article 32, GDPR), such as having SSL for web forms involving the processing of health-related data (decision No. 117/2021 of 22 October 2021) and logging mechanisms and access control for managers as well (decision No. 56/2021 of 26 April 2021).

Beyond regulator publications, it is common practice in Belgium to refer to guidelines from ENISA (see notably the recent Railway Cybersecurity – Good Practices in Cyber Risk Management or its Cybersecurity guide for SMEs) and the ecoDa Handbook (which provides useful guidance for organisations on how to integrate cybersecurity considerations at board level) as well as the NIST Cyber Security Framework.

14 How does the government incentivise organisations to improve their cybersecurity?

The government incentivises organisations to improve their cybersecurity through cybersecurity cheques, tax cuts and fines.

Firstly, the Walloon government created a 'cybersecurity cheque', allowing SMEs to receive up to €60,000 in three years, to help them with cybersecurity audits and diagnostics and the creation of a cybersecurity policy. Similar to the cybersecurity cheque, the 'digital maturity cheque' aims to help SMEs to transition into digital and cybersecure organisations.

Secondly, the Flemish side of the country allows several tax schemes to promote cybersecurity innovations. For instance, they allow up to 85 per cent tax cuts on income generated by innovations related to cybersecurity.

Thirdly, sector-specific legislation often imposes fines following the non-compliance of their provisions. For instance, the BDPA has the ability to give administrative fines of (in theory) up to €10 million or 2 per cent of the total worldwide annual turnover for violations of the GDPR. To date, the amount of fines has been significantly lower, but there is a trend towards increasing fines.

In addition, non-compliance with other legislation can lead to fines and other sanctions:

- criminal fines of up to €400,000 for non-compliance with the Belgian Act of 13 June 2005;
- fines between €500 and €100,000 as well as criminal penalties up to €240,000 for non-compliance by operators of essential services (OESs) and digital service providers (DSPs) with security measures obligations under the Belgian NIS Act, double in case of recidivism;
- in the case of payment service providers (PSPs), administrative fines between €10,000 and 10 per cent of yearly net turnover (based on the previous accounting year) or penalty fines of maximum €2.5 million per infringement of PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance; and
- (non-qualified) trust service providers (TSPs) may lose their ability to provide (non-)qualified trust services. The service provider losing his 'qualified' status must inform the users of its services about it (article XV.26, BCEL). If the service provider falsely claims having a 'qualified' status, he may face up to €800,000 of criminal penalties.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

PSPs must comply with the guidelines and standards issued by the European Banking Authority – EBA (article 52, PSD2 Act). Other useful industry standards include those issued by ETSI, such as those on consumer internet of things cybersecurity (ETSI EN 303 645 v2.0.0 [European standard] and ETSI TS 103 645 [technical specification]). Moreover, ENISA published a report about Standards Supporting Certification and is working to facilitate European standards. Finally, the ecoDa Handbook includes various references to useful standards and guidance.

16 Are there generally recommended best practices and procedures for responding to breaches?

In terms of compliance with legal obligations, in Belgium, reference is often made to the guidance by the former article 29 Working Party (WP29) on personal data breach notification to notify personal data breaches, the EDPB's Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (as modified in December 2021) and ENISA's methodology to assess risks in case of personal data breaches, as well as ENISA's reports on incident notifications for DSPs and TSPs.

PSPs also have the obligation to ensure monitoring, handling and follow-up of security incidents and customer claims linked to security (article 53(1) PSD2 Act), and the EBA's guidelines regarding incident notifications are important for PSPs in this respect.

More generally, regarding the handling of breaches (and not limited to official guidance on notifications), the ecoDa Handbook includes best practices that are increasingly referred to (eg, involvement of third-party forensic firms, sometimes via legal counsel to better protect confidentiality of the findings; regular tests of response to data breaches through simulations; etc).

Information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Data breaches or specific cyberthreats entail various notification obligations. However, voluntary notifications are also possible. For instance, potential OESs can voluntarily notify cybersecurity incidents to the national Computer Security Incident Response Team (CSIRT), the sector-specific authority or sector CSIRT, and to the national authority for identification of operators of essential services (article 30, Belgian NIS Act), although there are no clear incentives in the event of such notifications. More generally, at the level of the BDPA, voluntary notifications are also possible outside of the cases where a notification is required, and this is generally well perceived by the BDPA.

However, there is also a risk to even voluntary notifications, given that any indication that the breach was due to security failings or that the surrounding circumstances suggest an infringement of applicable requirements (eg, data protection principles) could give rise to an investigation.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

At this stage, there is no true structure for cooperation and the development of cybersecurity standards and procedures. From time to time, actors from the private sector act as consultants for the government regarding cybersecurity, but it typically depends on whether the government is prepared to start a (public or private) consultation process. This lack of interaction can lead to enforcement issues, as cybersecurity and data protection laws are often difficult to implement perfectly from a practical and business point of view.

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Cyber risk insurance is available in Belgium and adoption thereof is increasing. However, the exclusions and conditions accompanying such – in particular, exclusions of acts of war, given that some cyberattacks can be linked to disputes between nation states – have often given rise to discussions. Moreover, coverage is sometimes conditional upon demonstration of appropriate security measures put in place by the organisation, and insurers often send detailed questionnaires regarding the level of security prior to any premium being calculated. Finally, in practical terms, such insurance policies often require evidence in the form of a complaint with the police before they cover a breach, and although they cover certain costs there are frequently limitations in terms of which service providers can be covered and up to what amount (or for how many hours or days after an incident occurs all

qualifying costs are covered – eg, with the first 24 hours of legal support being covered).

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Belgian Data Protection Authority (BDPA) is the regulatory authority responsible for enforcing the General Data Protection Regulation (GDPR) (with specific additional authorities, such as a dedicated one for bodies forming part of the Flemish regional government). Other authorities responsible for enforcing compliance with information security standards are different from sector to sector. First, the Belgian National Bank may impose (administrative and penalty) fines to payment service providers (PSPs). Secondly, the Minister of Economy is in charge of enforcing cybersecurity rules for trust service providers (TSPs), with certain powers for the BDPA. Thirdly, the Belgian Institute for Postal Services and Telecommunications (BIPT) is in charge of compliance with the Belgian Act of 13 June 2005 (BAEC), in the telecommunication sector (with some rules falling within the jurisdiction of the BDPA). Finally, the national Computer Security Incident Response Team (CSIRT), the sector CSIRT, the national authority for identification of operators of essential services (OESs) as well as the Belgian National Bank are responsible for enforcing the Belgian NIS Act.

The authorities charged with prosecuting cybercrimes are the police and specialised units. The latter encompass the Regional Computer Crimes Units (RCCU), which conducts technical investigations and identify culprits and the Federal Computer Crime Unit, which has a strategic role and the operational role of supporting RCCU investigations.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Organisations are subject to cooperation obligations under various laws (eg, article 31, GDPR; article 122, sections 1 and 4, BAEC; article 46, Belgian NIS Act).

In addition, certain laws require organisations to actively document their processes (see eg, article 5(2) and 24 GDPR and article 107/3, section 4, BAEC), which creates authorities' expectations that these documents are readily available.

From the perspective of Belgian data protection law, for instance, the BDPA's Inspection Service and Litigation Chamber both tend to interpret articles 24 and 31 GDPR broadly, such that refusal to provide documents – even if they are not particularly relevant for a particular complaint – has been used against controllers in the past.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common issues that gave rise to enforcement are the assessment of risk in the event of an incident and knowing when to notify an incident and the existence (or lack) of sufficient measures to protect information or personal data.

Notably, one case before the BDPA revolved initially around whether the organisation had an adequate methodology for dealing with potential data breaches. After initially bringing the methodology into question, the case ended up focussing on other aspects (such as the role of the Data Protection Officer), likely because as the case progressed, the BDPA recognised the merit of the methodology used.

In 2021, two BDPA decisions had a more marked focus on cybersecurity:

- In a decision of 26 April 2021 (decision No. 56/2021), the BDPA stated that 'the absence of any system for access control of managers' in the relevant case was a 'blatant violation' of article 32 of the GDPR, in particular because the data accessible through the system was 'sensitive financial data'. This nature meant that the risks to the fundamental rights of data subjects were high, such that the measures taken had to be 'all the more appropriate'. The lack of logging or other security measures was also viewed as preventing data subjects from exercising their right of access concerning the (unlawful) processing carried out, since the financial institution did not keep any evidence of such processing.
- In a decision of 22 October 2021 (decision No. 117/2021), the BDPA held in relation to a website that health-related data (and their transfer and transmission) should be 'sufficiently secured' and that they should 'as a result and among others be sent with sufficiently strong encryption from the user's computer to the server for a website with a form. This can take place by use of a security certificate'. This suggests that SSL is considered a minimum requirement for web forms likely to involve health-related data.

In terms of incident response, the private sector has largely started referring to approaches quoted in previous questions, such as ENISA's data breach severity assessment methodology (for data protection), ENISA's digital service providers (DSP) incident notification report (for DSPs under the NIS rules) and the EBA's guidelines for PSPs.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

Depending on the applicable legal framework, several distinct notification obligations may apply.

First, under data protection rules, processors must notify controllers of any personal data breach relating to the personal data processed on behalf of the controller; a controller in turn must notify any personal data breach to the authority (in Belgium the BDPA) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (with three separate use cases having been identified by WP29). Data subjects must be notified of any personal data breach by controllers if such breach is likely to result in a high risk to their rights and freedoms (with three [other] use cases in which the GDPR considers that there is no 'high' risk).

When there is a risk of breach of the network security, publicly available electronic communications services (ECSPs) must notify such risk to the BIPT; where there is a personal data breach, they must notify it to the BDPA. ECSPs must also notify individuals where a personal data breach is likely to adversely affect their data or privacy, unless technological protection measures rendered the data unintelligible to anyone not authorised to access it. In addition, in the case of a specific and significant threat of a cybersecurity incident, the ECSP must inform any users that are potentially affected by such incident.

OESs and DSPs are subject to incident notification obligations as well: OESs for any incidents having a significant impact on the continuity of the essential services they provide; DSPs for any incidents having a substantial impact on the provision of the digital service (as defined) provided by the DSP in question. OESs must notify incidents simultaneously to the national CSIRT, the sector-specific authority or sector CSIRT and the national authority for identification of operators of essential services. FSOs must notify breaches to the National Bank of Belgium (article 25 Belgian, NIS Act and 96 PSD2). Those notification obligations apply even if there is not enough information for the determination of the notion of a 'significant impact'.

PSPs must notify any major operational or security incident to payment service users, if the incident may have or has an impact on their financial interests (article 96, PSD2).

TSPs must notify to the BDPA any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay (article 19, eIDAS).

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Failure to comply with the GDPR can in theory lead to administrative fines up to the higher of €10 million or 2 per cent of the total worldwide annual turnover (though to date, the highest fine for non-compliance with article 32, GDPR in Belgium was €100,000). Secondly, non-compliance with the BAEC can lead to criminal fines of up to €400,000. Furthermore, non-compliance with security measures obligations from the NIS can incur a fine between €500 and €100,000 as well as criminal penalties of up to €240,000. The fines are doubled in the event of recidivism.

Moreover, PSPs may be imposed administrative fines between €10,000 and 10 per cent of their yearly net turnover (based on their previous accounting year) or penalty fines of maximum €2.5 million per infringement of the PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance.

Finally, (non-qualified) TSPs may lose their ability to provide (non-) qualified trust services. The service provider losing his or her 'qualified' status must inform the users of its services of this (article XV.26 BCEL). The false claim of 'qualified' status may lead to a maximum of €800,000 of criminal penalties.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In theory, the BDPA has the ability to impose administrative fines up to the higher of €10 million or 2 per cent of the total worldwide annual turnover for failure to comply with the rules on reporting threats and breaches in relation to personal data (including failures from the telecommunication sector).

Furthermore, failure of DSPs and OESs to comply with notification obligations may amount to a fine of between €500 and €75,000 or even to criminal penalties up to €160,000. Fines are doubled for recidivists.

Moreover, PSPs may receive administrative fines of between €10,000 and 10 per cent of their yearly net turnover (based on their previous accounting year) or penalty fines of maximum €2.5 million per infringement of PSD2 (or both) or a maximum of €50,000 per (further) day of non-compliance.

Finally, (non-qualified) TSPs may lose their ability to provide (non-) qualified trust services. The service provider losing his 'qualified' status must inform the users of its services about it (article XV.26, BCEL). The false claim of a 'qualified' status may lead to a maximum of €800,000 of criminal penalties.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties may seek private redress in front of the courts against individuals (article 1382, Belgian Civil Code) or organisations (article 82, GDPR) to receive damages, provided demonstration of a 'fault' (eg, negligence) by the individual or the infringement of the GDPR by the organisation; the prejudice suffered by the parties; and the causal link between the aforementioned fault or infringement and prejudice.

Also, more and more organisations acquire the necessary status to initiate class actions to claim for collective redress (articles XVII.36 and XVII.39, BCEL). For instance, the privacy activism organisation NOYB has acquired this right in Belgium.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Few laws require specific policies or procedures, and even fewer currently require specific measures. Typically, the rule is that the organisation itself must decide what is appropriate – and that can then be challenged by the regulator.

The combination of various data protection principles (including the principles of 'data protection by design' and 'data protection by default') can be viewed as requiring companies to implement procedures to take cybersecurity into account in relation to personal data at every stage of the lifecycle of a data-related initiative. For instance, security is an important element to take into account when carrying out a 'data protection impact assessment' when their processing activity poses a high risk to the rights and freedoms of natural persons (article 35, General Data Protection Regulation (GDPR)).

The Belgian Data Protection Authority's (BDPA) predecessor, the Belgian Privacy Commission, had issued more specific guidelines on information security (on the need to have access controls (permissions; authentication; …) in place, on the importance of a security policy, etc), but those are no longer available. Instead, the BDPA's case law suggests specific measures that are required (eg, having SSL for web forms involving the processing of health-related data, and logging mechanisms and access control for managers as well).

Some sector-specific laws go further. For instance, qualified trust service providers (TSPs) must train their staff and subcontractors about security and must use trustworthy systems (article 24(2), eIDAS Regulation). Qualified electronic signature creation devices must be subject to certification that involves a security assessment (article 30, eIDAS Regulation). Moreover, the whole process for validating qualified electronic signatures must allow the person requesting validation to detect 'any security relevant issues' (article 32, eIDAS Regulation).

In the NIS and critical infrastructure legislation, security policies are required, but the content remains at the discretion of the organisation (although ISO/IEC 27001 certification is evidence of compliance with this requirement, according to the Belgian NIS Act).

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the GDPR, any controller must document any personal data breaches, including those not notified to an authority or data subject (article 33(5), GDPR). There is no guidance about the specifics of collecting or storing those records, but the BDPA has started to request ever more frequently a copy of such registers of breaches.

In terms of duration, data protection infringements are time-barred after five years in Belgium, as a result of which it is likely organisations will wish to keep such records for at least five years.

Outside of data protection, another statute of limitation may apply, so it is important to bear each situation into account when deciding on the retention period for such records.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Controllers must notify to the BDPA cybersecurity breaches that are likely to result in a risk to the rights and freedoms of natural persons. Such notification must contain the nature of the breach, the person to contact to obtain further information, a description of the likely consequences and the measures (proposed to be) taken to mitigate the adverse effects of the breach.

When there is a risk of breach of the network security, publicly available electronic communications services (ECSPs) must notify such risk to the Belgian Institute for Postal Services and Telecommunications (BIPT). The notification must contain, if the risk cannot be fully mitigated by the ECSP, the measures allowing such mitigation and an indication of their likely cost. If there is a personal data breach, the ECSPs must notify it to the BDPA. Therein, the ECSP must include their identity and their person of contact; the nature of the breach and the incident that caused it; the scope of the breach; the potential consequences for individuals; and the technical and organisational measures (to be) applied.

In the case of a specific and significant threat of a cybersecurity incident, ECSPs must inform the BIPT thereof and must indicate any protective or remedial action that its users should take and any measures it has taken or plans to take (article 107/3, Belgian Act of 13 June 2005 (BAEC)).

Operators of essential services (OESs), digital service providers (DSPs) and financial services operators (FSOs) must notify incidents having a significant impact on the availability, confidentiality, integrity or authenticity of network and information systems used by the essential service (article 24, Belgian NIS Act). OESs must notify incidents simultaneously to the national CSIRT, the sector-specific authority or sector CSIRT and the national authority for identification of operators of essential services. FSOs must notify breaches to the National Bank of Belgium (article 25, Belgian NIS Act and 96 PSD2). These notification obligations apply even if there is not enough information for the determination of the notion of a 'significant impact'.

Payment service providers (PSPs) must notify any major operational or security incident to payment service users if the incident may have or has an impact on their financial interests (article 96, PSD2).

TSPs must notify to the BDPA any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay (article 19 eIDAS).

Time frames

30 | What is the timeline for reporting to the authorities?

Controllers must notify personal data breaches to the BDPA 'where feasible, not later than 72 hours after having become aware of it'. Justification is required if this timeline is exceeded.

When a security breach occurs, or when the loss of the integrity of personal data entails a significant impact on the functioning of network and services, public electronic communications networks and ECSPs must notify such breach or loss to the BIPT without delay. If a personal data breach occurs, ECSPs must notify it to the BDPA without delay (article 107/3, BAEC).

OESs and DSPs must notify incidents without delay (article 35, Belgian NIS Act).

PSPs must notify any major operational or security incident without undue delay (articles 53(2) and 96 PSD2). According to the guidelines of the EBA, there must be an initial report of the major incident within four hours of the first detection followed by reports every three business days at the latest. The final report must be made a maximum of two weeks after the situation is back to normal.

NautaDutilh

Camille De Munter
camille.demunter@nautadutilh.com

Chaussée de La Hulpe 120
Brussels 1000
Belgium
Tel: +32 2 566 80 00
www.nautadutilh.com

Notifications by TSPs must be made without undue delay, but in any event within 24 hours after having become aware of the relevant incident (article 19, eIDAS).

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Controllers must notify personal data breaches to the person whose data they process (data subject) if such breach is likely to result in a high risk to the data subject's rights and freedoms. If no contact with individuals is possible, a public communication is required.

Organisations that process personal data on behalf of a controller ('processors' within the GDPR) must communicate personal data breaches to controllers 'without undue delay'. The parties are free to decide how the communication takes place.

ECSPs must notify a personal data breach to individuals when such breach is likely to adversely affect their data or privacy, unless technological protection measures rendered the data unintelligible to anyone not authorised to access it. In addition, in the case of a specific and significant threat of a cybersecurity incident, the ECSP must inform any users that are potentially affected by such an incident.

DSPs providing services to OESs must inform them of any incident with a significant impact on the continuity of those essential services (article 27, Belgian NIS Act). ENISA has published a report to help determine if the incident has a significant impact.

PSPs must notify any major operational or security incident to payment service users if the incident may have or has an impact on their financial interests (article 96, PSD2).

TSPs must notify any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein to their customers if it is likely to adversely affect them, without undue delay. The supervisory authority may also require TSPs to issue a public communication (article 19, eIDAS).

UPDATE AND TRENDS

Key developments of the past year

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The principal challenges are the development of useful, effective and realistic regulations. The government often only consults members of the academic world, which leads to regulations that are difficult to implement from a practical and business point of view. For instance, a recent bill regarding telecommunications data retention appeared to include a requirement for any encryption to include a backdoor, which led to significant pushback from cybersecurity professionals. The same issue arises with the case law from the Belgian Data Protection Authority, in particular with certain decisions about security and deletion of personal data. We expect that the importance of the topic will naturally lead many companies to seek greater interaction with legislators and be more vocal, including about the possibilities, priorities and necessities of investment in cybersecurity.

Some sectors are already the subject of some changes, such as the recent implementation in Belgium of the European Electronic Communications Code. Also, new rules on cybersecurity in connected vehicles will be applicable from July 2022. In addition, the Belgian government has announced its ambition to help Belgium score well with respect to cybersecurity, which may lead to more incentives to improve cyber resilience and capabilities.

* *The author would like to thank Peter Craddock of Keller & Heckman for his contribution to the chapter.*

China

Yunxia (Kate) Yin, Jeffrey Ding and Gil Zhang

Fangda Partners

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The general cybersecurity and data protection regime in China includes the Cybersecurity Law (CSL) and its implementation regulations and measures. There are also various sectoral regulators in China that have been issuing sectoral rules and regulating cybersecurity and data protection issues in their respective sectors.

The Civil Code, which came into force on 1 January 2021 and supersedes the General Principles of the Civil Law, provides for the right to personal data protection. Any organisations and individuals that collect and process personal data must ensure the security of the personal data. Unlawful collection, use, processing or transfer of personal data is prohibited.

Article 253 of the Criminal Law and the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues regarding Legal Application in Criminal Cases Infringing upon the Personal Data of Citizens specify certain activities that may constitute the crime of infringing the right to personal data protection. There are also other provisions in the Criminal Law that criminalise the intrusion of information systems and other cybercrimes.

The Decision on Strengthening the Protection of Online Information (the Decision) was adopted by the Standing Committee of the National People's Congress of China (the NPC) in 2012 and provides certain general principles on the protection of citizens' online information. Any network service providers and other entities that collect and process citizens' online information must comply with the rules provided in the Decision.

The Provisions on the Protection of Personal Data of Telecommunication and Internet Users, published in 2013, provide relevant rules on the protection of users' personal data. These measures apply to telecommunications service operators and internet information service providers in terms of their collection and processing of users' personal data.

The Administrative Measures for the Multi-level Protection of Information Security (the MLPS Measures), published in 2007, provide relevant rules for the Multi-level Protection Scheme (MLPS). These measures are generally referred to as MLPS 1.0. The Ministry of Public Security released the new draft Regulations on Multi-level Protection System for Cybersecurity for public consultation on 27 June 2018, which aim to repeal and replace the existing MLPS Measures. MLPS 2.0 (which comprises various national standards that have been revamped) was released in June 2019.

The Data Security Law (DSL), which was promulgated by the NPC on 10 June 2021 and which came into force on 1 September 2021, provides that any individuals or organisations that engage in data activities in China may be subject to the DSL. Data activities include data collection, retention, processing, use, provision, trade, public disclosure, etc, regardless of whether they are conducted through a network or not.

The Personal Information Protection Law (PIPL), which was passed by the NPC on 20 August 2021 and came into force on 1 November 2021, covers various areas of personal data protection. For example, the PIPL specifically provides various data protection principles, including transparency, fairness, purpose limitation, data minimisation, limited retention, data accuracy and accountability. Many provisions of the PIPL seem to be inspired by the EU General Data Protection Regulation (GDPR). These include hefty fines of up to 5 per cent of the revenue of the preceding year of a company or individual that processes personal data for a serious breach of the PIPL. There are, however, key differences, notably that the PIPL has a strong focus on consent by individuals on how their personal data is processed. The concept of 'legitimate interest' for processing personal data, which is widely used in the EU, is not recognised in the PIPL.

In addition to the above-mentioned laws and regulations, there are also various national standards on cybersecurity and data protection. The Information Security Technology – Personal Data Security Specification provides various recommended rules on personal data protection.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The CSL applies to the construction, operation, maintenance and use of networks in China. Any organisation or individual that uses a network will be a network operator regardless of the sector. More stringent requirements apply to critical information infrastructure (CII), in particular data localisation requirements. CII operators (CIIOs) also fall within the scope of network operators.

Article 31 of the CSL defines CII as information infrastructure in public communication and information services, energy, public transportation, water conservancy, the financial industry, public services, government information systems and other information infrastructure that may materially impact the national interest, public interest or society as a whole if it is compromised, damaged, disrupted or impacted by a data breach or otherwise. Though the CSL does not provide the specific scope of CII nor the approach to identify CII, network operators in these critical industries or sectors may be more likely to be designated as CIIOs.

On 17 August 2021, the long-awaited Regulations on Critical Information Infrastructure Security Protection (CII Regulation) was released and it took effect on 1 September 2021. The definition of CII under the CII Regulation is essentially the same as that under the CSL. For important industries and sectors, the relevant regulators will be charged with the responsibilities of protecting CIIs in their relevant

industries and sectors, which are termed the 'Protection Departments'. Once the Protection Department identifies the CII, it must notify the operators and the Ministry of Public Security (MPS).

There are also various sectoral rules regarding cybersecurity and data protection that apply to network operators in certain industries, such as fintech, financial services, pharmaceutical and medical services, land surveying and autonomous driving.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

China actively participates in the making of international standards and will recognise certain international standards by transposing relevant rules into the national standards according to the Standardisation Law of the PRC. Article 8 of the Standardisation Law provides that the Chinese government will actively facilitate the interoperability of international standards in China. The standards in China (including national, sectoral or provincial standards or standards applicable to certain associations) may adopt some of the terminology of the international standards to ensure correlation between them and China's national standards, and may also adopt the same rules in the international standard with or without modification when transposing them as national standards. For example, the Information Technology–Security Techniques–Information Security Management Systems–Requirements (GB/T 22080-2016) were made by the National Information Security Standardisation Technical Committee with reference to ISO 27001:2013, developed by the International Organization for Standardization.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The CSL requires network operators to designate a specific person to be responsible for its cybersecurity and data protection issues (the cybersecurity responsible person). Failure to do so would render the network operator subject to the administrative penalty imposed by the relevant supervisory authorities according to article 59 of the CSL, including a rectification order, warning or administrative fine in the case of a failure to rectify the incompliance or in the case of a significant impact to cybersecurity as a result of the violation of the law. The cybersecurity responsible person is responsible for assisting the network operator in complying with the CSL and safeguarding data and cybersecurity.

The CSL imposes liability on the 'directly responsible person' or the 'other responsible person' of the network operator for its violation of the CSL in certain circumstances. For example, article 64 of the CSL provides that the directly responsible person or the other responsible person of the network operator may be subject to a fine ranging from 10,000 yuan to 100,000 yuan for the network operator's infringement of an individual's right to personal data protection. However, the CSL is silent on what constitutes the directly responsible person or the other responsible person, which may be determined by prosecutors and courts on a case-by-case basis.

The 'directly responsible person' or the 'other responsible person' may also be penalised under the DSL where the organisation carrying out data processing activities fails to perform the data security protection obligations stipulated in the DSL, and may be fined up to 200,000 yuan.

The CSL and DSL are both silent on the obligations of directors to remain informed about the adequacy of the company's protection of networks and data. However, according to the Company Law, directors have fiduciary duties towards the company, and it is not yet clear whether a company's violation of the CSL will be interpreted as a director's breach of fiduciary duties to direct the company to comply with laws and regulations.

5 How does your jurisdiction define cybersecurity and cybercrime?

Cybersecurity

The CSL defines cybersecurity as meaning 'to maintain the stable and reliable operation of network and to safeguard the integrity, confidentiality and usability of network data, by taking necessary measures to prevent the network from attack, intrusion, interference, damage, unauthorised use and accidents'. Although the CSL does not define data privacy, the relevant articles of the CSL provide that data privacy refers to the protection of the confidentiality, integrity and availability of personal data.

Given that cybersecurity and data privacy intertwine as data is stored on an information system that relies on IT infrastructure and requires protection, the rules on cybersecurity would also apply in the context of data protection. A cybersecurity incident may not always lead to a data breach, such as in the event of a cybersecurity incident that gives rise to the outage of the network or information system, but the data is encrypted to prevent a data breach.

Cybercrime

The Criminal Law criminalises certain offences related to computers and computer networks that are commonly regarded as cybercrimes. Criminal activities include but are not limited to:

- illegally intruding into a computer system;
- illegally accessing or controlling data stored on a computer system;
- providing computer programs or tools to intrude into or illegally control a computer system;
- damaging a computer system;
- failing to fulfil the security management obligations for an information network; and
- illegally using an information network.

The Opinions on Several Issues Concerning the Application of Criminal Law in Cybercrime Cases issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on 4 May 2014 clarified the scope of cybercrimes as:

- endangering the security of computer information systems;
- theft, fraud or extortion carried out through endangering the security of computer information systems;
- posting information online or setting up websites or communication groups that are mainly used for criminal activities that target, organise, abet or assist an unspecified mass of people to commit crimes; and
- other cases in which criminal activities take place online.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The CSL requires network operators to adopt security measures (ie, technical and organisational measures) for cybersecurity and data protection, such as:

- formulate internal security management systems and operation instructions concerning cybersecurity and data protection, and specify the responsibilities of each relevant department;
- determine a cybersecurity responsible person;
- adopt technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;

- monitor and record network operation and cybersecurity events and maintain the cyber-related logs for no less than six months;
- adopt the rules of data classification and take respective measures according to the data categories; and
- back up and encrypt important data.

In the event that there is dissemination of prohibited content online, a massive data breach, loss of evidence for criminal investigation or other serious consequences as a result of a network operator's refusal to take appropriate technical and other necessary measures to protect information security as required by laws and regulations, and to rectify the situation as required by the relevant regulators, the failure may constitute the crime of 'refusal to perform security management obligations for the information network' according to article 286 of the Criminal Law.

The MLPS Measures require that the information system operator or user shall take certain prescriptive measures to ensure the security of the information system according to the grade of information system. The Information Security Technology – Baseline for Classified Protection of Cybersecurity has been implemented since 1 December 2019 to provide further clarity in conjunction with implementing the new Draft MLPS 2.0 Regulations. It provides the following security measures:

- apply access control to the information systems;
- take measures to protect the physical safety of information systems, such as anti-theft, fireproof and anti-invasion measures;
- ensure the security of telecommunications;
- determine the safety parameters and take relevant protection measures accordingly;
- conduct identity authentication for the access of information systems;
- perform data backups;
- set up internal company policies on security management and determine the responsible person or department;
- provide training to the employees concerning cybersecurity and data protection;
- grade the information systems and file the grade of the information system with the local police if graded as Level II or above;
- design a security plan for the information systems;
- ensure the security of the products and services purchased for the information systems; and
- prepare a security incident response plan and protocol.

Sectoral rules may provide more requirements on the protective measures for cybersecurity and data protection that apply to the network operators in certain sectors, such as banking and financial services.

Scope and jurisdiction

7 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The laws and regulations on the promotion of cybersecurity apply to the protection of networks, which applies to any theft of intellectual property if it is stored on an information system or a network, such as the crimes of illegally obtaining data from information systems (article 285 of the Criminal Law) and damaging an information system (article 286 of the Criminal Law).

8 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The CSL provides stricter requirements for the protection of CII.

Article 31 of the CSL defines CII as information infrastructure in public communication and information services, energy, public transportation, water conservancy, the financial industry, public services, government information systems and other information infrastructure that may materially impact the national interest, public interest or society as a whole if it is compromised, damaged, disrupted or impacted by a data breach or otherwise. However, the CSL does not provide the specific scope of CII nor the approach to identify CII.

The CII Regulation provides further rules in this regard. Under the CII Regulation, the relevant regulators will be charged with the responsibilities of protecting CIIs in their relevant industries and sectors, which are termed the 'Protection Departments'. In particular, Protection Departments have the power to make rules for identifying CII and to identify the CII according to such rules. In determining the rules, the Protection Departments will take the following factors into consideration, including:

- the importance of the network infrastructure and information systems to the key or core operation of the relevant industry or sector;
- the level of harm on the network infrastructure and information systems in the event of destruction, loss of function or data leakage; and
- any consequential impact on other industries or sectors.

Once the Protection Department identifies the CII, it must notify the operators and the MPS.

The Cyberspace Administration of China (CAC) released the revised Measures on Cybersecurity Review to implement article 35 of the CSL, which require that any purchase of network products and services by the CIIOs that affects or may affect state security is subject to relevant cybersecurity assessment.

The CAC released the draft Measures for the Administration of Publishing Cyberthreat Information on 20 November 2019. These measures provide stricter requirements on the publication of the regional comprehensive analysis report on cybersecurity attacks, incidents, risks and vulnerabilities that relate to important sectors, such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defence, science and technology. In addition to the prior report to the CAC, reporting to the relevant sectoral regulator would also be required if the Measures are brought into force.

9 | Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

According to article 29 of the CSL, China supports cooperation between network operators in the collection, analysis and reporting of cybersecurity information and the emergency response for the purpose of improving network operators' capabilities for cybersecurity protection. However, as stipulated in article 26 of the CSL, carrying out activities such as cybersecurity authentication, testing and risk assessment and releasing cybersecurity information, such as system bugs, computer viruses, network attacks and intrusions, are subject to relevant rules.

The draft Measures for the Administration of Publishing Cyberthreat Information provide relevant rules, including:

- the published cyberthreat information must not contain seven types of content, including the source code and production methods of computer viruses, Trojan horses, ransomware and other malware;
- the publication of information relating to a cybersecurity incident, such as an attack, damage or illegal access to a network or information system, is subject to prior reporting to the public security organ above the prefecture level of the place where the incident occurred; and

- without the approval or authorisation of a government agency, enterprises, social organisations and individuals must not add the phrase 'early warning' to the title of the published cyberthreat information.

The Regulation on the Management of Network Product Security Vulnerabilities, issued on 12 July 2021, requires that the release of security vulnerabilities information about cyber products to the public through cyber platforms, media, conferences, contests or otherwise, by any organisation or individual that discovers or collects security vulnerabilities of cyber products shall follow the principles of necessity, authenticity, objectivity and being conducive to preventing cybersecurity risks, and comply with the following provisions:

- it is not allowed to release vulnerability information before the cyber product provider provides remedial measures for security vulnerabilities of cyber products; the organisation or individual shall conduct joint assessment and consultation with the relevant cyber product provider if it or he or she deems it necessary to release such information in advance, and shall report the same to the Ministry of Industry and Information Technology and the Ministry of Public Security, which will release such information after organising assessment;
- it is not allowed to release the details of security vulnerabilities in the cyber, information system and equipment used by network operators;
- it is not allowed to deliberately exaggerate the hazards and risks of security vulnerabilities of cyber products, or to carry out malicious speculation, fraud, extortion and other illegal or criminal activities by making use of information of security vulnerabilities of cyber products;
- it is not allowed to release or provide programs or tools specifically used for activities that endanger cybersecurity by taking advantage of security vulnerabilities of cyber products;
- it is required to release repair or preventive measures at the same time as releasing security vulnerabilities of cyber products;
- it is not allowed to release information of security vulnerabilities of cyber products without the approval of the Ministry of Public Security during major events held by the state;
- it is not allowed to provide undisclosed security vulnerabilities of cyber products to any overseas organisation or individual other than cyber product providers; and
- other relevant provisions of laws and regulations (not specified).

The right to freedom and confidentiality of private communications is a constitutional right. Article 40 of the Constitutional Law provides that no organisation or individual may, on any ground, infringe the right to freedom and privacy of citizens' private correspondences. The only limitation to this right is that the police or procurators may search and access private correspondence in accordance with the applicable rules for protecting state security or investigating criminal offences.

The law does not provide specific rules on the collection and processing of metadata. However, if metadata forms part of state secrets, important data or personal data, the collection and processing of it will be subject to the relevant rules applicable to the category of the data.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The Criminal Law criminalises certain offences related to computers and computer networks that are commonly regarded as cybercrimes. Criminal activities include but are not limited to:

- illegally intruding into a computer system;
- illegally accessing or controlling data stored on a computer system;
- providing computer programs or tools to intrude into or illegally control a computer system;
- damaging a computer system;
- failing to fulfil the security management obligations for an information network; and
- illegally using an information network.

The Opinions on Several Issues Concerning the Application of Criminal Law in Cybercrime Cases issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on 4 May 2014 clarified the scope of cybercrimes as:

- endangering the security of computer information systems;
- theft, fraud or extortion carried out through endangering the security of computer information systems;
- posting information online or setting up websites or communication groups that are mainly used for criminal activities that target, organise, abet or assist an unspecified mass of people to commit crimes; and
- other cases in which criminal activities take place online.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The providers of cloud computing services in China must comply with the laws and regulations on cybersecurity and data protection. There are various regulations, measures and national standards that are made specifically for cloud computing, which cover aspects ranging from the procurement of the cloud services, security and management measures for cloud services providers. For example, the Cyberspace Administration of China released the Opinion on Strengthening the Administration of the Cybersecurity of the Cloud Computing Services Used by Departments of the Party and Government on 30 December 2014 and jointly released the Measures for the Security Assessment of Cloud Computing Service on 2 July 2019 together with the National Development and Reform Commission, the Ministry of Industry and Information Technology and the Ministry of Finance. Government agencies and the CIIOs must first assess the risks and assess the providers before using any cloud computing services that have passed the security assessment by the CAC. Use of public cloud computing services is prohibited if the network operator's information system stores any state secrets.

Where a network operator uses cloud computing services to store data, the network operator must also ensure that its cloud services providers comply with the technical and management measures under the MLPS regime so that the network operator can pass the annual testing of MLPS.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The CSL applies to network operators regardless of whether the companies are domestic companies or foreign-invested companies.

The CSL is silent on extraterritorial application and does not have a provision similar to article 3(2) of the GDPR. However, the view of the CAC seems to be that the CSL would have extraterritorial application. The CAC released the draft Measures on Security Assessment on Cross-border Transfer of Personal Data on 13 June 2019, which proposed a new requirement for appointing representatives in China for the remote collection of personal data outside China, similar to article 27 of the GDPR. The representative will assume the obligations of the network

operator under these measures, which includes conducting security assessments on cross-border transfers of personal data.

Article 2 of the DSL provides for extra-territorial application of the DSL in certain circumstances; that is, if overseas organisations or individuals engage in the data processing activities that damage national security, the public interests of China or the legitimate interests of the citizens or organisations of China, such overseas organisations or individuals (or both) may be subject to the DSL.

The PIPL applies to the processing of individuals' personal data that takes place in China regardless of the nationality of such individuals. Unlike the CSL, which provides limited extra-territorial application, the PIPL proposes clear and specific extra-territorial application to overseas entities and individuals that process the personal data of data subjects in China for the purpose of provision of products or services (or both) to data subjects in China; for analysing or assessing the behaviour of data subjects in China; or in other circumstances as provided by China laws and regulations.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes, China has published various national standards and technical guidelines on cybersecurity and data protection, which mainly include GB standards (mandatory national standards that are compulsory for companies to adopt), GB/T standards (recommended national standards that are not compulsory for companies to adopt) and technical guidelines. These national standards and technical guidelines cover various issues related to cybersecurity and data protection. For example, the Information Security Technology – Personal Data Security Specification (PDSS) provides various recommended rules on the protection of cybersecurity and personal data.

14 | How does the government incentivise organisations to improve their cybersecurity?

There is currently no specific monetary reward from the government to incentivise organisations to improve their cybersecurity. Protecting cybersecurity and data is an obligation for each network operator.

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

China has published various national standards and technical guidelines on cybersecurity and data protection, which mainly include GB standards (mandatory national standards that are compulsory for companies to adopt), GB/T standards (recommended national standards that are not compulsory for companies to adopt) and technical guidelines. These national standards and technical guidelines cover various issues related to cybersecurity and data protection. For example, the PDSS provides various recommended rules on the protection of cybersecurity and personal data. In general, the national standards and technical guidelines are made by the National Information Security Standardisation Technical Committee and are often published jointly by the Administration of Quality Supervision, Inspection and Quarantine and the State Administration of Standardisation. Various national standards can be found at www.tc260.org.cn. However, these national standards are published in Chinese and there is no official translation of them.

16 | Are there generally recommended best practices and procedures for responding to breaches?

China has released various rules on responding to data breaches and security incidents. In addition to relevant laws and regulations (eg, the Cybersecurity Law and the National Emergency Response Plan for Security Incidents), there are also recommended rules for responding to data breaches and security incidents. For example, the PDSS provides relevant recommended rules on responding to and managing personal data breaches, in particular on notifying competent supervisory authorities and the affected data subjects.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

China supports cooperation between network operators in the collection, analysis and reporting of cybersecurity information and the response to emergencies for the purpose of improving their capabilities for cybersecurity protection. If the draft Measures for the Administration of Publishing Cyberthreat Information are brought into force in their current form, the publication of cyberthreat information would be subject to prior reporting to relevant regulators, and the publication of cyberthreat information must not contain certain prohibited contents. The National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT), established in 2001, is a national cybersecurity emergency response agency established under the Cyberspace Administration of China. The CNCERT initiated the establishment of the National Vulnerability Database, with information provided by various telecoms operators, cybersecurity companies and internet services providers. The database aims to proactively monitor cyberthreats and incidents, and provide information for network operators to take preventive measures against cybersecurity incidents.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Other than the private sector giving comments on draft measures that are released for public consultation, the most common avenue of cooperation between government and the private sector is during the drafting of national standards on cybersecurity and data protection. Several members of the National Standardisation Committee (such as TC260) will select a national standard and join a working group to initiate research and the drafting of the national standard. As a member of TC260, our experience has been that the private sector's comments and opinions are very much welcome and accepted, and the process of making various national standards is generally very collaborative.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance for cybersecurity breaches in China is available, and it is common practice for companies in China to have it.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Various regulatory authorities enforce cybersecurity rules in China, such as the primary regulators: the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). Other sectoral regulators can also make rules to regulate data protection and cybersecurity issues in their respective sectors, such as the People's Bank of China, the China Securities Regulatory Commission, the China Banking and Insurance Regulatory Commission and the National Health Commission.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Chinese authorities in general have broad powers to monitor compliance, conduct government investigations, request cooperation and information and impose penalties for violating laws according to various administrative laws, such as the Administrative Penalty Law.

For example, according to the Measures for Internet Security Supervision and Inspection issued by the MPS under the authorisation of the Cybersecurity Law (CSL), the MPS may conduct on-site inspection and remote testing against certain types of network operators. During the on-site inspection, the MPS may take certain measures to investigate cybersecurity incidents, such as entering the premises to inspect computer rooms and the workplace; interviewing the cybersecurity responsible person of the network operator; consulting and copying information required for the investigation; and checking the operation of technical measures for network and information security protection.

When the MPS conducts remote testing to determine whether certain system vulnerabilities may exist on the network operator's network, prior notice will be given to the network operator concerned that will include the time of remote testing and the scope of testing. The MPS generally should not interfere with the normal operation of the network of the network operator.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

The provisions under the Criminal Law against the infringement of the right to personal data protection and against cybercrimes have been actively enforced in China. There have been many cases where organisations and individuals that unlawfully collected and processed personal data have been investigated, prosecuted and convicted.

Aside from the active criminal law enforcement, there have been law enforcement actions against the violation of the CSL, such as failure to: monitor and record network operation and cybersecurity incidents and maintain the network logs for no less than six months; take technical measures to prevent computer viruses, network attacks and network intrusion; and adopt online content moderation measures against the prohibited information released by app or website users. The unlawful use of VPNs has also been the subject of law enforcement in China.

As a coordinated law enforcement effort, the CAC, the MIIT, the MPS and the State Administration of Market Regulation (collectively, the Four Ministries) released a joint announcement of their law enforcement agenda on 25 January 2019, which aimed to curb certain privacy practices throughout 2019 and promote a certification scheme for personal data protection. The Four Ministries highlighted in this announcement that app operators must display a privacy notice for the collection and use of personal data in an easy-to-understand, clear and concise manner and allow data subjects to give consent freely instead of coercing consent by way of pre-ticked consent boxes or bundled consent. Many app operators have been inspected and required by the Four Ministries to rectify non-compliance. The Four Ministries have constantly published a list of names of app operators that have not yet complied with the CSL and have even ordered certain apps to be suspended or temporarily removed from app stores.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

The law requires notification of security incidents to the relevant regulators as well as to the affected data subjects, for example:

- article 1038 of the Civil Code requires the processor of personal data to report a data breach to the affected natural persons and the competent supervisory authorities;
- articles 25 and 42 of the CSL require network operators to report security incidents to the competent supervisory authorities as well as to the affected data subjects whose personal data has been breached;
- article 29 of the Data Security Law requires companies that process data to report security incidents to the competent supervisory authorities as well as to the affected data subjects whose personal data has been breached;
- article 57 of the Personal Information Protection Law requires companies to immediately take remedial measures and notify the authorities and the data subjects concerned where personal data has been or may be divulged, tampered with or lost;
- article 14 of the Provisions on the Protection of Personal Data of Telecommunication and Internet Users provides that telecommunications business operators and internet information service providers must report security incidents that will or may have severe consequences to the competent telecommunications administration authorities; and
- the National Emergency Plan for Cybersecurity Incidents defines and categorises security incidents and provides the threshold for reporting to the regulatory authorities as well as the relevant procedural requirements.

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

To prevent cybersecurity breaches, network operators are required to adopt the necessary technical and management measures to safeguard data and for cybersecurity.

Failure to take technical and other measures to ensure cybersecurity and protect the personal data collected, which can lead to a cybersecurity breach, would render the network operator concerned subject to the administrative penalty imposed by the relevant regulators according to the CSL, including a rectification order, a warning, confiscation of illegal gains, a fine, suspension of business or operation of apps or websites, or revocation of the permit or business licence if it is a serious violation.

In the event that the cybersecurity breach and serious consequences occur as a result of the network operator's refusal to adopt appropriate technical and other necessary measures to protect personal data as required by the relevant regulators in a rectification order, the refusal may further constitute the crime of 'refusal to perform security management obligations for the information network', as provided in article 286 of the Criminal Law.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

There are legal ramifications for network operators that fail to report cybersecurity breaches to the relevant regulators and the data subjects whose personal data has been breached. Legal ramifications include rectification orders, warnings, fines, confiscation of illegal gains, suspension of business or operation of apps or websites, and revocation of the permit or business licence if it is a serious violation. These administrative penalties are imposed by the relevant supervisory authorities according to article 64 of the CSL.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Data subjects may bring claims against organisations and individuals that unlawfully collect or process their personal data on the grounds of either tort or breach of contract (ie, a user agreement). Suing in tort is more common as the data subjects can choose either the Civil Code or the Law on the Protection of Rights and Interests of Consumers as the legal basis to bring a claim. There is a provision in the latter that provides private redress for consumers similar to article 111 of the Civil Code.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Cybersecurity Law (CSL) requires network operators to adopt security measures (ie, technical and organisational measures) for cybersecurity and data protection, such as:

- formulate internal security management systems and operation instructions concerning cybersecurity and data protection, and specify the responsibilities of each relevant department;
- determine a cybersecurity responsible person;
- adopt technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitor and record network operation and cybersecurity events and maintain the cyber-related logs for no less than six months;
- adopt the rules of data classification and take respective measures according to the data categories; and
- back up and encrypt important data.

In the event that there is dissemination of prohibited content online, a massive data breach, loss of evidence for criminal investigation or other serious consequences as a result of a network operator's refusal to take appropriate technical and other necessary measures to protect information security as required by laws and regulations, and to rectify the situation as required by the relevant regulators, the failure may constitute the crime of 'refusal to perform security management obligations for the information network' according to article 286 of the Criminal Law.

The Administrative Measures for the Multi-level Protection of Information Security require that the information system operator or user shall take certain prescriptive measures to ensure the security of the information system according to the grade of information system. The Information Security Technology – Baseline for Classified Protection of Cybersecurity has been implemented since 1 December 2019 to provide further clarity in conjunction with implementing the new draft Regulations on Multi-level Protection System for Cybersecurity. It provides the following security measures:

- apply access control to the information systems;
- take measures to protect the physical safety of information systems, such as anti-theft, fireproof and anti-invasion measures;
- ensure the security of telecommunications;
- determine the safety parameters and take relevant protection measures accordingly;
- conduct identity authentication for the access of information systems;
- perform data backups;
- set up internal company policies on security management and determine the responsible person or department;
- provide training to the employees concerning cybersecurity and data protection;
- grade the information systems and file the grade of the information system with the local police if graded as Level II or above;
- design a security plan for the information systems;
- ensure the security of the products and services purchased for the information systems; and
- prepare a security incident response plan and protocol.

Chapter 4 of the Data Security Law (DSL) stipulates various data protection obligations regarding data processing, as well as the principles of social morality and ethics applicable to data processing activity and the development of new technologies. The DSL also reiterates the importance of network protection, implementing the multi-level protection system, training and other technical measures (eg, risk monitoring and contingency measures) and other necessary measures.

The Regulation on the Management of Network Product Security Vulnerabilities issued on 12 July 2021 requires that network product providers shall perform a series of network product security vulnerability management obligations to ensure that their product security vulnerabilities are timely patched and reasonably released, and guide and support product users to take preventive measures. Network operators are also required to take measures immediately after discovering or learning about network security vulnerabilities, and to verify security vulnerabilities and complete repairs in a timely manner.

Sectoral rules may provide more requirements on the protective measures for cybersecurity and data protection that apply to the network operators in certain sectors, such as banking and financial services.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The CSL requires network operators to adopt technical measures to monitor and record network operation status, cybersecurity threat information and security incidents and to keep relevant logs for at least six months. There are other sectoral rules and circulars that require certain network operators in certain sectors to keep the logs for a minimum of one year.

The Information Security Technology – Personal Data Security Specification (PDSS) provides that records of data breach incidents must contain, at a minimum, who discovered the incident as well as when and where the incident was discovered, the categories of personal data affected, the number of affected data subjects, the names of the information systems involved and whether notification was made to the relevant regulators. The PDSS is silent on the retention period of the records of data breach incidents.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There are various laws and measures that require network operators affected by cybersecurity incidents to report the incidents to the relevant regulators, such as the CSL, the Civil Code, the E-commerce Law, the Provisions on the Protection of Personal Data of Telecommunication and Internet Users, and the Security Incidents Emergency Plan, as well as relevant sectoral rules. The thresholds for reporting to different regulators are not the same; however, the reporting obligation under different rules is generally triggered by the occurrence or potential occurrence of a cybersecurity incident. The report must be in Chinese, and it must contain at least the following information: the time of occurrence of the incident; the scope of the impact and damage; remedial measures that have been taken; the details of the personal data and data subjects involved in the breach; and the contact details of the relevant responsible department or person of the network operator.

Time frames

30 | What is the timeline for reporting to the authorities?

Upon the discovery of a cybersecurity incident, the network operator must immediately report the incident to the relevant regulators. Article 20 of the draft Regulations on the Graded Protection of Cybersecurity provides that a report of any online incidents must be made to the local public security organ within 24 hours. There are also sectoral rules that provide specific timelines for reporting the data breach to the authorities; for example, the new version of the Implementation Measures for the Protection of Rights and Interests of Financial Consumers, which was released by the People's Bank of China (PBOC) on 15 September 2020 and came into force on 1 November 2020, requires banking financial institutions and non-banking payment institutions to report a data breach that may damage financial consumers' life or property immediately to the local branch of the PBOC, and to report a data breach that may cause other negative influence on financial consumers within 72 hours to the local branch of the PBOC.

While there is no specific obligation to continue reporting after the initial report to the relevant regulators, in practice, once the regulators step in to investigate the incident, they will request cooperation and information from time to time until the closure of the investigation.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Network operators have specific obligations to notify the data subjects whose personal data has been breached. There is no specific data breach reporting obligation on a network operator to notify others in the same industry or sector as the reporting obligation is limited to the relevant Chinese authorities, should the cybersecurity incident meet the reporting threshold, and to the affected data subjects. The network operator can communicate with the affected data subjects using any of the following means: email, letter, telephone, in-app push notification and other proper means or announcement on the company website (if it is impractical to notify each of the affected data subjects).

FANGDA PARTNERS
方達律師事務所

Yunxia (Kate) Yin
kate.yin@fangdalaw.com

Jeffrey Ding
jding@fangdalaw.com

Gil Zhang
gil.zhang@fangdalaw.com

27/F, North Tower
Beijing Kerry Centre
1 Guanghua Road
Chaoyang District
Beijing 100020
China
Tel: +86 10 5769 5600

24/F, HKRI Centre Two
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041
China
Tel: +86 21 2208 1166

17/F, Tower One
Kerry Plaza
1 Zhong Xin Si Road
Futian District
Shenzhen 518048
China
Tel: +86 755 8159 3999

26/F
One Exchange Square
8 Connaught Place
Central
Hong Kong
Tel: +852 3976 8888

17/F, International
Finance Place
8 Huaxia Road
Zhujiang New Town
Guangzhou 510623
China
Tel: +86 20 3225 3888

www.fangdalaw.com

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Although the Cybersecurity Law (CSL) is the primary law that provides rules on cybersecurity and data protection, its provisions are mostly high-level principles, and it is still very much dependent on the implementation measures and regulations for consistent law enforcement. As the CSL authorises several ministries (as opposed to one specific ministry) to make rules under the CSL and enforce the laws, the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security have been actively creating ministry-level measures since the passage of the CSL.

The Data Security Law (DSL) and the Personal Information Protection Law (PIPL), effective in 2021, together with the CSL, form the legal framework for cybersecurity in China. To supplement the CSL, the DSL introduces various new principles and rules regarding

data processing and data protection. For example, the DSL stipulates various requirements for the processing of important data, including that important data processors must designate a specific individual or department in charge of data security and periodically file with the relevant authorities a risk assessment report regarding the processing of important data. The DSL also provides that data related to restricted items that are subject to export control restrictions under Chinese law is also subject to export control, and without pre-approval by supervisory authorities of the Chinese government no organisation or individual in China may provide data stored on the territory of China to foreign authorities or judicial bodies. The DSL lays a good foundation for many rules to come. To strengthen the protection of personal data, the PIPL requires personal data handlers to take a series of protection measures that also touch on cybersecurity topics such as data encryption and categorisation.

The principal challenge to compliance with data protection laws in China in 2022 is that companies have to meet various regulators' expectations. Not only do the regulations and measures promulgated by different regulators require careful reconciliation by companies, but companies also need to consider certain recommended national standards that provide guidance. Companies may start taking a holistic approach to harmonise these rules and build a comprehensive data protection programme to ensure continuous compliance with the CSL and implementation regulations and measures. Based on many law enforcement actions, it is easier to convince regulators that a company has taken sufficient measures for cybersecurity and data protection if they are shown evidence of compliance and a comprehensive data protection programme.

Some important draft measures that are the key pillars of the cybersecurity and data security regime were released for public consultation in 2021, such as the draft Security Assessment Measures on Cross-border Data Transfer, which requires data handlers to complete a security assessment at the local cyberspace administration under certain circumstances before their cross-border transfer of personal data or 'important data' that is collected and generated in China, and the draft Regulations on Cyber Data Security Management which sets out more specific protection requirements and obligations on cyber data handlers on the basis of the PIPL and DSL. It is expected that these important draft measures may be finalised in 2022, and there is no doubt that active law enforcement agencies will follow the new measures. Law enforcement will continue to be strong and active, and there may be more coordinated efforts in addressing data protection practices in further sectors in 2022.

European Union

Thomas Kahl, Detlef Klett and Paul Voigt

Taylor Wessing

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In the past, the European Union has placed great focus on enacting uniform regulations for sufficient cybersecurity. There are laws that deal directly with the topic of cybersecurity and laws that contain indirect regulations. The most important regulations include the following:

- ePrivacy Directive (last revised in 2009);
- NIS Directive (2016);
- Cybersecurity Act (2019);
- Cyberattack Regulation (2019); and
- Directive on attacks against information systems (2013).

The directives do not apply directly in all member states but require transformation into national law. All member states must comply with this transformation obligation. Regulations, on the other hand, apply directly in all member states without the need for transformation. Work is currently under way on an ePrivacy Regulation.

The NIS Directive was a major step for the European Union to improve cybersecurity across the board. In particular, cooperation between member states was strengthened through joint working groups. In addition, focus was placed on ensuring that companies in specific essential sectors implemented improved protection against cyberattacks.

The Cyber Security Act has strengthened the position of the European Union Agency for Cybersecurity (ENISA) and set the course for a Europe-wide certification procedure to be developed to simplify the certification of IT products and services, and to have a uniform assessment concept for respective IT security certifications.

In addition to the regulations that deal directly with cybersecurity, there are also those that deal with the issue indirectly alongside other regulations. This includes the General Data Protection Regulation (GDPR). At various points, it contains specifications on security measures to be taken by companies when processing personal data.

In December 2020, the European Commission published a draft for a new cybersecurity directive that will revise the NIS Directive. The aim of the Directive on measures for a high common level of cybersecurity across the Union is to further adapt and increase the level of protection in the different member states. This is to close up possible gaps that the NIS Directive did not achieve or that arose because member countries implemented the Directive to varying degrees. This includes closer cooperation between member states through the creation of a working group and the obligation to develop a national cybersecurity strategy.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The NIS Directive addresses member states and requires them to identify and oblige operators of essential services in their country to implement an adequate level of security. These critical infrastructures are mostly found in the following sectors:

- energy;
- transport;
- banking;
- financial market infrastructures;
- healthcare;
- drinking water supply and distribution; and
- digital infrastructure.

In addition to essential services, the NIS Directive also requires digital service providers to ensure sufficient cybersecurity. This applies in particular to digital service providers that use an online marketplace, an online search engine or cloud computing services within the European Union to provide their services.

As all member states had to fulfil their obligation to transpose the NIS Directive into national law, companies from the aforementioned sectors are those most affected by cybersecurity legislation. Many of these companies have implemented a corresponding security strategy or are still working on it. Not least because of the looming consequences of not complying with the national requirements, cybersecurity is more pronounced in these sectors than elsewhere.

Even beyond critical infrastructures and digital service providers, small and medium-sized enterprises may be required to take appropriate cybersecurity measures. Although there is no explicit regulation or directive that prescribes that protective measures must be taken, such an obligation often arises from other laws that only marginally deal with cybersecurity (eg, the GDPR). According to the GDPR, anyone who processes personal data must take appropriate technical and organisational measures to protect that data. This affects all companies working with personal data, regardless of their size.

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

The European Union has taken on many international standards. This is not least due to the fact that member states and expert groups of the European Union have actively participated in the drafting of many International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards. Over time, many ISO standards have been implemented, even if they are not binding at EU level. ENISA's Risk Management and Risk Assessment guidelines refer to the ISO standards and see them as a helpful support to ensure standardisation of appropriate security standards on a supranational level.

The most prominent example is ISO 27001:2013, which specifies the requirements for establishing, implementing, maintaining and continuously improving an information security management system. ISO 27002 to 27007 complement it by serving as guides for dealing with ISO 27001.

The standards are not always of a general nature and are often aimed at specific industries. Among others, the automotive industry (ISO/SAE/DIS 21434) is affected by such regulations. In addition, there are also special requirements for industrial automation (IEC 62443).

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

At an EU level, there are no laws that establish the direct responsibility of competent persons and directors with regard to cybersecurity compliance. The obligation of the responsible personnel and directors to take sufficient measures to ensure the security of the company is a consequence of company law, which the member states regulate themselves. Ensuring the safety of the company includes paying attention to business-critical areas and taking appropriate measures. Cybersecurity is also a business-critical area. Thus, at the national level, the directors or other responsible persons may be liable for inadequate cybersecurity.

5 How does your jurisdiction define cybersecurity and cybercrime?

ENISA's Definition of Cybersecurity – Gaps and overlaps in standardisation states:

> *Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.*
>
> *...*
>
> *Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack).*

ENISA refers to the protection of networks, computer systems, cyber-physical systems and robots against theft or damage to their hardware and software or the data they process, as well as against disruption or misuse of the services and functions offered.

Data privacy is intended to safeguard the individual's right to protection of his or her personal data. To uphold this right, companies processing personal data must establish, among other things, sufficient cybersecurity.

According to the European Commission, cybercrime consists of 'criminal acts that are committed online by using electronic communications networks and information systems'. The European legislator has enacted the Cyberattack Regulation, which is directly applicable in all EU member states. The Cyber Attack Regulation deals with the protection of the European Union and its member states against external cyberattacks. The European legislator has also issued directives that member states must transpose into national law. These include the Directive on attacks against information systems, which calls for stronger criminal laws to prosecute cyberattacks against information systems. At the national level, there are a variety of regulations that address cybercrime.

There are two different approaches behind the prosecution of cybercrime and the implementation of appropriate cybersecurity measures. It is up to the companies themselves to establish an adequate security structure. An adequate security structure should act preventively against cybercrime in the form of hacking attacks or similar. However, if an attack does occur, it is up to the member state to prosecute it. If the attack was only successful because no measures were taken on the part of the company, this can be punished with a fine under certain circumstances. In this case, however, the company itself is not committing cybercrime.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

There is no simple answer applicable to all circumstances. The European legislator has not issued a catalogue of minimum standards. In the event that there are relevant legal regulations, such as article 32 of the GDPR, the legislator regularly uses undefined legal terms. In addition, the measures to be taken depend on the type of data being processed. The more sensitive the data, the higher the protection must be. It is, therefore, not possible to name specific measures.

A helpful tool for the operators of critical infrastructures, according to the NIS Directive, is the tabular summary of all important standards, including the ISO standards, that are relevant for the individual subject areas. ENISA released Minimum Security Measures for Operators of Essentials Services, which summarised these and presented them clearly. However, the table demonstrates why a summary of the minimum standards at the legislative level is almost impossible: even the compact summary runs to several pages.

For affected companies, a well-thought-out cybersecurity strategy is, therefore, all the more important. To this end, they can use the ISO standards or recommendations from government agencies as a guide.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no EU legislation that explicitly addresses the threat of cyberattacks on intellectual property. However, in November 2020, the European Commission adopted a new Action Plan on Intellectual Property. This plan includes, among other things, the targeted raising of awareness of companies to the dangers posed to intellectual property by cyberattacks. In addition, companies are to be trained on how to deal with the economic impact of a possible attack on their intellectual property.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The NIS Directive gives member states the task of identifying the operators of essential services in their country. In doing so, sectors are identified from which essential services arise. In this case, essential services are services that are essential for the maintenance of critical societal and economic activities, the provision of that service depends on network and information systems and an incident would have significant disruptive effects on the provision of that service (article 5(2), NIS Directive).

The sectors defined by the NIS Directive are:

- energy;
- transport;
- banking;
- financial market infrastructures;

- healthcare;
- drinking water supply and distribution; and
- digital infrastructure.

However, it is up to each member state to identify the critical infrastructures and describe them in more detail in their national laws. All member states have fulfilled this obligation.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There is no law that explicitly prohibits the disclosure of information about a cyberthreat. However, the disclosure of such information may violate other laws. A violation of the GDPR is conceivable if personal data is disclosed or a violation of the right to confidentiality of communications if the communication took place in private (article 5, ePrivacy Directive; article 8, European Convention on Human Rights (ECHR); and article 7, EU Charter of Fundamental Rights).

According to article 6 of the GDPR, the processing of personal data is generally unlawful unless it is exceptionally justified. In the case of a disclosure of cyberthreat information, which also contains personal data, the processing can potentially be justified according to article 6(1)(f) of the GDPR. Justification depends on a balancing of interests. The severity of the attack and the potential damage must be taken into account. In addition, it must be considered to whom the attack is to be reported, whether a specific state agency or the entire private sector. If the interests of the data subject do not prevail, the disclosure of information regarding a cyberthreat may be justified under the GDPR.

Particular attention should be paid to the fact that disclosure of private communications may violate the confidentiality of communications under article 5 of the ePrivacy Directive, which indirectly incorporates the rights under article 8 of the ECHR and article 7 of the EU Charter of Fundamental Rights. The Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure provides an indication of the weighting of the threat to trade secrets. Nevertheless, whether private communications may also be released to provide information regarding cyberthreats depends on the individual case.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

In recent years, the fight against cybercrime has increasingly become the focus of the European legislator. In addition to two directives dealing with the handling of cybercrime, the European legislator has also enacted the Cyberattack Regulation, which is directly applicable in all EU member states. This Regulation deals with the protection of the European Union and its member states against external cyberattacks. 'External' in this case means that the attack is perpetrated from outside the European Union. The Cyberattack Regulation applies to cyberattacks that have a significant or potentially significant impact. The significance of the impact is to be determined by comprehensive balancing. If a critical infrastructure is affected by a cyberattack, it can be assumed that the impact is significant.

In addition to the Cyberattack Regulation, there are two directives that have been transposed into the national laws of various member states. According to the 2013 Directive on attacks against information systems, member states must ensure that, for example, unlawful interference with data or the unlawful interception of data is punishable. In 2019 the Directive on combating fraud and counterfeiting in connection with non-cash means of payment was adopted. This intends to prevent fraud in non-cash payments as well as fraud in connection with information systems and to prosecute this fraud more efficiently.

Furthermore, the European Commission plans to propose new legislation to improve the safety of children online. In April 2021 the Council and the European Parliament reached a provisional agreement on temporary rules to allow providers of electronic communications to continue to detect, remove and report child sexual abuse online until permanent legislation is in place.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

An increasing number of companies are not buying IT equipment themselves but are opting to use cloud service providers. However, the use of cloud services may pose security concerns. For this reason, the European legislator also saw the need to establish a new set of regulations to make cloud computing easier and more secure. Through the Cybersecurity Act, which entered into force in 2019, ENISA was commissioned to develop a certification system for cloud providers. This should ensure more transparency in the market and raise the overall security standard.

In addition, various groups are working on issuing rulebooks with guidance on compliance issues for companies. The European Commission is currently working with other expert groups to set standards for cloud computing. Overall, the focus is on making it easier for businesses to move to cloud solutions without sacrificing security.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The relevant laws at EU level may also apply to foreign companies. The GDPR applies to all companies that process the personal data of EU citizens if the processing is in connection with the offering of goods or services, or monitoring the behaviour of data subjects in the European Union.

EU directives, such as the ePrivacy Directive, the NIS Directive and the Directive on attacks against information systems, can have extraterritorial effect if they explicitly provide for this. The ePrivacy Directive, for example, does not contain any information in this regard. However, the NIS Directive provides for rules to be implemented with regard to digital service providers that are not based in the European Union but offer their services in the European Union. These include, among other things, that they must appoint a representative in the European Union. The directives have been transformed into national law. For the most part, national regulations do not deviate from this.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Within the European Union, such recommendations are largely rooted in national law and based on national considerations. Therefore, the stance on the protections recommended varies depending on the member state one is situated in. However, the European Union Agency for Cybersecurity (ENISA) has analysed national recommendations for small and medium-sized enterprises and collated general recommendations in its Review of Cyber Hygiene practices. These include:

- having records of all hardware and software;
- utilising secure configuration for all devices;
- managing data flows in and out of the network;

- scanning all incoming emails;
- minimising administrative controls;
- regularly backing up data and testing that it can be restored;
- establishing an incident response plan;
- enforcing similar levels of security across the supply chain; and
- ensuring suitable security controls in any service agreements.

Further, the NIS Directive established a network of computer security incident response teams (CSIRTs) across Europe. Companies and individuals can use the network to receive detailed local advice on best practice and how to best respond to cyberattacks.

14 | How does the government incentivise organisations to improve their cybersecurity?

In this area, the European Union has left the process largely up to member states. Within the European Union, tax breaks and VAT exemptions to incentivise the improvement of cybersecurity (as outlined in ENISA's National Cyber Security Strategy Good Practice Guide 2016) are only used by three member states and generally have been linked with a low level of cybersecurity. The mechanisms used by the majority of states are public-private partnerships (PPPs). PPPs involve private companies in the legislation and implementation process of cybersecurity laws, incentivising the improvement of cybersecurity on an industry level and generating greater awareness of the threats. ENISA has found that approaching private actors at an early stage of the implementation of any cybersecurity law leads to a stronger commitment to the results, as the companies can voice concerns in advance and can be directly involved in the solutions.

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

Within the European Union, industry standards and codes of practices exist mostly on a decentralised level, created by private actors. Among these, there is ISO 27001, a specification for information security management systems. It sets out conditions on the general organisation of processes relevant to cybersecurity regardless of the business area or industry. While the European Union does not provide codes of practice per se, it does offer a certification process on a centralised level. Under the Cybersecurity Act, companies involved in information and communications technology (ICT) can have their products certified to prove their security. Manufacturers of ICT products, providers of ICT services or processes and regulatory authorities wishing to ensure the security of ICT products within their regulations can all request certification. The goal of certification is to showcase the level of protection afforded by their products. With this initiative, the European Union hopes to improve the internal market conditions for ICT products in general.

16 | Are there generally recommended best practices and procedures for responding to breaches?

Under EU law there are robust notification obligations in place for certain security breaches. All companies must report any breach of personal data to the relevant data protection supervisory authority unless it is unlikely to result in a risk to the rights and freedoms of the affected individuals (article 33(1), General Data Protection Regulation (GDPR)). A company must additionally inform the individuals affected if the data breach is likely to pose a high risk of adversely affecting their rights and freedoms (article 34(1), GDPR). The NIS Directive and its transposition into national law impose further notification obligations on operators of essential services and digital service providers (articles 14(3) and 16(3), NIS Directive) that need to report an incident to the relevant supervisory authorities or the CSIRTs if it has a substantial impact on the provision of a service. The provision applies irrespective of whether personal data is affected by the breach.

However, notification alone is not an adequate measure when responding to a breach. Companies, particularly when dealing with hacking attacks, should also consider taking the following actions:

- determine leadership for the incident and involve the data protection officer, if appointed;
- involve IT-forensic professionals to investigate the attack and identify the targeted software and hardware, describe how systems were accessed, determine the categories of data affected and document the analysis;
- check whether personal data was affected by the attack and the level of risk to be expected for those whose data was breached;
- identify possible measures to alleviate the issue;
- contact the data protection supervisory authorities within 72 hours of awareness of the breach, if necessary;
- make data subjects aware of the breach if there is a high risk their freedoms and rights will be impacted;
- let others who may have been affected know of the breach on a voluntary basis (eg, contract partners and banks to ensure money flows are not redirected), if necessary;
- consider any cross-border implications and duties arising in other jurisdictions or on a national level;
- contact the insurance provider if the plan covers cyberattacks; and
- create a framework for dealing with similar issues in the future and implement systems to recognise them at earlier stages.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Information about cyberthreats is primarily collated through mandatory reporting under EU law and member states' laws as well as the predictions of experts, which is why there are limited legal or policy incentives for voluntary sharing of information. ENISA creates frequent reports on the threats in the cyber landscape using this information. Nevertheless, there are various platforms at EU level to facilitate further voluntary information-sharing within certain sectors or on specialised topics. In the finance and banking sector, for example, the European Financial Institutes – Information Sharing and Analysis Centre was founded to exchange information on cyber incidents. Another good example is the European Advanced Cyber Defence Centre. Its goal is to foster extensive sharing of information about cyberthreats across member states to improve detection.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The main way to ensure cooperation between the government and the private sector is through public-private partnerships (PPPs), as they provide a basis for cooperation and ensure open communication, particularly when drafting and implementing legislation. For the private sector, this form of cooperation gives companies the opportunity to influence national legislation as well as to help achieve resilience in the cyber ecosystem of the relevant country. The government also benefits, as the private sector is more likely to implement more robust cybersecurity measures and have a stronger commitment to the rules. Within the European Union, more than 15 member states have PPPs set up. They are particularly prevalent in the larger countries.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance for cybersecurity is available across the European Union. Core coverage for this type of insurance includes data breaches and leakages, business interruption and cyber extortion. Additionally, it also generally covers third-party risks such as privacy liability and electronic media liability. The market for cyber insurance in the European Union has grown significantly in recent years, with a majority of businesses purchasing cyber liability insurance. Increasingly, it is becoming the standard.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In the area of cybersecurity, authorities at EU level do not, typically, have the power to directly enforce cybersecurity requirements in the member states. The competencies are usually limited to supporting and coordinating tasks (eg, the European Union Agency for Cybersecurity has this role according to the Cybersecurity Act).

Competencies for monitoring and enforcement of legal requirements for cybersecurity are instead located at the level of the member states. According to the NIS Directive, national authorities, such as the German Federal Office for Information Security, are monitoring compliance with cybersecurity requirements in the public sector (such as government agencies) for organisations classified as essential services operators and for providers of certain digital services.

Monitoring compliance with cybersecurity requirements is, typically, further split into sector-related competencies – for example, in the telecommunications, energy, financial institutions and insurance, or healthcare sectors. In addition, at the national level, data protection supervisory authorities monitor the enforcement of data protection law requirements, which includes data security requirements (see article 32, General Data Protection Regulation (GDPR)).

The prosecution of cyber-related crimes is subject to national laws and is the responsibility of the competent law enforcement agencies, which are generally the police and the public prosecutors' offices.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Several authorities of EU member states have comprehensive powers in the area of monitoring and investigating breaches of cybersecurity requirements for public bodies and regulated organisations (including essential infrastructure and digital service providers).

The monitoring takes place either by proactive reporting and verification obligations or by the competent authority further investigating and being able to demand inspections and the elimination of identified deficiencies (see articles 14 to 17, NIS Directive).

Sector-specific competencies – for example, in the telecommunications, energy, financial institutions and insurance, and healthcare telematics sectors – are partially designed in a similar manner.

In addition, national data protection supervisory authorities have wide-ranging powers to monitor compliance with data protection requirements, including investigative and remedial powers, and the ability to issue warnings, order the elimination of deficiencies, and restrict or prohibit individual procedures and processing activities (see article 58, GDPR).

In the context of the prosecution of cyber-related crime, law enforcement authorities are usually entitled to the general powers of investigation under criminal procedure provided for by national laws. For example, this could include investigative powers concerning the interception of communications and the power to collect traffic data and search and seize IT equipment.

In addition, the Council of the European Union is empowered to impose targeted restrictive measures to prevent and respond to cyberattacks that pose an external threat to the European Union or its member states (including imposing sanctions on individuals or entities or freezing assets).

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

Data protection supervisory authorities regularly conduct audits on selected topics, including compliance with legal requirements for IT security in their respective areas of responsibility (most recently, for example, on IT security measures against ransomware). Authorities may use the results of the surveys to request companies to improve their security measures and, in individual cases, to impose sanctions for past failures.

In particular, owing to the comprehensive reporting requirements and tight deadlines, many companies have implemented special processes for cyber incident response management to manage corresponding incidents quickly and effectively, and minimise any resulting (liability) risks.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

In the event of a cybersecurity incident, the most relevant notification obligations can be found in national laws implementing the NIS Directive. Operators of essential services and digital service providers must report incidents to the competent national authorities without delay, particularly for disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems (see articles 14 and 16, NIS Directive). Member state laws may provide for an even broader scope and may include companies that are, for example, of great economic importance or other relevant public interest (for example, defence manufacturers).

Similar obligations exist on a national level for other sectors – for example, for healthcare telematics service providers, as well as in the telecommunications and energy sectors.

In the event of a personal data breach in the context of a cybersecurity incident, the responsible entity must report the incident to the competent national data protection supervisory authority without undue delay. If possible, the report should be made within 72 hours of becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (see article 33, GDPR).

If the personal data breach is likely to result in a high risk to the personal rights and freedoms of natural persons, the controller must inform the data subjects of the breach without undue delay (see article 34, GDPR).

Obligations to inform users or other third parties of cybersecurity incidents may also arise from other, mostly sector-specific, laws (eg, national laws implementing Directive 2009/136/EC, amending, among others, Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services).

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Several authorities on a national level have the power to award penalties for breaching the requirements to prevent cybersecurity breaches. Penalties can vary widely between sector-specific legislation and can range from €50,000 to €3 million (or more), depending on sectoral and member state law.

Insofar as the requirements of the GDPR stipulating the implementation of technical and organisational measures are violated, the competent supervisory authorities may punish corresponding violations with fines of up to €10 million or 2 per cent of the global annual revenue of the corporate group achieved in the previous fiscal year.

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Several member state authorities have the power to award penalties for breaching the requirements on reporting threats and breaches.

Penalties can vary widely between sector-specific legislation and can range from €50,000 to €3 million (or more) depending on sectoral and member state law.

Violations of the notification and information obligations can be sanctioned with a fine of up to €10 million or, in the case of a company, up to 2 per cent of its total annual worldwide turnover in the previous fiscal year (articles 33, 34 and 83(4)(a), GDPR).

26 | How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Individuals may take action against responsible companies for inadequate measures in the area of cybersecurity.

The main rights result from the GDPR. Most prominently, the GDPR expressly provides for claims for damages (including non-material damages) that the data subject can assert against the controller or processor in the event of a breach of data protection law (article 82(1), GDPR). Furthermore, data subjects have the right to lodge a complaint with an authority.

In addition, it may also be possible for data subjects to assert corresponding claims based on national laws (eg, civil law) and contractual agreements.

In the event of criminal acts in the area of cybersecurity, those who are affected have the option of filing a criminal complaint with the responsible law enforcement agency, which may initiate further measures.

THREAT DETECTION AND REPORTING

Policies and procedures

27 | What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Although EU legislation does not explicitly provide for it, the General Data Protection Regulation (GDPR) and other sector-specific requirements may require organisations to implement an information security management system. How such a system should be designed is not specified by law but is typically aligned with recognised industry standards such as ISO 27001.

The core of such a framework typically consists of:

- the documentation of the relevant processing activities;
- a corresponding risk assessment;
- the definition of measures to be taken derived from it; and
- the documentation of the implementation together with the associated processes (including plans, guidelines and other documentation for the purpose of preparing for and handling cyber incidents).

Organisational measures to prevent cyberattacks typically include, for example, proper audit mechanisms, sufficient training of employees and the performance of test runs and simulations.

For the implementation of actual technical measures to protect against cyberthreats, companies can take their cue from a variety of laws, for example, the NIS Directive and its national implementations or article 32 of the GDPR (mostly referring to 'state of the art' measures to be implemented) and further specifications or standards (ISO 27001).

According to the European Union Agency for Cyber Security (ENISA) Review of Cyber Hygiene Practices, typical measures that would be deemed necessary under applicable laws and standards include:

- application of industry-standard encryption technology;
- regular monitoring and logging of system access, including proper access rights management and minimising administrative controls;
- application of industry-standard malware protection, including scanning all incoming emails; and
- the overall secure management of data flows in and out of networks, using secure configuration for all devices, and regularly backing up data and testing that it can be restored.

A helpful tool for the operators of critical infrastructures, according to the NIS Directive, is the ENISA Minimum Security Measures for Operators of Essential Services, which is a tabular summary of all important standards, including the ISO standards, that are relevant for the individual subject areas.

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Pursuant to article 33 of the GDPR, in the event of a breach of security when processing personal data, the controller must document the breach and the remedying measures taken. There are no specific requirements as to the form of storage.

In the telecommunications sector, operators must maintain a record of incidents that complies with certain requirements provided by national member state laws implementing Directive 2009/136/EC (including a predefined storage period of five years).

With the exception of the above, EU and EU member state law does not typically provide for a specific length of time for which corresponding data must be stored. In practice, storage periods, among other things, will be based on applicable limitation periods, whether for claims by data subjects, third parties or demands by authorities (including sanctions).

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

In the event of a cybersecurity incident, the most relevant notification obligations can be found in national laws implementing the NIS Directive. Operators of critical infrastructures and digital service providers must report incidents to the competent regulator without delay, particularly if there are disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or services. Depending on the national law the group of companies that fall within the scope of these obligations might be even broader (eg, companies of great economical importance or of special public interest).

Similar obligations may exist on a member state level – for example, for healthcare service providers as well as in the telecommunications and energy sectors.

In the event of a personal data breach in the context of a cybersecurity incident, the responsible entity must report the incident to the competent data protection supervisory authority without undue delay. If possible, the report should be made within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (see article 33, GDPR). Information obligations may result from other laws as well (eg, member state laws implementing Directive 2009/136/EC in the telecommunications sector).

Time frames

30 | What is the timeline for reporting to the authorities?

As a general rule, where notification obligations exist, organisations must report cybersecurity incidents to the competent authorities or concerned individuals without undue delay. Reporting on a continual or routine basis may apply in exceptional cases and is typically subject to sector-specific regulations. In the event of a breach of security of personal data pursuant to article 33 of the GDPR, the controller must report the breaches to the competent supervisory authority without undue delay, but generally within 72 hours of becoming aware of the breach.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are certain obligations to report corresponding incidents to third parties.

Data subjects may have to be informed about a cyber incident according to article 34 of the GDPR or other sector-specific national laws (eg, in the telecommunications sector). Insofar as the information of data subjects, pursuant to article 34 of the GDPR, would generate a disproportionate effort, the law expressly provides for the possibility of a public announcement or similarly effective measure.

In the telecommunications sector, regulated operators may also have to notify users where disturbances originate from their systems in accordance with the national laws implementing Directive 2009/136/EC.

Under article 28 of the GDPR, the processor must inform the controller in the event of a data protection incident (article 33, GDPR).

The obligation to inform third parties may also result from a contractual agreement and related obligations.

The relevant laws do not usually provide for a specific format or means of notification other than that it needs to be properly documented (which can typically also occur in electronic format).

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The challenges to cybersecurity regulations are multifaceted (see the European Union Agency for Cyber Security's reports ENISA Threat Landscape – Emerging trends and ENISA Threat Landscape 2021). The speed at which the digital world changes poses a large burden on regulations. The law in this area needs to adapt quickly as new technologies are constantly emerging that bring about new challenges. Adversarial AI detection is a great example of this. Adversaries are increasingly using AI to launch attacks and avoid detection of their botnets, which cannot be warded off effectively by current cybersecurity measures. Another great example is the internet of things, which is creating different cyberthreats altogether.

A barrier to effective cybersecurity regulation is the lack of meaningful evaluation and accountability. The lack of consistent statistics around cybersecurity coupled with the broad formulation of the regulation objectives makes it difficult to show a causal relationship between legislation and any practical changes. Therefore, it is hard to assess the effectiveness of the regulations and create future drafts on that basis.

In the coming years, cybersecurity laws will likely change in two major ways. First, the NIS Directive will be replaced and further developed by the NIS 2.0 Directive in the near future. The European Commission adopted its proposal in December 2020. In October 2021, the ITRE Committee adopted a proposal that will probably become the position of the European Parliament in the upcoming trilogue negotiations. On the basis of these current proposals, it is very likely that the sectoral scope of the Directive will be extended to include sectors such as essential facilities in sewage, public administration, space and – according to the ITRB proposal – education and research. Furthermore, to reduce administrative burdens and make EU law more efficient, the NIS 2.0 Directive will most likely establish, among other things, a regime for significant fines as well as expanded cooperation between member states' authorities. Overall, the NIS 2.0 Directive will make a significant impact in countering the increasingly fast advance of digitalisation as well as the partly inadequate implementation of the NIS Directive by some member states so far. Secondly, there has been a trend of member states becoming increasingly more active in the area of cybersecurity. As a result, what may occur is that companies operating across the European Union will be subject to divergent cybersecurity rules depending on the jurisdiction, which may pose problems because of the interconnected nature of the internet.

TaylorWessing

Thomas Kahl
t.kahl@taylorwessing.com

Detlef Klett
d.klett@taylorwessing.com

Paul Voigt
p.voigt@taylorwessing.com

Benrather Str 15
40213 Düsseldorf
Germany
Tel: +49 211 8387 0
www.taylorwessing.com

France

Claire Bernier
ADSTO

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Article L111-1 of the Code of Homeland Security provides that the state shall maintain security, which extends to cyberspace. It is in this regard that France has enacted not one specific law but several acts and regulations promoting cybersecurity. They are as follows.

- The Military Programming Act No. 2013-1168 of 18 December 2013 for 2014 to 2019. Pursuant to this act, the state has a duty and responsibility to take appropriate measures to protect essential sectors that are deemed 'of utmost importance for state survival', such as banks, hospitals and nuclear power plants.
- Decrees Nos. 2015-350 and 2015-351 of 27 March 2015, which enact the Military Programming Act of 2013. These decrees state that essential sectors that are deemed 'of utmost importance for state survival' are bound to:
    - adopt detection tools in their networks and information technology (IT) infrastructures so as to prevent any cyberattack;
    - notify immediately any cybersecurity breach to the relevant authorities;
    - regularly audit their IT infrastructures; and
    - adopt specific measures requested by relevant authorities. The law further provides that non-compliance may lead to a fine of up to €150,000.
- The Military Programming Act No. 2018-607 of 13 July 2018 for 2019 to 2024. The purpose of this act is to reinforce the national security level. A whole chapter is dedicated to cyber defence.
- Decree No. 2018-1136 of 13 December 2018, which enacts the Military Programming Act of 2018. This decree reinforces the collaboration between the authorities, electronic communications operators and web hosts to prevent any threat to the security of information systems. The decree provides measures regarding the implementation of detection tools in networks and information technology infrastructures.
- The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is a governmental agency operating under the authority of the General Secretary for Defence and National Security to ensure correct application of the law and, more precisely, the security of the network and information systems. Its prerogatives have been extended by the Military Programming Act of 2018.
- Even before the EU General Data Protection Regulation (GDPR) entered into force, the Data Protection Act of 1978 (modified by Ordinance No. 2018-1125 of 12 December 2018) took into consideration cybersecurity, ensuring that when dealing with personal data, technical and organisational measures shall be implemented by data controllers and processors, either private or public, to ensure a level of security appropriate to the risk when processing personal data. These include protection from unauthorised access, alteration or theft. Additionally, internet service providers (ISPs) processing personal data are obliged to inform the French Data Protection Authority (CNIL) immediately in case of a breach. These ISPs are even compelled to keep records of cyberattacks. Under the GDPR, applicable since 25 May 2018, these obligations have been extended to all data controllers and processors, private and public. Failure by private and public data controllers and processors to take adequate security measures could have led to an administrative fine of up to €3 million according to the Data Protection Act of 1978. From now on, and since the entry into force of the GDPR, data controllers and processors may face an administrative fine of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million, whichever is higher, in case of failure to report and adopt appropriate security measures. By Act No. 2018-493 of 21 June 2018, France formally implemented the GDPR legal provisions.

Finally, reference can be made to the Directive on Security of Network and Information Systems (the NIS Directive) adopted by the European Union on 6 July 2016. This directive requires Essential Service Operators and digital service providers to adopt security measures and to report incidents affecting networks and information systems. The NIS Directive was transposed into French law by Act No. 2018-133 of 26 February 2018 and Decree No. 2018-384 of 23 May 2018.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The sectors most affected by security laws and regulations are the sectors providing essential services for the functioning of society and are, among others, the energy, transport, water, banking, financial market and healthcare industries. An exhaustive list of those sectors is provided in Decree No. 2018-384 of 23 May 2018.

On a more general aspect, every data controller and processor, private and public, is also bound by the French Data Protection Act of 1978 and the GDPR to provide adequate security measures when collecting, processing, transferring and storing data. In this regard, to meet this obligation and to be compliant with article 32 of the GDPR, they must adopt cybersecurity measures.

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

No.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Pursuant to article 32 of the GDPR, data controllers and processors processing personal data shall implement adequate technical and organisational measures to ensure a level of security appropriate to the risk. These include protection from unauthorised access, alteration and theft. ISPs (extended to all data controllers and processors under the GDPR) processing personal data are also bound to inform the CNIL immediately in case of a breach. They are also compelled to keep records of cyberattacks.

According to article 83 of the GDPR, non-compliant personnel and directors may be fined up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million by the CNIL. Additionally, pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and be fined up to €300,000. This amount is multiplied by five for organisations, pursuant to article 131-38 of the Criminal Code.

A relatively important act was adopted on 27 March 2017, namely Act No. 2017-399. This act requires that firms with more than 5,000 workers in France undertake a mapping of the potential risks that may negatively affect public liberties, fundamental rights and health and security, and take appropriate measures to mitigate their effects. This mapping must identify the risks, categorise their level of importance and analyse their potential consequences.

5 How does your jurisdiction define cybersecurity and cybercrime?

Neither cybersecurity nor cybercrime have universal and precise definitions. However, according to the ANSSI, cybersecurity can be defined as an information system that is sufficiently resilient to sustain and mitigate the impact of a cyberattack. The ANSSI further adds that cybersecurity is achieved by applying appropriate technical security measures to the information system, fighting cybercriminal acts and adopting cyber defence strategies.

Cybercrime is defined as the act of using an information system or network to commit a misdemeanour or a crime that is punishable by domestic law and international treaties.

A distinction must be made between cybersecurity and data privacy, as cybersecurity is considered to be a component of data privacy under French and EU law. As such, to have data privacy, cybersecurity measures would have to be implemented. In addition to this distinction, France's cybersecurity and cybercrime policies are increasingly seen as sections of the cyber defence policy.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In September 2017, the ANSSI published 42 measures to protect data and IT systems from cyberthreats. According to these measures, cybersecurity shall be seriously addressed and, therefore, it generally recommends to firms and organisations that they, among others:

- raise awareness;
- regularly update their IT systems;
- restrict access and encourage the use of strong authentication;
- conduct an audit;
- encrypt highly sensitive data and information when they are transferred; and
- decentralise the network.

The same measures have been recommended by the CNIL to personal data controllers and processors, either private or public. Regarding personal data, the GDPR requires a level of security adapted to the digital risk. It affirms the importance of assessing and dealing with risks to individuals. In particular, it requires organisations to implement appropriate technical or organisational measures, which may include encryption of data and tools to ensure confidentiality, integrity, availability and resilience.

Regarding essential sectors, several ministerial orders were adopted in 2016 and 2017. These orders provide for compulsory security measures, such as adopting detection tools, defensive tools, strong authentication and restricted access protocols that shall be taken by entities mainly operating in the electricity, maritime, finance, ISPs, space, gas, media, nuclear and arms industries.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Naturally, any cybercriminal offence committed that has been catered for in the Criminal Code shall apply to intellectual property (see below). Similarly, any violation of intellectual property that has been catered for in the Intellectual Property Code shall apply to cyber acts or acts committed within cyberspace. However, and on a more specific note, the law better protects against copyright breach and counterfeiting of trademarks and patents on the internet. Counterfeiters may face a fine of up to €500,000 (multiplied by five for organisations) and up to five years of imprisonment.

Cybersquatting is amenable to a €15,000 fine (multiplied by five for organisations) and up to one year of imprisonment. Providing software for the purpose of encouraging copyright breach may lead to a fine of up to €300,000 (multiplied by five for organisations).

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Pursuant to the Military Programming Act of 2013 for 2014 to 2019, the state has a duty and responsibility to take appropriate measures to protect essential sectors that are deemed 'of utmost importance for state survival'.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

France does not have any cybersecurity laws or regulations that specifically restrict the sharing of cyberthreat information. Such an approach will not be coherent and will surely hinder the proactive approach adopted to tackle cybercrime and cyberattacks. Article L2321-4 of the Defence Code even provides for the sole purpose of protecting an information system, namely that someone acting in good faith may inform the ANSSI about a cyberthreat. The whistle-blower's identity is also protected. Moreover, dedicated websites have been set up to disclose cyberthreats and vulnerabilities.

Additionally, if every individual has a right to privacy, which entails the right to private communication, this right may be levied, and metadata can be accessed by the government in cases of terrorism and organised crime.

10 | What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

France has enacted laws regarding a wide range of cybercrime-related offences since 1988. In this regard, the following cyberactivities are criminalised.

- Any cyberattack on an information system (article 323-1 of the Criminal Code) through unauthorised access or maintenance is criminalised, and cybercriminals may face a fine of up to €60,000 and up to two years of imprisonment (this fine is multiplied by five for organisations, thus up to €300,000).
- Should this access or maintenance lead to the alteration or deletion of data contained in the system or alter the good running of the system, this will be constitutive of an additional offence amenable to a fine of up to €100,000 (multiplied by five for organisations) and imprisonment of up to three years.
- Attacking state-operated information systems may lead to five years of imprisonment and a fine of up to €150,000 (multiplied by five for organisations).
- Any cyberattack that disrupts or distorts the good running of an information system is sanctioned by up to five years of imprisonment and a fine of up to €150,000 (multiplied by five for organisations). Disrupting or distorting state-operated information systems is sanctioned with seven years of imprisonment and a fine of up to €300,000 (multiplied by five for organisations).
- Introducing, extracting, cloning, transferring, modifying or deleting data of an information system is sanctioned with a fine of up to €150,000 (multiplied by five for organisations) and up to five years of imprisonment. Should the above-mentioned acts be committed to a state-operated information system, contraveners will face a fine of up to €300,000 (multiplied by five for organisations) and up to seven years of imprisonment.
- Importing, proposing or possessing any equipment, software or other tool developed to commit cybercriminal activities is amenable to the same sentence as the act itself or whichever sentence is higher.
- The organised commission of cybercriminal activities is amenable to the same sentence as the act itself or whichever sentence is higher. However, the organised commission of cybercriminal activities against information systems operated by the state is amenable to 10 years of imprisonment and a fine of up to €300,000. (Attempts are sanctioned in the same manner as the act itself.)
- Any unlawful collection, use, storage, transfer and processing of personal data, and failure to meet the security obligations and respect the right to object are also criminal offences amenable to a fine of up to €300,000 (multiplied by five for organisations) and up to five years of imprisonment.
- Impersonation or identity theft is amenable to one year of imprisonment and a fine of up to €15,000 (multiplied by five for organisations).
- Credit or debit card fraud is amenable to seven years of imprisonment and a fine of up to €750,000 (multiplied by five for organisations). Importing, proposing or possessing any equipment, software or other tool developed to commit credit or debit card fraud is amenable to the same sentence as the act itself or whichever sentence is higher.
- Cyber scams, such as phishing, are punishable by five years of imprisonment and a fine of up to €375,000 (multiplied by five for organisations).
- A breach of trust committed by means of accessing an information system is amenable to three years of imprisonment and a fine of up to €375,000 (multiplied by five for organisations).

The legislator has enhanced the investigatory powers of the police and established specialised cybercrime courts to deal in an efficient manner with cybercrime and attacks.

Additionally, dedicated institutional internet websites aiming to fight against unlawful cyber acts have been set up and allow the public to report such acts (eg, Pharos).

11 | How has your jurisdiction addressed information security challenges associated with cloud computing?

In December 2016, the ANSSI published its binding guidelines on the minimum cybersecurity standards and requirements that are to be maintained by software as a service, platform as a service and infrastructure as a service businesses. As such, it provides for the basic security measures (physical, environmental and operational), update policy, internal risk management (before and after cyberattacks), database and network management and information security policies, among others. On 5 October 2020, the ANSSI published a list of cloud computing providers that are certified and meet the security standards.

Additionally, the CNIL published its recommendations for businesses storing personal data on cloud service providers in 2012. The CNIL is very clear about the matter: cloud computing firms shall guarantee their compliance with French and EU legislation on data protection laws. Security measures are a core subject in this recommendation. It has provided a template that consists of the essential clauses and aspects that must be covered in a cloud computing contract.

12 | How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Data controllers and processors are bound by the obligation to secure the processing of personal data. In this regard, article 121 of the present Data Protection Act of 1978 and article 32 of the GDPR require that foreign organisations operating in France or offering goods or services (irrespective of whether a payment of the data subject is required) to such data subjects in France are bound by cybersecurity measures. The monitoring of their behaviour (as far as it takes place) within France is also bound by these measures.

Notwithstanding this particular case, and, on a broader perspective, from the moment when a cybercriminal offence is committed in French territory, French law and French jurisdiction will be competent, pursuant to article 113-2 of the Criminal Code. In this regard, should foreign organisations be either the victims or the cybercriminals, they will be bound by the Criminal Code should the offence be committed in France.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) and the French Data Protection Authority (CNIL) recommend additional cybersecurity protections beyond those that are mandated by law. As such, 42 measures to protect data and IT systems from cyberthreats have been published.

According to these measures, cybersecurity shall be seriously addressed and, therefore, it is generally recommended to firms and organisations that they, among others:

- raise awareness;
- regularly update their IT systems;

- restrict access and encourage the use of strong authentication;
- conduct an audit;
- encrypt highly sensitive data and information when they are transferred; and
- decentralise the network.

The same measures have been recommended by the CNIL to personal data controllers and processors, either private or public. Regarding personal data, the GDPR requires a level of security adapted to the digital risk. It affirms the importance of assessing and dealing with risks to individuals. In particular, it requires organisations to implement appropriate technical or organisational measures, which may include encryption of data and tools to ensure confidentiality, integrity, availability and resilience.

Regarding essential sectors, several ministerial orders were adopted in 2016 and 2017. These orders provide for compulsory security measures, such as adopting detection tools, defensive tools, strong authentication and restricted access protocols that shall be taken by entities mainly operating in the electricity, maritime, finance, internet service providers, space, gas, media, nuclear and arms industries.

14 How does the government incentivise organisations to improve their cybersecurity?

The approach taken towards cybersecurity is clear in France: it must be taken seriously, and appropriate measures must be set up. As such, the ANSSI and CNIL regularly publish guidelines and recommendations for good practice.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The 42 measures to protect data and IT systems from cyberthreats (which are very broad) can be accessed via www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

Recently, a dedicated website has been set up to help small and medium-sized enterprises, which can be accessed via www.cybermalveillance.gouv.fr.

The CNIL has also released detailed guidelines and a checklist regarding the good safekeeping of personal data, available respectively via:

- www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles; and
- www.cnil.fr/fr/securite-des-donnees.

16 Are there generally recommended best practices and procedures for responding to breaches?

France has adopted best practices and procedures. As such, the ANSSI and the CNIL recommend that the first step is to have recourse to a host-based intrusion detection system and a network-based intrusion detection system to identify in real time and certify the extent of the intrusion (compulsory for organisations identified as of essential importance).

Should a breach be identified, it is recommended that the organisation should:

- disconnect the affected IT system from the network;
- inform the local computer emergency response team;
- make a clone copy of the hard disk drive;
- gather evidence and search for a digital footprint; and
- file a complaint to the police.

For organisations of essential importance, notification shall be made to the ANSSI. For private and public data controllers and processors, notification shall be made to the CNIL.

After the attack, it is recommended that, to analyse the intrusion, organisations should:

- search for any modifications made to the operating system and operating system files;
- analyse if there has been any alteration or modification of data;
- search for any data or tool that may have been introduced by the hacker;
- analyse the logs;
- look for any sniffer on the network; and
- analyse the other devices and hardware connected to the affected network.

Information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Article L2321-4 of the Defence Code provides that, for the sole purpose of protecting an information system, someone acting in good faith may inform the ANSSI about a cyberthreat. Further, the whistle-blower's identity is protected, and several websites have been set up to encourage the sharing of information.

In this regard:

- illegal internet content may be declared via: www.internet-signalement.gouv.fr/PortailWeb/planets/SignalerEtapeAccepter!load.action;
- vulnerabilities may be declared via: www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite; and
- information on cyberthreats and vulnerabilities is available via: www.cert.ssi.gouv.fr.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The government and the private sector cooperate through non-profit organisations. As such, the ANSSI (acting on behalf of the government) and large companies such as Thales, Airbus and Enedis form part of the European Cyber Security Organisation (ESCO). The ESCO combines public and private entities and aims to develop, promote and encourage European cybersecurity. Additionally, a public-private partnership on cybersecurity was signed on 5 July 2016 to better equip the European Union against cyberattacks and to strengthen the competitiveness of its cybersecurity sector. Naturally, these include, and will benefit, French industries and the government.

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Europe represents 10 per cent of the cyber risk insurance market, and it is a fast-emerging market in France, as is shown from looking at the increasing number of institutional reports (for instance, those of the OECD or Club des Juristes). Insurers are proposing such services, and given the rise in awareness about the matter, the demand for such services will constantly grow. However, as cyberattacks are not easily predictable (regarding nature and consequence), these types of insurance may be expensive.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Military Programming Act of 2013 defines the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) as the primary authority for enforcing cybersecurity rules when dealing with organisations of essential importance.

When dealing with personal data, the French Data Protection Authority (CNIL) will be responsible for enforcing cybersecurity rules as well as prosecuting administratively, pursuant to the Data Protection Act of 1978 and the EU General Data Protection Regulation (GDPR).

Neither entity has the power to prosecute criminally since it will be within the sole jurisdiction of the public prosecutor.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Regarding the enforcement of security measures provided in the Data Protection Act of 1978 and the GDPR, compliance, monitoring, investigations and administrative prosecution will be conducted by the CNIL. As such, for monitoring and conducting investigations, the CNIL can go on-site and search and seize any relevant documents and information. When an offence has been proved, it has the power to prosecute administratively, but most importantly, the power to impose fines, issue injunctions, remove authorisation for data processing, impose warnings and publish its decisions.

The ANSSI will be responsible for carrying out compliance monitoring and investigations for sectors of essential importance and any information system that is operated by the state.

The above-mentioned entities do not have the power to prosecute criminally and request criminal sanctions provided in the Criminal Code, as this power is only vested in the public prosecutor.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

Concealment of data breaches is an important issue because organisations fear the negative impact that will follow. However, this approach is not recommended, and given the particular consequences of cyberattacks (for the economy when speaking of sectors of essential importance or for personal data regarding the right to privacy), the legislator has imposed heavy fines for non-compliance to encourage enforcement. Additionally, the legislator has also encouraged whistle-blowers to inform the ANSSI, but this information must be communicated in good faith. Dedicated websites have even been set up to facilitate notification to the respective authorities on cyberattacks, data breaches and incidents.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

For businesses that are part of the essential sectors and classified as 'of utmost importance for state survival', the ANSSI might have to be informed or notified if provided for in the specific rules strictly applicable to the businesses.

In the event of a personal data breach (which includes deliberate security breaches by third parties and accidental loss or corruption of data) that may likely result in a risk to the rights and freedom of individuals, any 'data controller' businesses that are victims of such a breach must notify the CNIL 'without undue delay and, where feasible, not later than 72 hours' after having become aware of the breach (article 33 of the GDPR and article 58 of the French Data Protection Act). Any 'data processor' businesses must notify the data controller without undue delay after having become aware of the breach (the notification to CNIL resting on the data controller once aware of the breach).

When a personal data breach is 'likely to result in a high risk for the rights and freedoms' for individuals, data controller businesses must inform the individuals without undue delay of the breach, unless:

- appropriate protection security measures or subsequent satisfactory measures to avoid such a risk have been taken;
- it would involve disproportionate effort (article 34 of the GDPR and article 58 of the French Data Protection Act) and so alternative solutions could be considered (public communication);
- the profile of the persons concerned is sensitive (police officer, military, civilian staff of the Ministry of Defence, customs officers); or
- such information may pose a risk to national security, national defence or public security.

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Since 25 May 2018, the GDPR provides that non-compliance with personal data security measures may be subject to an administrative fine by the CNIL of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million. Additionally, pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and face a fine of up to €300,000 (multiplied by five for organisations). Organisations of essential importance may be subject to criminal fines of up to €150,000 in cases of contravention of cybersecurity laws, pursuant to article L1332-7 of the Defence Code.

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Pursuant to the GDPR article 83, personal data controllers and processors who fail to comply with the rules on reporting breaches (provided in article 33) may face an administrative fine by the CNIL of up to 2 per cent of the total worldwide annual turnover of the preceding financial year or €10 million. Organisations of essential importance may be subject to a €150,000 fine in the case of contravention of cybersecurity laws. Additionally, and pursuant to article 226-17 of the Criminal Code, contraveners may face up to five years of imprisonment and be fined up to €300,000 (multiplied by five for organisations).

26 | How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties can seek private redress for any unauthorised cyberactivity or failure to adequately protect systems and data under article 1240 of the Civil Code. As such, and under the cause of action of negligence, parties may seek damages as a result of the damage suffered.

THREAT DETECTION AND REPORTING

Policies and procedures

27 | What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

It depends on whether the organisation is defined as an organisation of essential importance or whether the organisation is considered a data controller or processor.

For organisations of essential importance, rules and procedures are imposed on them by either decree, ordinance or ministerial orders. As such, since 2016, entities operating in the electricity, maritime, finance, internet service providers (ISPs), space, gas, media, nuclear and arms industries shall adopt compulsory security measures, such as detection tools, defensive tools, strong authentication and restricted access protocols.

The same cybersecurity measures have been recommended by the French Data Protection Authority (CNIL) regarding personal data on data controllers and processors, private or public. The EU General Data Protection Regulation (GDPR) has even provided, under article 32, security requirements that may be expected from data controllers and processors, namely:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

France has rules requiring organisations to keep records of cyberattacks. As such, pursuant to article 83 of the Data Protection Act of 1978 ISPs are required to keep records of cyberattacks. Article 33 of the GDPR extends this obligation to all data controllers and processors. The records are collected by way of audit and must specify how the attack happened, its consequences and the measures taken. The law does not specify for how long these records must be kept.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Pursuant to article 83 of the Data Protection Act of 1978, ISPs must report, without any delay, data breaches to the CNIL. Under the GDPR, this obligation is now borne by every data controller and processor, private or public.

According to article 29 of the Data Protection Working Party Opinion 03/2014 on breach notification, three types of incidents must be reported:

- confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data;
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
- integrity breach – where there is an unauthorised or accidental alteration of personal data.

To facilitate reporting, dedicated forms have been provided online and, in the particular case of personal data, can be submitted online.

ADSTO
Avocats à la Cour

Claire Bernier
clairebernier@adsto.legal

24 Boulevard de Douaumont
75017 Paris
France
Tel: +33 1 77 14 42 33
Fax: +33 9 72 61 22 95
www.adsto.legal

Regarding organisations of essential importance and in accordance with article L1332-7 of the Defence Code, they must report any cybersecurity breach or incident to the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Notification of violation and breach is followed by a report. Information required in reports of cyberthreats depends on the business sector of the organisation considered of essential importance. Regarding personal data, the GDPR is more precise on the matter: data controllers and processors must provide precise information on the time of the attack, its nature, the personal data affected, the remedies applied and the potential consequences of the breach, among others.

Time frames

30 | What is the timeline for reporting to the authorities?

Entities must report without any delay to the CNIL when personal data is concerned, and to the ANSSI if the entities affected are qualified as of essential importance. The GDPR provides more precision about the timeline, namely that the incident must not be reported later than 72 hours (where feasible) after the entity has become aware of the breach.

To facilitate reporting, dedicated forms have been provided online and, in the particular case of personal data, can be submitted online.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

According to article 83 of the Data Protection Act of 1978 and in the case of a personal data breach, ISPs are compelled to report, without any delay, to customers aggrieved by such breach. This obligation has been extended to all data controllers and processors under the GDPR. Such notification may be levied if the CNIL certifies that appropriate measures have been taken to make direct or indirect identification impossible. According to article 29 of the Data Protection Working Party, in its guidelines on personal data breach notification for the new regulation, dedicated messages should be used when communicating a breach. These include, among others:

- direct messaging (eg, email, SMS and direct message);
- prominent website banners or notifications;
- postal communications; and
- prominent advertisements in print media.

UPDATE AND TRENDS

Key developments of the past year

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

No updates at this time.

India

Rohan Bagai and Aprajita Rana*

AZB & Partners

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

While India does not have a dedicated cybersecurity law, there are several legislations and sector-specific regulations which, inter alia, promote the maintenance of cybersecurity standards. One of the primary legislations dealing with cybersecurity, data protection and cybercrimes is the Information Technology Act 2000 (the IT Act), read with the rules and regulations framed thereunder. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but also contains provisions that are aimed at safeguarding electronic data, information or records, and preventing unauthorised or unlawful use of a computer system. Some of the cybercrimes that are specifically envisaged and punishable under the IT Act are hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft.

In accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, the Computer Emergency Response Team (CERT-In) has been established as the nodal agency responsible for the collection, analysis and dissemination of information on cyber incidents and taking emergency measures to contain such incidents.

Other relevant rules framed under the IT Act in the context of cybersecurity include:

- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for collection and the processing of personal or sensitive personal data;
- the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, which require specific information security measures to be implemented by organisations that have protected systems, as defined under the IT Act; and
- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the Intermediaries Guidelines) which supersede the erstwhile Information Technology (Intermediaries Guidelines) Rules, 2011, require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein. The intermediaries are also required to report cybersecurity incidents (including information relating to such incidents) to CERT-In.

Other laws that contain cybersecurity-related provisions include the Indian Penal Code 1860, which punishes offences, including those committed in cyberspace (such as defamation, cheating, criminal intimidation and obscenity), and the Companies (Management and Administration) Rules 2014 (the CAM Rules) framed under the Companies Act 2013, which require companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

In addition to the above, there are sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India, the Department of Telecommunication (DOT) and the Securities Exchange Board of India (SEBI), which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Regulated entities operating in sensitive sectors, such as financial services, banking, insurance and telecommunications, have exhibited higher standards of cybersecurity preparedness and awareness, partly because of regulatory intervention but also because of voluntary compliance with advanced international standards. Sectors such as e-commerce, IT and IT-enabled services that have seen an infusion of foreign direct investment have also proactively deployed robust cybersecurity frameworks and policies to counter the evolving nature of cyber fraud as they have borrowed advanced cybersecurity practices and procedures from their parent entities in the United States, the European Union and other mature jurisdictions.

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased and become complex. While the RBI has been active in requiring companies operating payment systems to build secure authentication and transaction security mechanisms (such as two-factor authentication, EMV chips, PCI DSS compliance and tokenisation), given that these payment companies often offer real-time frictionless payment experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyberthreats. In light of the above, there is an increased need for entities to identify and develop cybersecurity standards commensurate with the nature of the information assets handled by them and evaluate the possible harm in the event of any cybersecurity attack, to ensure that these emerging risks are mitigated.

Moreover, the covid-19 pandemic has led to increased dependencies on digital infrastructure for many organisations, as employees are being given the option of working remotely on a long-term or permanent basis. This has led to enormous cybersecurity-related vulnerabilities and challenges for large and small organisations alike and made them

rethink cybersecurity preparedness, policies and budgets. We have already witnessed large-scale cyberattacks and disruption in sensitive sectors in India. The demand for remote work, new technologies and vulnerabilities resulting therefrom will continue to be relevant, and we expect cybersecurity standards to be given critical importance in the immediate future.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Yes, the SPDI Rules require body corporates that handle sensitive personal data or information to implement 'reasonable security practices and procedures' by maintaining a comprehensively documented information security programme. This programme should include managerial, technical, operational and physical security control measures that are commensurate with the nature of the information being protected. In this context, the SPDI Rules recognise the International Standard ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements as one such approved security standard that can be implemented by a body corporate for protection of personal information. All body corporates that comply with this standard are subject to audit checks by an independent government-approved auditor at least once a year or as and when they undertake a significant upgrade of their processes and computer resources.

Sector-specific regulators have also prescribed security standards specifically applicable to regulated entities. For instance, the RBI guidelines mandate banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards for ensuring adequate protection of critical functions and processes. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to implement data security standards and best practices such as PCI-DSS and PA-DSS. Similarly, SEBI requires stock exchanges, depositories, clearing corporations, etc, to follow standards such as ISO/IEC 27001, ISO/IEC 27002 and COBIT 5.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

While there is no specific statutory provision that requires information security personnel to keep directors informed of an organisation's network preparedness, in the event of a cybersecurity breach, the persons in charge of an organisation are required to demonstrate before regulators that they have implemented security control measures as per their documented information security programmes and information security policies. Therefore, it would be necessary for these persons to be aware of and updated about the information security preparedness of their organisation to effectively discharge their responsibilities.

Section 85 of the IT Act also specifically states that in case of any contravention of the provisions stipulated thereunder, any person who is in charge of supervising the affairs of a company will be liable and proceeded against, unless he or she is able to prove that the contravention took place without his or her knowledge, or that he or she exercised all due diligence to prevent such contravention. Therefore, personnel can protect themselves from liability by being aware of and deploying adequate cybersecurity measures.

Separately, as per the CAM Rules, the managing director, company secretary, or any other director or officer of the company (as may be decided by the board) is responsible for the maintenance and security of electronic records. This person is required, inter alia, to provide adequate protection against unauthorised access, alteration or tampering of records; ensure that computer systems, software and hardware are secured and validated to ensure their accuracy, reliability and accessibility; and take all necessary steps to ensure the security, integrity and confidentiality of records. Any failure by such personnel in this regard may be construed to be a breach of their duties towards the organisation and is punishable with a monetary penalty.

5 How does your jurisdiction define cybersecurity and cybercrime?

Under the IT Act, 'cybersecurity' means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. 'Cybercrime', on the other hand, has not been defined under any central statute or regulations; however, the National Cyber Crime Reporting Portal (a body set up by the government to facilitate reporting of cybercrime complaints) has defined 'cybercrime' to mean 'any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime'.

The courts in India have also dealt with various instances of cybercrime over the years. The Gujarat High Court, in the case of *Jaydeep Vrujlal Depani v State of Gujarat* (R/SCR.A/5708/2018 Order), recognised a publicly available definition of 'cybercrime' to mean 'the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)'.

While the IT Act does not make any distinction between cybersecurity and data privacy, in our view, these issues are distinct but also deeply interconnected, as ensuring the privacy of any data (whether of an individual or a corporate) requires adequate cybersecurity processes to be implemented by organisations. Further, cybersecurity and information security frameworks are developed by organisations at a broader level to build resilience against various forms of cyberthreat, including cybercrimes that entail more extensive engagement with regulatory authorities depending on the extent of the harm caused, the nature of the information handled by the body corporate, sector sensitivities, etc.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

As per the SPDI Rules, any body corporate that possesses, deals with or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements).

Sector-specific cybersecurity measures have been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the RBI requires banks to undertake certain security measures, including, inter alia, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security. The RBI also requires

payment aggregators to implement data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc. as per the Guidelines on Regulation of Payment Aggregators and Payment Gateways.

Additionally, in the telecommunications sector, the licence conditions imposed by the DOT require every licensee to implement the following measures:

- ensure protection of privacy of communication so that unauthorised interception of messages does not take place;
- have an organisational policy on security and security management of its network, including network forensics, network hardening, network penetration tests and risk assessment; and
- induct only those network elements into its telecom network that have been tested as per relevant contemporary Indian or international security standards (eg, the IT and ITES elements) against the ISO/IEC 15408 standards (eg, the ISO 27000 series standards for information security management systems and the 3GPP and 3GPP2 security standards for telecoms and telecoms-related elements).

Further, critical information infrastructure (CII) is separately regulated by the National Critical Information Infrastructure Protection Centre (NCIIPC) and the 'Guidelines for the Protection of National Critical Information Infrastructure' (CII Guidelines). CII has been defined under the IT Act to mean any computer resource, the incapacitation or destruction of which can have a debilitating impact on national security, the economy, public health or safety. Under the CII Guidelines, certain best practices and controls are provided as minimum recommendations to be implemented by the CIIs at different stages of CII functioning, to maintain safe and secure operations. In addition to the CII Guidelines, the NCIIPC in April 2020 also issued covid-19 guidelines titled 'Building Resilience against Cyber Attacks during COVID-19 Crisis', which intend to provide guidance to CIIs on various issues, including managing email phishing risks, protection of organisational assets and enabling employees to work remotely.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The IT Act and related laws are equally applicable to cyberthreats involving intellectual property and grant similar protection.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

As per section 70 of the IT Act, the government may notify any computer resource that directly or indirectly affects the facility of CII to be a 'protected system'. CII means any computer resource of which the incapacitation or destruction can have a debilitating impact on national security, economy, public health or safety. Under the Protected System Rules, specific cybersecurity practices are applicable in the context of a protected system, such as setting up an information security steering committee (Committee) to approve all information security policies relating to the protected systems, designating a chief information security officer (CISO) and carrying out vulnerability, threat or risk analysis on an annual basis. Significant changes in network configuration would need to be approved by the Committee, and organisations would need to ensure timely communication of cyber incidents to the Committee.

Under the provisions of the IT Act, a nodal body – the NCIIPC – has been set up to work in the interest of CII protection. The NCIIPC is authorised to reduce vulnerabilities of CII against cyberterrorism, cyber warfare and other threats. Certain identified CIIs are in sectors such as transport, telecoms, banking, insurance, finance, power, energy and governance.

The Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations 2010 mandate utilities such as entities engaged in the distribution and transmission of electricity to implement a cybersecurity framework to identify critical cyber assets and protect such assets for reliable operation of the grid. New regulations, namely the Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations 2020 have been proposed, which require all entities to have an information security policy in place to prevent unauthorised access, use, disclosure, modification, destruction, etc of information, have necessary protection mechanisms such as firewalls for all systems interfacing with the network, and take necessary backup and protection measures for classified and sensitive data.

Sector-specific cybersecurity regulations are also available for sectors such as banking, telecommunications, finance and insurance.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In the judgment of *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under article 21 of the Constitution of India and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence. Given that this issue is unsettled, the permissibility of recordings will need to be determined on a case-by-case basis.

In any case, the SPDI Rules require a body corporate to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the IT Act for the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes. The SPDI Rules also permit disclosure without consent in cases where the disclosure is made pursuant to an enforceable order under applicable law.

Certain laws, such as the Indian Telegraph Act 1885 (the Telegraph Act) and the IT Act, permit governmental and regulatory authorities to access private communications and personally identifiable data in specific circumstances. The Telegraph Act empowers the government to intercept messages in the interest of public safety, national security or the prevention of crime, subject to certain prescribed safeguards. In that scenario, the telecoms licensee that has been granted a licence by the DOT is mandated to provide necessary facilities to the designated authorities of the central government or the relevant state government for interception of the messages passing through its network.

The IT Act also grants similar authority to the government and its authorised agencies. Any person or officer authorised by the government (central or state) can, inter alia, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event that it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data

for cybersecurity incidents if they relate to contravention or investigation of any crime.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

Cybercrime activities are specifically dealt with under the IT Act. It prescribes penalties ranging from fines to imprisonment for various types of cyber activities, including hacking, tampering of computer source code, denial-of-service attacks, phishing, malware attacks, identity fraud, electronic theft, cyberterrorism, privacy violations and the introduction of any computer contaminant or virus.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

There is no separate set of laws or regulations that regulate the provision of cloud computing services in India. However, given that cloud computing services are rendered and received over the internet or through the digital medium, certain provisions of the IT Act, the SPDI Rules and the Intermediaries Guidelines may be relevant to these services.

For instance, the SPDI Rules allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer. Accordingly, in our view, any entity engaged in the cloud computing business will need to ensure that it maintains the same level of information security standards as that of the data controller (ie, the person collecting the information from the data subject).

Also, depending on the business model, a cloud services provider may fall within the definition of an intermediary under the IT Act (defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecoms service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cybercafes). As an intermediary, the cloud service provider will need to observe due diligence measures to claim safe harbour protection from liability arising from the content stored by it. These due diligence measures include taking all reasonable steps to secure its computer resource and the information contained therein by adopting the security practices prescribed under the SPDI Rules.

The RBI also issued 'Guidelines on Regulation of Payment Aggregators and Payment Gateways' on 17 March 2020, where it mandates all payment aggregators to adhere to the data storage requirements applicable for payments data to ensure that all data is stored only in India for the RBI's unfettered supervisory access.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The IT Act also applies to any offence committed outside India if the act that constitutes the offence involves a computer, computer network or computer resource in India. Hence, the applicability of this law is agnostic to the presence of foreign organisations in India so long as users in India can access the services provided by the organisations and the operation of the services amounts to the contravention of any provision described thereunder.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In addition to minimum statutory cybersecurity standards, various regulatory bodies have advised businesses to adopt more robust measures in areas of cybersecurity. For example, the Ministry of Communication and Information Technology released the National Cyber Security Policy in 2013, which recommended creating a secure cyber ecosystem, strengthening laws and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy intended to encourage all organisations to develop information security policies integrated with their business plans and implement the policies in accordance with international best practices.

Under the Digital India initiative, the Ministry of Electronics and Information Technology (MeitY) has set up the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), operated by the Computer Emergency Response Team (CERT-In), to work with internet service providers and product or antivirus companies to provide information and tools to users on botnet and malware threats. Similar proactive measures are deployed by sector-specific regulators from time to time.

14 How does the government incentivise organisations to improve their cybersecurity?

In recent years, the government has rolled out some beneficial measures to incentivise both public and private sector organisations to improve cybersecurity standards. One example is the Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products notified by MeitY on 2 July 2018, wherein cybersecurity was named as a strategic sector, and it was further mentioned that government procurement agencies will give preference to domestically manufactured or produced cybersecurity products.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In addition to the Information Technology Act 2000 and the applicable rules framed thereunder, industry-specific standards have been prescribed by specific regulators. Some examples are given below.

- Financial sector: the Reserve Bank of India has issued various guidelines for ensuring cybersecurity and the handling of cyber fraud within the banking sector. They can be accessed at www.rbi.org.in and include the following:
  - Cyber Security Framework in Banks, prescribing standards to be followed by banks for securing themselves against cybercrimes;
  - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks, prescribing certain basic cybersecurity controls for primary urban cooperative banks;
  - Sharing of Information Technology Resources by Banks – Guidelines, ensuring that privacy, confidentiality, security and business continuity are fully met;
  - Information Technology Framework for the NBFC Sector, 2017, focusing on IT policy, IT governance information and cybersecurity; and
  - Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, prescribing IT policy and outsourcing guidelines and recommendations.

- Insurance sector: the insurance sector is subject to the 'Guidelines on Information and Cyber Security for Insurers' (Insurance Cyber Guidelines), issued by the Insurance Regulatory and Development Authority of India. Under these guidelines, the insurers are responsible for putting in place adequate measures to ensure that cybersecurity issues are addressed. Insurers are also mandated to appoint a chief information security officer (CISO), formulate a cyber crisis management plan and conduct audits.
- Telecommunications sector: the licence conditions for a unified licence granted by the Department of Telecommunication (DOT) prescribe various cybersecurity obligations on the licensee entity. For instance, the licensee is obligated to ensure the protection of privacy of communication and that unauthorised interception of messages does not take place; the licensee is to be completely responsible for security of their networks and must have an organisational policy on the security and security management of their networks, etc. Due to the large surge in cybersecurity incidents fuelled by large-scale remote work adoption during the covid-19 pandemic, the DOT has been issuing, inter alia, various security-related circulars to update stakeholders, such as Best Practices – Cyber Security, which provides protocols to be followed by organisations; and Unsafe Practices to be Avoided at Workplace for Cyber Security, which describes unsafe workplace practices that may be avoided, such as using common passwords, leaving devices unlocked, ignoring operating systems and software updates and downloading files without scanning.

16 | Are there generally recommended best practices and procedures for responding to breaches?

Depending on the nature and the extent of the cybersecurity incident and the sensitivity of the sector, cyber incident response strategies may differ from one business to another. Some common measures that are recommended include:

- deploying a detailed information security policy to be approved by the board;
- conducting regular transaction monitoring;
- conducting information security risk assessments;
- setting up risk mitigation and transition plans;
- updating relevant stakeholders within the organisation on their role in advance; and
- allocating appropriate personnel to engage with regulatory authorities and to deal with clients, service providers, etc.

Many companies also prefer to conduct regular assessments of the vulnerabilities in their systems, including by inviting focused hacking. Depending on the sector, organisations can also reach out to CERT-In and seek advice on incident recovery, containing the damage and restoring their systems to operation. From time to time, CERT-In also issues advisories on actions recommended for parties that have been affected by cybersecurity incidents.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 require individuals and corporate entities affected by certain types of cybersecurity incidents to mandatorily report the incidents to CERT-In. In addition, it is also possible for individuals and organisations to voluntarily report any other cybersecurity incidents and vulnerabilities to CERT-In and seek requisite support and technical assistance to recover from them. Whether timely and voluntary reporting will help mitigate the imposition of a penalty for failing to implement reasonable security practices will be a fact-specific assessment.

In addition, the Securities Exchange Board of India (SEBI), in its 'Cyber Security & Cyber Resilience Framework' for Stock Brokers/ Depository Participants, has mandated stockbrokers and depository participants to submit quarterly reports to stock exchanges and depositories with information on cyberattacks and threats experienced by such entities and the corresponding measures that were taken to mitigate the vulnerabilities, threats and attacks.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The government issues consultation papers to invite feedback and suggestions from the private sector, which aids the formulation of policies and laws in respect of cybersecurity. For instance, presently, the government is working with the private sector to develop its 2020 cybersecurity strategy. In addition, the National Cyber Security Coordinator and the Data Security Council of India have in 2019 launched an online repository on cyber tech called 'Techsagar' to facilitate exchange and collaboration on matters of innovation and cybersecurity between businesses and academia. It is intended to provide an overview of India's cybersecurity preparedness and relevant stakeholders.

In a first of its kind public-private partnership, MeitY in 2018 launched 'Cyber Surakshit Bharat' to strengthen the cybersecurity ecosystem in India, by spreading awareness about cybercrime and undertaking capacity-building for CISOs and IT staff across all government departments. The founding partners of the consortium are IT companies Microsoft, Intel, WIPRO, Redhat and Dimension Data. Additionally, knowledge partners include CERT-In, NIC, NASSCOM and the FIDO Alliance and consultancy firms Deloitte and EY.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Cybersecurity insurance has gained momentum in India. It is aimed at shielding online users against the damage and loss that may arise as a result of unauthorised disclosure of or access to personal and financial data. Cyber insurance is prevalent in the banking, IT and ITES, retail and manufacturing sectors.

Furthermore, the much-awaited National Cyber Security Strategy 2020 is also expected to promote and provide a framework for cyber insurance in India, given the appreciated risk due to large-scale remote work adoption, including for protected and critical systems.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Computer Emergency Response Team (CERT-In) is the nodal agency recognised under the Information Technology Act 2000 (IT Act) for the coordination of cyber incident response activities and the handling of cybersecurity incidents. Further, the government has also established certain authorities and agencies for according protection specifically to the critical infrastructure of India, such as the National Critical Information Infrastructure Protection Centre, which was created to assess and prevent threats to vital installations and critical infrastructure in India. As and when a cybersecurity incident is determined,

individuals and organisations can seek remedy from the adjudicating authorities appointed under the IT Act.

Sector-specific regulators have also attempted to enforce compliance with their respective information security standards. For example, the Reserve Bank of India (RBI) imposed a monetary penalty of 1 million rupees on the Union Bank of India for non-compliance with the directions of the Cyber Security Framework in Banks.

In January 2020, the Union Minister for Home Affairs inaugurated the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime in a comprehensive and coordinated manner. One of the components of I4C is the National Cyber Crime Reporting Portal, which is a citizen-centric initiative that enables citizens to report all kinds of cybercrime online, with a specific focus on crimes against women and children – particularly child pornography, child sexual abuse material and online content pertaining to rapes, gang rapes and similar crimes. The complaints reported on this portal are dealt with by law enforcement agencies and police, based on the information made available in the complaints.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Given that CERT-In is the national agency responsible for cybersecurity, it has the authority to call for information and give directions to service providers, intermediaries, data centres, body corporates and any other person to perform their functions under the IT Act and the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013. Failure to respond to CERT-In's information requests may lead to the imposition of monetary penalties.

Further, the adjudicating authorities appointed under the IT Act have the powers of a civil court to call for evidence and documents, and summon witnesses in connection with an inquiry into any contravention under the IT Act.

As per the provisions of the IT Act, for national security and for investigation of any offence (including cybersecurity offences), authorised government officers can issue orders to intercept, monitor or decrypt any computer resource, ask intermediaries to provide access to any information or to block access to any information stored, received or generated in any computer resource. Additionally, law enforcement agencies can be authorised to monitor and collect traffic data or information generated, received or transmitted in any computer resource, and can confiscate any computer resource in respect of which any contravention of the IT Act has been carried out.

Indian law also provides law enforcement authorities with various other mechanisms to pursue, investigate and prosecute cyber criminals. For instance, the Indian Penal Code 1860 (IPC) is a comprehensive code intended to cover most substantive aspects of criminal law. Criminal activities punishable under the IPC do extend to the online cyberspace infrastructure and will be dealt with in the same manner.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Regulators in India have relied on the provisions of the IT Act and the IPC to prosecute entities found to be non-compliant with mandatory information security requirements. However, from a practical perspective, enforcement agencies often face challenges in prosecuting offshore entities that do not have a business presence in India, as well as affixing liability in multi-layered business outsourcing structures. The absence of a comprehensive data protection law that allocates cybersecurity responsibilities between all relevant stakeholders is also a concern. Over time, the private sector and the government have felt the need to develop more cybercrime and prosecution expertise among the police personnel responsible for prosecuting offences under the IT Act, and specific local cyber cells have been set up to address this gap.

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

There is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. However, under the Intermediaries Guidelines, the intermediary is required to inform CERT-In of cybersecurity breaches as soon as possible. Further, specific types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) have to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the occurrence or noticing the incident to aid timely action.

In addition, sector-specific regulators have their own reporting requirements. For instance, the RBI requires banks to comply with the Cyber Security Framework in Banks, which, inter alia, requires banks to report cybersecurity incidents to the RBI within two to six hours. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to put in place a mechanism for the monitoring, handling and follow-up of cybersecurity incidents and breaches. Such incidents and breaches are to be reported immediately to the Department of Payment and Settlement Systems, RBI, Central Office, Mumbai, and reported to CERT-In.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The IT Act provides for penalties for varied instances of cybersecurity breaches, some of which are described here. Section 43 of the IT Act provides that any person accessing a computer or a computer system or network without permission of the owner, downloading copies and extracting any data or causing disruption of any system will be liable to pay damages to the person affected. Section 66 of the IT Act also provides for punishment of imprisonment for a term up to three years or with a fine of up to 500,000 rupees if the person dishonestly or fraudulently commits the offence.

Section 66C of the IT Act provides that a person who, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person will be punished with imprisonment of up to three years and will also be liable for payment of a fine of up to 100,000 rupees.

Additionally, the IT Act provides for imprisonment of up to one year or a fine of up to 100,000 rupees, or both, for any failure by an entity (service provider, intermediary, data centre, body corporate, etc) to provide requisite information requested by CERT-In. Furthermore, sector-specific authorities (such as the RBI) may also levy penalties for non-compliance with their respective cybersecurity standards.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Any failure by intermediaries to report cybersecurity incidents to CERT-In is punishable under the IT Act by a monetary penalty not exceeding 25,000 rupees. Any failure of a body corporate to report specific cyber breaches mandated under the IT Act is punishable by the same amount. Further, if CERT-In specifically requests any information from an entity (including the service provider, intermediary or body corporate), then a

failure to submit the information is punishable by imprisonment of up to one year or a fine that may extend to 100,000 rupees, or both.

In addition, sector-specific regulators have their own reporting requirements. For instance, failure to report within the timelines prescribed for banks under the Cyber Security Framework in Banks may result in the imposition of penalties by the RBI. For the telecommunications sector, the unified licence conditions stipulate that any failure by the licensee to comply with the obligations provided therein, including reporting of any intrusions, attacks and frauds on the technical facilities, may render the concerned licensee liable to a monetary penalty of up to 500 million rupees per breach.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

There is no specific private remedy available; however, the IT Act makes statutory remedies available to persons affected. Section 43A of the IT Act expressly provides that whenever a body corporate possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security practices and procedures that in turn cause wrongful loss or wrongful gain to any person, the body corporate shall be liable to pay damages to the person affected. Therefore, the affected party may initiate a civil action against the negligent body corporate, making it liable to pay damages.

Further, a civil action may also be brought against any person who, without permission of the owner of a computer or a computer system or network, does any of the acts mentioned under section 43 of the IT Act, including but not limited to accessing or securing access to the computer or computer system or network, downloading or extracting any data from it, contaminating it with a virus or other malware, or causing any damage to it.

In addition, the Securities Exchange Board of India's Guidelines ('Cyber Security & Cyber Resilience Framework' for Stock Brokers/Depository Participants) have mandated stockbrokers and depository participants to draft their cybersecurity and cyber resilience policy document and ensure provisioning of alternate services or systems to customers in the event of any security incident.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are no general cybersecurity policies and procedures applicable to all organisations. Some specific requirements are mentioned below.

- Information Technology Act 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules): as per the SPDI Rules, all organisations handling sensitive personal information of natural persons (financial and health information, passwords, biometric data, etc) should, inter alia:
  - have information security systems in place that are commensurate to the information assets sought to be protected;
  - appoint a grievance officer to address any discrepancies and grievances of the provider of such information;
  - have a privacy policy for providing information on how such information is used and disclosed, etc; and
  - in addition, organisations are required to audit the reasonable security practices and procedures that have been implemented at least once a year, or as and when the body corporate or a person on their behalf undertakes significant upgrading of their process and computer resources.
- Companies (Management and Administration) Rules 2014: companies, when dealing with electronic records, are required to ensure the security of any such records, including:
  - protection against unauthorised access;
  - protection against alteration;
  - protection against tampering;
  - maintaining the security of computer systems, software and hardware;
  - protecting signatures; and
  - taking periodic backups; etc.
- The Reserve Bank of India (RBI) has issued a notification on 'Cyber Security Framework for Banks', which prescribes standards to be followed by banks for securing themselves against cybercrimes, including, for example, a mechanism for dealing with and reporting incidents, a cyber crisis management plan, and arrangements for continuous surveillance of systems and protection of customer information. A similar framework is applicable to non-banking finance companies. The Guidelines on Regulation of Payment Aggregators and Payment Gateways require payment aggregators to put in place a Board-approved information security policy for the safety and security of payment systems operated by them and to implement security measures in accordance with this policy to mitigate identified risks.
- The Insurance Regulatory and Development Authority of India (IRDA) has issued 'Insurance Cyber Guidelines', which mandate insurers to appoint a chief information security officer, formulate a cyber crisis management plan and conduct audits.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Generally, no specific record-keeping requirements have been prescribed for cyber threats or attacks; however, maintaining records may become necessary to adhere to security standards. For instance, the Computer Emergency Response Team (CERT-In) issued the CERT-In Security Guidelines CISG-2009-01, which describe a 'log' as a record of actions and events that take place on a computer system. The guidelines recommend that organisations have appropriate auditing policies in place that efficiently collect the information logs relating to events, including critical events occurring in the network and systems. No specific timeline for record-keeping has been prescribed.

Sector-specific regulators have prescribed storage requirements for regulated entities. For instance, the IRDA issued the 'Insurance Cyber Guidelines', which require all registered insurance companies to retain security logs of different systems and devices to be maintained for a minimum period of six months. The guidelines also mandate the implementation of an incident management system that should include security incident reporting and recording.

Lastly, in accordance with the Securities Exchange Board of India Guidelines ('Cyber Security & Cyber Resilience Framework' for Stock Brokers/Depository Participants), stockbrokers and depository participants are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period not less than two years.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Reporting under the IT Act

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 permit cybersecurity incidents to be reported by any person to CERT-In. However, specified types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) need to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and bodies corporate within a reasonable time of the incident occurring or being noticed to aid timely action.

The Intermediaries Guidelines require the intermediaries, as part of their due diligence obligations, to notify CERT-In of security breaches. CERT-In publishes the formats for reporting cybersecurity incidents on its website from time to time, which requires mentioning the time of occurrence of the incident, the type of incident, information regarding the affected systems or network, the symptoms observed, the relevant technical systems deployed, and the actions taken, among others.

Reporting in other sectors

In addition to the reporting requirements under the IT Act, separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the Cyber Security Framework in Banks requires banks to inform the RBI of any cybersecurity incident within two to six hours of the breach and include details of it in a standard reporting template. Such report must include all unusual cybersecurity incidents (whether they were successful or were attempts that did not succeed). Similarly, as per the Insurance Cyber Guidelines issued by the IRDA, insurers are required to report cybersecurity incidents that critically affect business operations and a large number of customers within 48 hours of having knowledge of the cybersecurity incident.

In the telecommunications sector, every telecommunication licensee is required to establish a creative facility (within 12 months of grant of authorisation) for monitoring intrusions, attacks and frauds on its technical facilities, and to provide reports of such intrusions, attacks and frauds to the Department of Telecommunication.

Time frames

30 | What is the timeline for reporting to the authorities?

The Intermediaries Guidelines require intermediaries to inform CERT-In of cybersecurity breaches as soon as possible. Further, specific types of cybersecurity incidents, such as target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc have to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the occurrence or of noticing the incident, to aid timely action.

Separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the RBI requires banks to report cybersecurity incidents within two to six hours. The IRDA requires insurers to report cybersecurity incidents that critically affect business operations and a large number of customers within 48 hours of having knowledge of the incident.

AZB & PARTNERS
ADVOCATES & SOLICITORS

Rohan Bagai
rohan.bagai@azbpartners.com

Aprajita Rana
aprajita.rana@azbpartners.com

AZB House
Plot No. A-7 and A-8
Noida 201301
National Capital Region
India
Tel: +91 120 417 9999
www.azbpartners.com

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There is no obligation to report cybersecurity threats or breaches to the general public or affected parties.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Various factors have contributed to the delayed formulation of cybersecurity regulations in India, including the rapid advancement of technology, which continues to outpace regulatory response; intermittent and ineffective reporting of incidents; the private sector's inability to accurately assess the criticality of available information and the likely harm that may be caused in the event of an incident; lack of cross-functional expertise on the nature of cybersecurity incidents that may be experienced by varied sectors; and government and private sector hesitation to mandate minimum standards for all categories of businesses, in view of the time and expense involved.

In the last year, however, there has been a renewed focus on the adoption of robust cybersecurity practices in India, from both, the government and the private sector. Due to the covid-19 pandemic and the large-scale remote work and new technology adoption resulting from it, the private sector has been quite vigilant in adapting its processing, updating its budgets and responding to cyber threats in a timely and nuanced manner. Several organisations, such as the Data Security Council of India, have proactively issued advisories and assisted other private sector organisations to seamlessly transition to safer digital processes. We expect these initiatives to guide the government in terms of the level of cybersecurity preparedness expected from organisations, how the private sector has responded to cybersecurity

threats, a renewed focus on the revision of policies and the diversified skill-set of response stakeholders, and testing the efficacy of protective technologies and strategies. Timely and descriptive cybersecurity reporting by the private sector will bring in more collaboration and clarity on better practices. The varied experiences of regulated businesses regarding cyber incidents will help guide policy, as it is likely that sensitive sectors such as healthcare and social security will require a higher standard of compliance in view of the nature of their operations and risk assessment.

We expect some regulatory developments proposed by the government to further energise compliance. The National Cyber Security Strategy 2020 is a long-awaited policy initiative of the government, and it is hoped that better security standards and priority allocation will be the norm after it is notified. The Guidelines on Regulation of Payment Aggregators and Payment Gateways require payment aggregators to implement security standards and best practices that will benefit the financial technology sector in India.

The proposed personal data protection legislation will also play a critical role in shaping the regulatory environment in relation to the protection of personal data, as it seeks to prescribe the security safeguards to be implemented by data fiduciaries (data controllers that determine the purpose and means of processing of personal data), which includes the use of methods such as de-identification and encryption, steps necessary to protect the integrity of personal data, and steps necessary to prevent the misuse, modification, disclosure or destruction of, or unauthorised access to, personal data.

LAW STATED DATE

Correct On

33 | Give the date on which the information above is accurate.

09 December 2021.

* *The authors wish to thank Shagun Badhwar, Senior Associate and Suyash Tiwari, Associate for their assistance in the preparation of this chapter.*

Italy

Paolo Balboni, Luca Bolognini, Valerio De Feo, Francesca Tugnoli and Francesco Capparelli*

ICT Legal Consulting

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Italy, there are a number of regulations that guide the management of cybersecurity practices. Within the framework of the regulations applicable in Italy, the following should be mentioned.

- Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR) and Legislative Decree 196/2003, (Italian Personal Data Protection Code, dated 30 June 2003) regulate specific aspects of personal data protection in Italy. This legislation contains a number of rules, including article 32 GDPR and other specific provisions regarding the security measures to be applied for the processing of health-related personal data (article 2-septies Personal Data Protection Code), which require data controllers to adopt technical and organisational measures to protect personal data on the basis of the risks underlying the processing operations carried out. To be able to demonstrate that technical measures to protect data have been adopted, data controllers are required to identify and map possible IT risks and strengthen their cybersecurity resilience.
- Legislative Decree 51/2018, dated 18 May 2018, which transposed Directive (EU) 2016/680 in Italy. This legislative decree contains a series of requirements to regulate the adoption of security measures with respect to the protection of data processed by law enforcement agencies in the context of judicial police activities.
- Legislative Decree 231/2001, dated 08 June 2001, which concerns the criminal liability of companies and constitutes an indirect safeguard for the implementation of cybersecurity measures, as it requires companies to adopt protocols aimed at preventing the commission of computer crimes.
- Decree-Law No. 105/2019, dated 21 September 2019, on the 'National Cybersecurity Perimeter', which dictates a set of measures aimed at ensuring a high level of security of the networks, information systems and IT services of public administrations, as well as national, public and private entities and operators, through the establishment of a National Cybersecurity Perimeter and the provision of appropriate measures to ensure the necessary security standards aimed at minimising risks while allowing for the most extensive use of the most advanced tools offered by information and communication technologies. This Decree-Law has been followed by Prime Ministerial Decree No. 131/2020, dated 30 July 2020, which establishes the criteria to identify operators subject to the obligations of the National Cybersecurity Perimeter. To implement and regulate specific processes within the established framework, Presidential Decree No. 54 of 5 February 2021 was issued. In particular, the Presidential Decree identifies procedures and methods to be followed to mitigate supply chain attacks. The purpose of the assessments, carried out by entities providing essential services for the state, identified pursuant to Prime Ministerial Decree 131/2020 and the established National Evaluation Centre, is to identify and mitigate risks arising from the supplier of the subjects. Entities included in the 'perimeter' are required to notify the National Evaluation Centre of their intention to initiate procurement procedures in relation to ICT goods, systems and services. Presidential Decree No. 54/2021 also includes the procedures and methods by which the competent authorities carry out verification and inspection activities for the purpose of assessing compliance with the obligations set forth in Decree-Law 105/2019. In conclusion, Presidential Decree No. 54/2021 also provides for the issuance of a subsequent Prime Ministerial Decree which, following the directive criteria set out in article 13 of the same Presidential Decree, would identify in detail the categories of ICT goods, systems and services in relation to which the entities included in the perimeter will be required to make the notification to the CVCN. To set up a series of controls to assess the compliance of the supplier, audits and risk assessment must be carried out by the entities that fall under the perimeter.
- Legislative Decree 65/2018, dated 18 May 2018, which transposed Directive EU 2016/1148 (NIS Directive), providing guidance on risk management and the prevention, mitigation and notification of cyber incidents and attacks.

With regard to the public sector, mention should be made of the Three-Year Plan for IT in Public Administration (2020–2022), Chapter 6 of which is entirely dedicated to IT security.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Healthcare, banking and finance, together with sectors closely related to national security (defence, energy, telecommunications, etc) are the most regulated sectors in Italy from a cybersecurity perspective.

However, the covid-19 pandemic has forced companies in almost all sectors to move to smart remote working. Due to the nature of the emergency situation, however, in many cases adequate technical checks were not carried out to ensure that IT security was sufficiently taken into consideration. On the contrary, the forced and impromptu use of previously less-used tools and ways of working has created new opportunities for cyber criminals who, thanks to the vulnerabilities inherent in the new tools, have multiplied their attacks over the past year, which is why many companies in all sectors are making significant investments in IT security.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

In 2015, the National Cybersecurity Framework was presented, the result of collaboration between academia, public bodies and private companies. The Framework, inspired by the Cybersecurity Framework devised by the National Institute of Standards and Technology, provides an operational tool for organising cybersecurity processes suitable for public and private organisations of all sizes. With the entry into force of EU Regulation 679/2016 and the change in approach it has brought about, a new version of the National Framework for Cybersecurity and Data Protection has been introduced, a tool to support organisations that need strategies and processes aimed at personal data protection and cybersecurity.

Through the Italian standards agency (Ente Italiano di Normazione), Italy has adhered to the most important ISO international security standards.

In addition, the Agency for Digital Italy (AgID) has accredited CSA STAR certification as the only alternative to ISO 27001 certification (integrated with ISO 27017 and 27018) to certify the security of software as a service cloud services for the Italian Public Administration.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

A company may be liable both for failure to adopt adequate safeguards and for lack of controls. This may have an impact from an administrative point of view, as the Italian Data Protection Authority (DPA) may impose a fine on the company that has failed to adopt adequate security measures, and from a criminal point of view deriving from the failure to adopt suitable protocols to prevent the commission of computer crimes.

In the latter case, the liability of the responsible personnel and directors in the case of inadequate cybersecurity may be recognised in the new criminal offence introduced by article 24-bis 'Computer crimes and unlawful data processing' of Legislative Decree No. 231/2001.

The introduction of computer crimes and unlawful data processing in the list of offences set out in Italian Legislative Decree No. 231/2001 makes it necessary to carry out an analysis in relation to the relevant risks associated with the company's operations. At the same time, it will be fundamental to identify the necessary safeguards and assess any actions required for the appropriate updating of the Organisation and Management Model pursuant to the aforementioned legislative decree.

In addition to forms of liability of the entity, however, there is also the liability of the individual employee who has acted in breach of the rules of the company's code of ethics and organisational and management model, which may lead to the imposition of disciplinary sanctions provided for therein.

The proactive and risk-based approach also requires the provision of training plans that are suitable for disseminating the measures adopted within the corporate structure.

5 How does your jurisdiction define cybersecurity and cybercrime?

Article 3 of Legislative Decree 65/2018 defines cybersecurity, or 'network and information system security' as the ability of a network and information systems to withstand, at a given level of confidentiality, any action that compromises the authenticity, integrity or confidentiality of data stored or transmitted or processed and of the related services offered or accessible through such network or information systems.

Cybercrimes are defined as any crime committed with an information system, enlisted under the provision of articles 615-ter to 615-quinquies, 635-bis to 635-quinquies, 640-ter and 491-bis et seq of the Italian Criminal Code.

Data Privacy is to be intended as the protection of natural persons in relation to the processing of personal data and is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her. Cybersecurity is an integral part of the protection of personal data, but it also extends to information that is not related to an identified or identifiable natural person.

In any case, personal data privacy, cybersecurity and criminal provisions are strictly interconnected. Only if a company has an adequate system of security measures can it prevent cybercrimes. In Italy, the same conducts that are punished as cybercrimes could result in a liability for the companies themselves if they are committed to the advantage of the legal entities (as provided for in Legislative Decree 231/2001).

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

While the Italian legislator adopted the risk-based approach as provided for in article 32 of the GDPR regarding personal data security, specific provisions are included within the Italian Personal Data Protection Code. Further provisions regarding special categories of personal data are also found in the guidelines of the Italian DPA. However, the actual definition of security measures to be implemented is contained in old provisions of the relevant legislation, which need to be updated, or is delegated to future sectorial regulation yet to be issued.

The same approach may be found in Legislative Decree 65/2018, in particular in article 14 where criteria to assess the security measures to be applied are included. However, the evaluation of the precise security measures adopted is left to the discretion of the specific operator.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The legal framework of cyberthreats to intellectual property (IP) can be broadly differentiated between:

- legal provisions that discipline the protection of IP assets that were originally conceived in an offline scenario, in whose context cyberthreats to intellectual property represent a new technological way to carry out an attack on third-party IP owners and assets; and
- legal provisions that identify specific cyberthreat conduct as an administrative or criminal offence, that may also eventually (yet not necessarily) result in a violation of third-party IP rights.

Among the first group it is possible to include, inter alia:

- Legislative Decree No. 30/2005, dated 10 February 2005, (Italian Code of Industrial Property); just by way of example, cyberthreats might result in the illegal gathering, use or disclosure of confidential information of a competitor (articles 98–100); likewise, the disclosure is not to be taken into account in determining the novelty of a design or a patent if it occurred due to an abuse to the prejudice of the applicant (eg, by means of a cyberthreat) (articles 34 and 47);
- provisions on intellectual property rights set forth in the Italian Civil Code (articles 2569 to 2594);
- specific provisions of the Italian Criminal Code that identify criminal offences pertaining to intellectual property assets (eg, disclosure

of trade secrets or scientific inventions, known by reason of office (article 623); unlawful use of third-party trademarks, marketing of counterfeit products (articles 473, 474 and 517-ter); and

- Law No. 633/1941, dated 22 April 1941, (the Italian Copyright Law), to the extent an unlawful exploitation of copyrightable works of a third party is committed by means of a cyberthreat; and the Italian Communications Regulatory Authority Regulation dated 31 March 2014 on the protection of online intellectual property pursuant to Legislative Decree No. 70/2003, dated 09 April 2003.

On the other hand, the Italian legal framework also identifies provisions that identify certain cyberthreats as an administrative or criminal offence, that might also eventually (yet not necessarily) amount to or otherwise be aimed at perpetrating a violation of third-party IP rights. Reference can be made in particular to:

- Provisions of the Italian Criminal Code, such as unlawful access to computer systems (article 615-ter); detention, disclosure or dissemination of keywords, access codes or any other means to access a protected computer or telematic system, or providing any assistance in support thereof (article 615-quater); unlawful possession or distribution of access codes to IT systems (article 615-quater); distribution, offering or sale of devices or software tools having the purpose of damaging computer, telematic system, information, data or software programs contained therein (article 615-quinquies); unlawful interception and destruction of communications articles 616 and 617); damage to information, data, software programs or IT systems of a third party (articles 635-bis to 635-quinquies); computer fraud (article 640-ter).

On 29 November 2021, Legislative Decree No. 184/2021 introduced into the Criminal Code the new crimes under article 493-ter (undue use and falsification of non-cash payment instruments) and article 493-quater – (possession and diffusion of equipment, devices or computer programs aimed at committing offences regarding payment instruments other than cash), and a new aggravating circumstance to computer fraud as per article 640-ter penal code, in the case that alteration of the computer system determines a transfer of money, monetary value or virtual currency. Some of these new crimes have become relevant also under Legislative Decree No. 231/2001.

- Provisions of the Italian Copyright Law that prohibit conducts, including cyberthreats, perpetrated either to bypass the technical protection measures implemented by a legitimate right holder to prevent access by unauthorised users to copyrighted works (even if no explicit mention is made to cyberthreats: eg, articles 102-quater and 102-quinquies), or violate the scope of copyright exceptions and limitations (eg, illustration for teaching, public security, etc: articles 70 and the following of Italian Copyright law). Some of the aforementioned conduct constitutes a criminal offence, such as the importation, distribution or sale of computer programs or any means, the sole intended purpose of which is to allow or to facilitate the unauthorised removal or circumvention of any technical device applied to protect a computer program (article 171-bis); the broadcast, by whatever means, of 'an encrypted service received by means of devices or parts of devices capable to decode the conditioned-access transmissions' (article 171-ter, paragraph 1, letter e); the distribution, sale or set-up of special devices or decoding elements that allow to have access to an encrypted service without paying the due subscription fee (letter f); the production, import, distribution or sale of products or services whose main purpose is to circumvent any effective technological measures, or which are primarily designed or performed for enabling or facilitating any such circumvention (letter f-bis); unlawful removal or altering of the electronic rights-management information under article 102-quinquies, or distribution of protected works or other subject matter whose electronic information has been removed or altered (letter h).

Cybercrimes that affect intellectual property rights, where performed by the representatives of organisations or subjects under the latter's authority, are also relevant for the purposes of Legislative Decree No. 231/2001 on corporate criminal liability, if and to the extent the relevant criminal offences were committed either in the company's interest or for the company's benefit, while no corporate liability occurs where directors, managers or individuals subject to direction and coordination of the former acted exclusively in their own (or a third party's) interest.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Prime Ministerial Decree No. 131/2020, implementing Decree-Law No. 105/2019 concerning the National Cyber Security Perimeter, entered into force on 5 November 2020, thus laying the first concrete foundations of the Italian National Cyber Security Perimeter.

Entities that are included in the Perimeter must carry out important tasks, such as updating the list of ICT assets annually; carrying out risk analyses to identify the risk factors of incidents; managing and implementing necessary security measures; indicating the ICT assets it needs; and the related risk analysis to ensure the integrity, efficiency and security of the data and information they contain. In addition, obstructing or conditioning the inspection and verification activities carried out within the Perimeter may lead to criminal liability.

Legislative Decree 65/2018 transposed Directive EU 2016/1148 (NIS Directive), providing guidance on risk management and the prevention, mitigation and notification of cyber incidents and attacks.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Italian Criminal Code and Personal Data Protection Code contain provisions aimed at preventing the dissemination of confidential information. In fact, article 615-ter et seq of the Criminal Code contains provisions on computer offences in relation to a series of criminal offences committed by means of computer systems, such as abusive access to a computer system; the dissemination of equipment, devices or computer programs intended to damage or interrupt a computer or telecommunications system; computer fraud; and other offences in the illicit use of payment instruments.

Specific provisions of the Italian Criminal Code that identify criminal offences pertaining to intellectual property assets may also come into play.

With reference to the criminal law on privacy, the incriminating provisions are contained in the Italian Personal Data Protection Code. In particular, the entire second Chapter of the third Title of the Personal Data Protection Code is dedicated to criminal offences, such as the unlawful communication and dissemination of personal data subject to large-scale processing or the communication of a personal data database (or a substantial part of it) of personal data subject to large-scale processing without consent, when consent is required for the data processing activity.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal crimes punished in the Italian Criminal Code concern abusive access to the computer system (under the provision of article 615-ter), damage to computer systems (articles 635-bis and 635-quarter) and computer fraud (article 640-ter), also when committed with the alteration of the computer system that determines a transfer of money, monetary value or virtual currency. Under these provisions, the most important forms of cybercrimes that can be committed by company employees or by cybercriminals are criminalised, such as unauthorised access to an employee's email account, phishing or ransomware. The illicit use of payment instruments that could be the result of phishing activities and ransomware viruses is punished.

Additionally, article 24-bis 'Computer crimes and unlawful data processing' of Legislative Decree 231/2001 punishes companies where the same criminal conduct indicated above has been committed in the interest of and to the advantage of the company.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

No specific rules have yet been issued in Italy for the private sector. In any case, ISO 27017 and 27018 contain precise security controls to be followed by those offering cloud services and to ensure that both customer and supplier data are processed in a safe and secure environment.

For the public sector, the AgID has accredited CSA STAR certification as the only alternative to ISO 27001 certification (integrated with ISO 27017 and 27018) to certify the security of SaaS cloud services for the Italian Public Administration. Moreover, the three-year plan for IT in public administration for 2020–2022 expressly mentions the use of cloud systems.

To date, therefore, apart from the above indications, no specific requirements have been issued to operators offering cloud services.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Italian cybersecurity laws do not provide any specific distinctions for foreign organisations.

Any company that does business in Italy falls within the applicability of the cybersecurity legislation mentioned in this chapter and shall comply with the same obligations as Italian companies. Regulatory obligations are generally aligned with European legislation and international standards; however, foreign organisations must be aware of and also comply with the specific national requirements.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Cyber Security Framework introduces a series of useful controls depending on the type of business (small or medium-sized enterprise). In addition, since July 2019, as required by the Network and Information Security (NIS) Directive and Legislative Decree 65/2018, Italy has added a new instrument for national cybersecurity, the guidelines on risk management and the prevention, mitigation and notification of cyber incidents and attacks, which have been shared with the operators of essential services. Moreover, the Agency for Digital Italy (AgID) has accredited CSA STAR certification as the only alternative to ISO 27001 certification (integrated with ISO 27017 and 27018) to certify the security of software as a service cloud services for the Italian Public Administration.

14 How does the government incentivise organisations to improve their cybersecurity?

Transition 4.0 (formerly Industry 4.0) is the national plan that provides for a series of facilities to help the Italian entrepreneurial system face the challenge of the fourth industrial revolution.

A further strengthening of the Transition 4.0 plan has also been provided for in the Budget Law 2021 It includes measures to develop cybersecurity. The Transition 4.0 three-year plan provides for:

- the replacement of the former hyper-depreciation in tax credit for 4.0 assets; and
- the replacement of the former super-depreciation into a tax credit for tangible capital goods, with an increase in the rate from 6 to 10 per cent. In the case of assets useful for smart working, the rate will increase to 15 per cent, at least for the first year.

In addition, some further incentives have been provided, such as:

- a 'Call for proposals' by the MADE Competence Center to finance projects of innovation, industrial research and experimental development on the themes of Industry 4.0;
- a notice by MISE 'Digital Transformation' to support the technological and digital transformation of the production processes of SMEs through the realisation of projects directed to the implementation of the enabling technologies identified in the National Plan Impresa 4.0 as well as other technologies related to digital technological solutions of the chain; and
- from Simest (a mostly state-owned company):
    - financing for digital and ecological transition for SMEs with an international focus. Thanks to PNRR (the Piano Nazionale di Ripresa e Resilienza, the plan prepared by Italy to relaunch its economy after the covid-19 pandemic to permit the green and digital development of the country) funds, Simest has launched a new financing tool for SMEs for the realisation of investments aimed at favouring the digital (at least 50 per cent of the financing) and ecological transition of SMEs and strengthening their competitiveness in foreign markets; and
    - financing for e-commerce abroad. Thanks to PNRR funds, Simest supports the realisation of digital investment projects of SMEs for the creation or improvement of a proprietary e-commerce platform (dedicated) or access to a third-party platform (marketplace) for the marketing of goods or services produced in Italy or with an Italian brand; and
    - a call for Temporary Export Management: digital vouchers for the internationalisation of manufacturing companies.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

AgID is responsible for implementing the objectives of the Italian Digital Agenda, in accordance with the guidelines laid down by the President of the Council of Ministers or the Minister delegated to him or her, and with the European Digital Agenda. In particular, AgID promotes digital innovation in the country and the use of digital technologies in the organisation of the public administration and in the relationship between the latter and citizens and businesses, in compliance with the principles of legality, impartiality and transparency and according to criteria of efficiency, cost-effectiveness and effectiveness.

It collaborates with the institutions of the European Union and carries out the tasks necessary for the fulfilment of the international obligations assumed by the state in the matters for which it is responsible. AgID set out a series of obligations to promote cybersecurity in the Public Administration such as the Minimum ICT security measures, which are a practical reference for assessing and improving the level of IT security of administrations to combat the most frequent IT threats. Depending on the complexity of the information system to which they refer and the organisational reality of the Administration, the minimum measures can be implemented in a gradual manner following three levels of implementation.

16 | Are there generally recommended best practices and procedures for responding to breaches?

The most suitable standard in information security to deal with a cybersecurity incident is ISO/IEC 27035:2016. From a risk perspective, this standard should be only a model for the organisation to start its compliance process.

Furthermore, the indications coming from the Data Protection Authority (DPA) (many of which are collected on this page) constitute an important guide and indication for the correct management of security incidents.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Article 18 of Legislative Decree 65/2018 encompasses the conceptual core of the regulatory framework. As the purpose of the NIS directive is to foster the resilience of the European information system, the basis of this resilience can only be identified in the necessary information sharing that allows a multi-sectoral and proactive approach to cybersecurity issues, creating a climate of cooperation and unity.

The provision in article 18 of Legislative Decree 65/2018 provides that those who have not been identified as operators of essential services and are not providers of digital services may equally voluntarily notify any incidents that have occurred that have generated a significant impact on the continuity of the services they provide. An organisation that has IT systems and infrastructure similar to those of an essential service operator or a digital service provider, by notifying incidents, will allow the competent NIS authorities and the Italian Computer Security Incident Response Team (CSIRT) to take preventive action to avoid incidents that could compromise the continuity of services considered of fundamental importance to citizens. Voluntary notification is, therefore, not an instrument of self-reporting but intended to prevent the possibility that known vulnerabilities on the European territory are exploited to the detriment of the essential and digital services within the Union.

In addition, the Whistleblowing Directive (1937/2019), which must be transposed in Italy by 17 December 2021, provides for the companies with more than 50 employers to create a system dedicated to the reporting of facts committed by a company in violation of EU law (ie, for all areas of EU competence). People who make such reports are granted some forms of protection. In addition, the EU member states should provide a 'public' channel to allow reporting if the internal channels are not available or are unsuitable.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The first of the implementing regulations of Decree-Law No. 105/2019, concerning the National Cybersecurity Perimeter, Prime Ministerial Decree No. 131/2020, provides for the establishment of an inter-ministerial platform, in which representatives of public and private entities and operators may be called upon to offer their expertise.

In addition, Legislative Decree 65/2018 established the CSIRT, whose operation is regulated by the Prime Ministerial Decree of 8 August 2019. The CSIRT, in addition to intervening in the event of cyber incidents and monitoring their frequency at the national level, promotes the adoption and use of common or standardised practices in the areas of incident and risk-handling procedures and incident, risk and information classification systems.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Yes, there are insurance policies that cover cybersecurity breaches, and they are usually included in the broader coverage related to personal data protection. Typically, policies cover various risks such as those related to cyber-attacks or failures (including malware, cybercrime, unauthorised data dissemination and unauthorised data operations) that can also result in data breaches (ie, loss of control of personal data). They also cover cybersecurity and losses resulting from events such as cyber terrorism and cyber-attacks, including abusive access to computer systems, but also human error (operational or in IT management) of employees. Moreover, they cover service interruptions and access interruptions (including due to internet outages). The coverage typically offers the cost of restoring computer systems and compensates for the direct economic loss resulting from business interruption due to flaws in computer security and arising from malicious use of or access by third parties to the computer systems. Policies usually require a careful risk assessment before calibrating the cost of coverage. More widespread use of these policies has been seen with the entry into force of the General Data Protection Regulation, which imposes very high fines, allows for damage recovery (eg, when caused by lack of data security) and, more specifically, in article 32 requires the adoption of adequate security measures to protect personal data. In fact, risk coverage is often subject to the policyholder maintaining the security measures required by the data protection regulations.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

As far as the designation of competent authorities for the implementation and supervision of the Network and Information Security (NIS) Directive legislation is concerned, the institutional model chosen by the Italian government is highly decentralised. In fact, five ministries are designated as 'competent NIS authorities': Economic Development; Infrastructure and Transport; Economy and Finance; Health and Environment; and Land and Sea Protection. Each ministry is responsible for one or more sectors falling within its areas of competence, as well as, for certain limited areas, the Italian regions and autonomous provinces.

The main Italian authority in charge of the prosecution of cybercrimes is the Prosecutor's Office, assisted by the police and in particular the Postal Police.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Italian Department of Security Intelligence (DIS) is designated as the single point of contact under article 8(3) of the NIS Directive. The DIS is, therefore, responsible for liaising with the EU and coordinating with cybersecurity authorities in other member states.

Legislative Decree 65/2018 has also provided for the establishment at the Presidency of the Council of Ministers of a single Computer Security Incident Response Team, called the Italian Computer Security Incident Response Team (CSIRT), to perform tasks related to the prevention of and response to computer incidents, carried out in cooperation with other European CSIRTs.

The CSIRT offers a number of services in response to reports received. These include:

- reactive services:
  - alerts and warnings
  - incident management and analysis; and
  - vulnerability management;
- proactive services:
  - review and assessment of security levels;
  - configuration and maintenance of security;
  - development of security tools; and
  - dissemination of security-related information; and
- security quality services:
  - risk analysis;
  - support for business continuity and disaster recovery activities; and
  - awareness raising and training.

The Italian Data Protection Authority (DPA) through the Special Unit for the Protection of Privacy and Technological Fraud of the financial police, has the power to investigate compliance with data protection law. For example, it may be verified if the company has adopted adequate measures to prevent risks to the rights of individual, pursuant to article 32 General Data Protection Regulation (GDPR).

The Italian Personal Data Protection Code has also introduced a new form of cooperation between the Judicial Authority and the Italian DPA. Therefore, in the context of the respective activities of investigation it is possible that, where relevant facts emerge on the criminal side or on the privacy side, the file is immediately transmitted to the competent authority.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

At present, cybersecurity enforcement in Italy is mainly conducted by the Italian DPA, as the approval of dedicated cybersecurity laws is still relatively recent.

The Italian DPA has issued a number of notable fines for data breach violations. Among them, a fine of €600,000 has been issued to one of the leading Italian banks following a complex investigation into a data breach caused by abusive access to the personal data of over 700,000 customers. The Italian DPA determined the failure of the bank to adopt adequate technical and organisational measures.

Another example is the €27.8 million fine for one of the leading national telecommunication operators for several instances of unlawful data processing in relation to marketing activities that affected millions of data subjects. In this case, the DPA found that there was also a breach of the provisions that aim to guarantee the integrity and confidentiality of systems by way of suitable technical and organisational measures.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

The provisions of article 33 GDPR are also taken into account, where applicable, by article 13 Legislative Decree 65/2018, which outlines a framework for cooperation between the competent NIS authority and the Italian DPA in the event of security incidents that also include personal data breaches. This measure would, therefore, entail a double notification if a security incident results in a personal data breach. The operator is called upon to notify the DPA under article 33 GDPR and the competent NIS authority under articles 12 and 14 of Legislative Decree 65/2018.

Regarding data subjects, the notification of a data breach is regulated under article 34 GDPR. The Italian DPA recently released a self-assessment tool on its website to help controllers and processors evaluate the necessity to notify the breach to the DPA and to data subjects.

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

In the transposition of article 21 of the NIS Directive in Italian legislation, it should be noted that penalties of a criminal nature have been excluded from the list of penalties that may be imposed. Article 21 does not distinguish between the types of penalties that may be imposed, allowing member states a wide margin of discretion in that regard.

Furthermore, pursuant to article 15 Legislative Decree 65/2018, sanctions may be applied, at least for digital service providers, only after the demonstration of non-compliance, since only in the event of this condition will the NIS competent authorities be able to activate their verification powers.

Article 21 of Legislative Decree 65/2018 lists the sanctions that can be imposed by prioritising their commensuration subject to the occurrence of various circumstances. The administrative fines, ranging from €12,000 to €150,000, are provided for operators of essential services where they fail to adopt adequate and proportionate technical and organisational measures, to notify to the Italian CSIRT of incidents having 'a significant impact on the continuity of the essential services provided' or to comply with the instructions issued by the competent authority.

Moreover, if the breach is caused by a computer crime committed in the interest and to the advantage of the entity and this is due to the lack of adequate security measures, this may entail, in addition to the administrative sanctions referred to above, criminal liability under article 24-bis of Legislative Decree No. 231/2001.

Lastly, article 83 GDPR provides the administrative fines for non-compliance with article 32 GDPR regarding the application of the security measures to the processing of personal data.

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Article 21 of Legislative Decree 65/2018, and specifically paragraphs 3, 6, 7, regulates in the case of a failure to notify by an essential service operator or a digital service provider.

- Paragraph 3 punishes the failure to notify the Italian CSIRT of incidents having a significant impact on the continuity of the essential services provided. The penalty is a pecuniary administrative sanction ranging from €25,000 to €125,000.

- Paragraphs 6 punishes the failure by a digital service provider to notify an incident to the CSIRT with a fine ranging from €25,000 to €125,000.
- Paragraph 7 regards the lack of notification of incidents that affected third parties that provides the operator of essential services with the digital services necessary for the provision of a service that is indispensable for the maintenance of fundamental economic and social activities. The sanction in this case is an administrative fine ranging from €12,000 to €120,000.

Moreover, although not strictly determined by the mere presence of a data breach, when the data breach is determined by a computer crime committed in the interests and to the advantage of the entity and this is due to the lack of adequate security measures, this may entail not only the administrative sanctions mentioned above, but also criminal liability under article 24-bis of Legislative Decree No. 231/2001.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Depending on their nature as a legal or natural person, any party that believes itself to have been damaged by an unauthorised cyberactivity or failure to adequately protect systems and data may seek redress by bringing the matter to court or reporting the violation to the relevant authority.

Where the matter concerns personal data, the data subject may always lodge a complaint with the DPA or file a court case.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

It is advisable for companies to put a comprehensive cybersecurity framework in place to address any specific risks and to have a comprehensive approach to possible threats. Such a framework shall at least include policies and procedures on information security, access control, asset management, cryptography, network management, third-party management and business continuity.

Under article 14 of Legislative Decree 65/2018 (in relation to digital service providers) and article 32 GDPR, companies must demonstrate that they have put in place all appropriate technical and organisational measures to prevent risks to the freedoms and rights of data subjects.

Furthermore, the last Confindustria Guidelines for the creation of a Model of Organisation, Management and Control in accordance with Legislative Decree 231 of 8 June 2001 specified that companies must promote integrated forms of compliance, including in the field of cybersecurity, so that all the IT and security procedures put in place are coordinated with each other and suitable to protect the company from all possible forms of liability.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Without prejudice to the documentation obligations provided for by the GDPR (article 33 article 5) where an attack or incident has led to a personal data breach, Legislative Decree 65/2018 provides for security incident reporting obligations for essential service operators and digital service providers. Because under articles 13 and 15 these entities must provide the 'competent NIS [Network and Information Security] authorities' (ie, the ministries indicated in article 7) with the information necessary to assess the security of their network and information systems, including documents relating to security policies, it can be indirectly inferred that they need to keep track of incidents that have occurred, and the countermeasures adopted.

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Legislative Decree 65/2018 provides for a specific notification obligation for digital service providers and operators of essential services in articles 12 and 14. These are required to notify the CSIRT and the competent NIS authority of any incidents with a significant impact on the provision of their services. To determine the significance of the impact, the following shall be taken into account:

- the number of users affected by the incident, in particular users who depend on the digital service for the provision of their services;
- the duration of the incident;
- the distribution in geographical terms of the area affected by the accident;
- the extent of the disruption to the operation of the service; and
- the extent of the impact on economic and social activities.

While not being required to, companies that fall outside of the scope of Legislative Decree 65/2018 may notify cybersecurity breaches to the Italian CSIRT on a voluntary basis (article 18 of the same legislative decree).

Any cybersecurity breach that involves personal data shall be notified to the Italian Data Protection Authority (DPA), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The notification must include:

- the name of the organisation;
- the time at which the incident occurred;
- the duration of the incident;
- information regarding the impact and nature of the incident;
- information regarding any transnational impact; and
- any other information that may help the CSIRT to determine the relevance of the incident.

To facilitate the notification process, the Italian CSIRT has prepared a notification template and provided instructions on the same on the dedicated website.

The notification is to be considered confidential and will be forwarded through protected channels via the above-mentioned website.

Time frames

30 What is the timeline for reporting to the authorities?

Organisations that fall within the Perimeter must adopt a comprehensive process for security management that starts from the prevention or identification of events and ends with their management and reporting. This process must involve technological, procedural and organisational aspects and is composed of various activities, including cyber threat intelligence (collection, analysis, attribution or reporting); implementation of incident management policies and procedures (detection, analysis, classification, response, eradication, recovery, closing, notification or lessons learned); and implementation of operations centres or control rooms dedicated to the management and monitoring of cybersecurity events (eg, SOC or CERT).

In addition, the GDPR requires that in the event of a personal data breach, the Authority must be notified of the incident within 72 hours.

Reporting

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Articles 33 and 34 of the GDPR require that security incidents in which it is likely that the breach may result in risks to the rights and freedoms of data subjects are notified to the DPA and the data subjects. Pursuant to article 28 GDPR, the processor shall promptly inform the controller of security incidents that have occurred.

Moreover, according to article 12 of the NIS Directive, operators of essential services shall notify the Italian CSIRT without undue delay and, for their information, the competent NIS authority, of incidents having a significant impact on the continuity of the essential services provided. The Italian CSIRT then promptly forwards the notifications to the body set up at the Security Intelligence Department in charge of any crisis situations.

UPDATE AND TRENDS

Key developments of the past year

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Check Point Research, the Threat Intelligence division of Check Point Software Technologies, a global cybersecurity solutions provider, has announced that cyber-attacks in 2021on businesses worldwide rose by 40 per cent compared with 2020, with losses of $6 trillion by 2021. According to the Clusit report published in October 2021, while in 2020 'critical' impact attacks accounted for 13 per cent of the total and 'High' impact attacks accounted for 36 per cent, in the first half of 2021, critical and high impact attacks accounted for 74 per cent of attacks. The great challenge of the pandemic requires investing heavily in cybersecurity. That is why, in July 2020, the European Commission issued a strategy document aiming for an effective and coordinated approach to rapidly evolving threats over the next five years. In particular, to take action against hybrid threats (ie, those posed by physical and digital means) some priorities and guiding principles have been indicated. Among these, collaboration between the private and public sectors is paramount. The first step in this approach was made through the issue of the Network and Information Security Directive (NIS Directive).

An important step towards an integrated framework for cybersecurity at European level has been taken thanks to the General Data Protection Regulation and the NIS Directive. Nevertheless, Italy has decided to create a further standard, the Cybersecurity Perimeter, which has effectively extended the scope of the NIS Directive. In this sense, the extension of the subjects included among the organisations subject to the NIS Directive and a strengthening of the security measures aimed not only at reporting incidents but above all at their prevention, is fundamental.

* *Antonio Landi and Alessandro Fratini also contributed to this chapter.*

Paolo Balboni
paolo.balboni@ictlc.com

Luca Bolognini
luca.bolognini@ictlc.com

Valerio De Feo
valerio.defeo@ictlc.com

Francesca Tugnoli
francesca.tugnoli@ictlc.com

Francesco Capparelli
francesco.capparelli@ictlc.com

Via Borgonuovo, 12
20121 Milan
Italy
Tel: +39 02 84247194
Fax: +39 02 700512101
www.ictlegalconsulting.com

Japan

Masaya Hirano and Kazuyasu Shiraishi

TMI Associates

LEGAL FRAMEWORK

Legislation

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Japan has a dedicated cybersecurity law called the Basic Act on Cybersecurity, which was enacted on 6 November 2014 and promulgated on 12 November 2014.

Ensuring cybersecurity while also guaranteeing free distribution of information is a pressing task for Japan. In light of such circumstances, the principal purpose of the Basic Act on Cybersecurity is to move cybersecurity-related policies forward in a comprehensive and effective manner and to contribute to the creation of a more energetic and continuously developing economic society, as well as the national security of Japan.

Owing to increased threats to cybersecurity, the Basic Act on Cybersecurity was amended on 5 December 2018 and became effective on 1 April 2019, with a view to further ensuring cybersecurity in Japan and to fully preparing Japan to host the Tokyo 2020 Olympic and Paralympic Games (held in 2021). The principal amendments are as follows.

- A cybersecurity council will be established to enable various public and private entities to mutually cooperate in sharing cybersecurity information and discussing necessary countermeasures, etc. It is planned that the members of the council will be representatives of national and local administrative organs, principal infrastructure and cyber entities, educational and research institutions, experts and others.
- Additional operations will be handled by the Cyber Security Strategy Headquarters in communicating and making adjustments with parties inside and outside Japan upon the occurrence of cybersecurity incidents.

The Basic Act on Cybersecurity is a basic law, and specific provisions regarding cybersecurity are set forth in relevant laws and regulations.

At present, Japan has substantive laws that cover cybercrime issues, such as the:

- Personal Information Protection Act;
- Penal Code;
- Unauthorised Computer Access Prohibition Act;
- Unfair Competition Prevention Act;
- Copyright Act;
- Telecommunications Business Act;
- Specially Designated Secret Protection Act;
- Basic Act on the Formation of a Digital Society (renamed from 'Basic Act on the Formation of an Advanced Information and Telecommunications Network Society' on 1 September 2021);
- Act on Electronic Signatures and Certification Business; and
- Act on Facilitation of Information Processing.

Through the amendments and enactments of the above laws, the policies and regulations related to cybersecurity and penal law provisions for respective cybercrimes, etc have been established one after another in a manner of following the progression of the information and communications society.

In addition to cybercrime legislation, the Personal Information Protection Act was enacted in 2003 from the perspective of ensuring information security. Further, the Social Security and Tax Number Act was enacted in 2013.

The Personal Information Protection Act relates to information security, and more specifically to the proper handling of personal information, rather than to cybersecurity. Although the current Personal Information Protection Act prescribes concrete duties of a business operator handling personal information as prescribed in article 2, paragraph 5 (personal information-handling business operator), it does not prescribe concrete duties of administrative organs, independent administrative agencies and local governments. The concrete duties of administrative organs are prescribed in the Act on the Protection of Personal Information Held by Administrative Organs; those of independent administrative agencies are prescribed in the Act on the Protection of Personal Information Held by Independent Administrative Agencies, among others; and those of local governments are prescribed in privacy protection ordinances enacted by each local government. However, this framework has been amended (promulgated on 19 May 2021) to integrate these two laws with the Personal Information Protection Act and convert the three laws into one law, which is due to come into force on 1 April 2022. In addition, the integrated law also stipulates nationwide common rules regarding local government personal information protection systems, which are due to come into effect within two years from 19 May 2021. Accordingly, the Personal Information Protection Commission, as an independent regulatory body, will have overall administrative jurisdiction in a centralised manner.

The amended Personal Information Protection Act sets forth that the Act shall be reviewed every three years. Consequently, the Act was amended in June 2020, and, except for some of the provisions including strengthened penal provisions, has already come into force and the remaining provisions will fully come into force on 1 April 2022. The principal amendments made therein are outlined below.

- Regarding personal rights:
  - in regard to personal rights to demand discontinuation of use, removal, etc, of personal data, making such a demand will be possible if any personal rights or due interests may be harmed, in addition to cases where there is some violation of the law, including unauthorised acquisition thereof, etc;
  - in regard to the manner of disclosure of retained personal data, the data subject may issue instructions for the manner

of disclosure, including by way of providing electromagnetic records or delivering documents (digitalised manner of disclosure);
    - data subjects may demand disclosure of the records regarding a third party's provisions of personal data where there is an obligation to keep records for traceability;
    - short-term storage data that will be removed within six months shall be included in personal data subject to disclosure, discontinuation of use, etc; and
    - the scope of personal data that can be provided to any third party in accordance with the opt-out provisions shall be limited (not including personal data that was improperly obtained and personal data that was provided in accordance with the opt-out provisions).
- Regarding business operators' duties:
    - if there is any leakage, etc that may harm personal rights or interests, there is an obligation to report this to the Personal Information Protection Commission (PPC) and make notification to the data subjects; and
    - the amended law establishes a new provision stating that personal information shall not be used in an improper manner, including for fostering illegal or improper acts.
- Regarding encouraging business operators to make efforts in a voluntary manner:
    - for certified organisations that deal with complaints on handling of personal information, etc and establish voluntary rules, etc – such organisations that target specific areas (sectors), and those targeting all areas (sectors), should be certified.
- Regarding policies on data utilisation:
    - from the perspective of promoting innovation, 'pseudonymised information' from which names and other information are deleted shall be created; obligations for responding to demands for disclosure and discontinuation of use shall be exempted on the condition that such data shall be used only for internal analysis, etc; and
    - there shall be an obligation to confirm that consent has been obtained from the data subject for any provision to a third party of information related to an individual, including cookie and action history linked therewith, which may not constitute personal data on the information provider side but does so on the information receiver side.
- Regarding strengthening penalties (came into force on 12 December 2020, prior to some of the other provisions):
    - statutory penalties shall be increased for acts including violations of orders issued by the PPC or false reporting to the PPC; and
    - serious crimes in relation to dual-penalty provisions shall be adopted, with the maximum fine to be imposed on a juridical person (corporation) increased to ¥100,000,000, which is higher than the fine to be imposed on the offender (natural person).
- Regarding legal extra-territorial applications and cross-border transfers:
    - foreign business operators handling personal information, etc relating to persons located within Japan shall be subject to the collection of reports and orders by the PPC; and
    - at the time of providing personal data to any third party located overseas, there should be a requirement to improve the provision of information to data subjects regarding the legislative system for protection of personal information in such foreign country and the handling of personal information by the business operators to which information is transferred.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The Basic Act on Cybersecurity specifically prescribes, in addition to the cybersecurity duties of the state and the local authorities, the cybersecurity duties of critical infrastructure business operators (ie, those engaged in business pertaining to such infrastructure that forms the basis of the lives of Japanese nationals and economic activities and that is likely to have a considerable impact thereon in the event of any discontinuance or decrease of its functions), cyber-related business operators, universities and other educational or research institutions in the economic field. There is a possibility that, in the future, duties for these business operators may be prescribed in further detail by more specific laws.

In The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) published by the Cyber Security Strategy Headquarters (decided in 2017 and revised in 2020), the following 14 sectors are specified as critical information infrastructure sectors and, among those engaged in businesses belonging to such sectors, CI (critical infrastructure) operators, etc, covered by such policy are specified:

- information and communications technologies;
- finance;
- aviation;
- airports;
- railway;
- electricity;
- gas;
- government and government services (including local authorities);
- medical;
- water;
- logistics;
- chemical;
- credit cards; and
- petroleum.

In addition to the above, the 4th Edition Policy prescribed that measures would be taken to safeguard information in a further improved and reinforced manner in line with the far-ranging spread of internet of things (IOT) systems and to deal with increased risks surrounding critical infrastructure in connection with the then-upcoming Tokyo 2020 Olympic and Paralympic Games. The 4th Edition Policy, in principle, covers the period up to the end of the Tokyo 2020 Olympic and Paralympic Games (initially scheduled for 2020 but postponed to 2021 due to covid-19) and the policy is now being revised, with the next edition planned to be developed by 31 March 2022.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

In Japan, the ISMS Conformity Assessment Scheme is being operated. Under this system, certification bodies accredited by an accreditation body (ISMS-AC: ISMS Accreditation Center) assess and certify whether or not the information security management system (ISMS) created by a company or any other organisation is in conformity with ISO/IEC 27001.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Under the Personal Information Protection Act, a personal information-handling business operator is required to take, in relation to information security, necessary and suitable measures for the prevention of any

leakage, loss or damage of any personal data handled by it and for the security management of other personal data (article 20). In addition, to ensure security management of personal data, the business operator is required to perform the necessary and suitable supervision over its employees or contractors who handle personal data (articles 21 and 22). Furthermore, the PPC has developed guidelines regarding the Personal Information Protection Act (general rules, as well as rules concerning transfers to third parties located overseas, and confirmation or recording obligations in the event of transfers to third parties and anonymised information). In the medical, financial, telecommunications and other sectors, while the guidelines developed by the PPC are basically applicable, additional guidelines are also applicable in view of the nature, method of use and conventional control of personal information in those sectors.

If any personal information-handling business operator violates its obligation to take security management measures, the PPC or any other authority to which the PPC delegates the relevant power may, where necessary, recommend or order that such personal information-handling business operator cease the violation and take necessary measures for correcting the violation (articles 42 and 44 of the Personal Information Protection Act). Any person in violation of such an order issued by the PPC shall be sentenced to imprisonment for up to one year or be subject to a fine of up to ¥1,000,000 (¥100,000,000 in the case of a juridical person (corporation)) (article 83 of the Personal Information Protection Act).

In the case of a large company, defined in article 2, item 6 of the Companies Act, the company must, to develop a system to ensure good governance of the company, decide on matters concerning internal regulations and other systems. Internal regulations concerning such risk management are general in nature, and they are typically not intended for ensuring cybersecurity. Provisions for ensuring cybersecurity, however, may be required to be made as part of the internal policies, depending on the type or the volume of information held by the applicable large company or its business type.

The directors of a company limited by shares, if not a large company as defined in article 2, item 6 of the Companies Act, have a duty of due care of a prudent manager (article 330 of the Companies Act and article 644 of the Civil Code) to the company, and there is a possibility that any failure to develop a system for risk management constitutes a violation of the duty of care of a prudent manager. If a director is recognised to have violated the duty of due care of a prudent manager, the director shall be liable for providing compensation for damage caused thereby (article 423, paragraph 1 of the Companies Act).

5 How does your jurisdiction define cybersecurity and cybercrime?

In Japan, the term 'cybersecurity' has been legally defined as follows in article 2 of the Basic Act on Cybersecurity:

> *The conditions where the measures necessary for the prevention of leakage, loss or damage, and for other security management of information which is recorded, sent, transmitted or received using an electronic method, a magnetic method, or any other method not recognisable to human senses, as well as measures necessary for securing the safety and reliability of information systems and information communication networks have been taken, and where such conditions are being properly maintained and managed.*

There is no clear comprehensive definition of the term 'cybercrime'; only the types of acts to be punished as a crime (constituent elements of a crime) are prescribed in the respective criminal penalty provisions of the Penal Code, the Unauthorised Computer Access Prohibition Act and other cybersecurity laws.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In terms of the Personal Information Protection Act, in the case that serious infringement that will be caused to the data subject's rights and benefits in the event of leakage, etc of personal data, personal information-handling business operators are required to take concrete security management measures as necessary and appropriate, in line with the risks associated with various factors such as the size and nature of the business concerned, the status of handling the personal information (including the nature and volume of personal data handled) and the nature of the media on which personal data is recorded. The PPC's guidelines prescribe concrete approaches for the development of basic policies and personal information-handling rules, as well as human-related, physical and technical security management measures.

In addition to these guidelines, according to the Guidelines for Protection of Personal Information in the Finance Sector developed by the PPC and the Financial Services Agency (FSA), each personal information-handling business operator (ie, financial institution) must take necessary and suitable measures as to the development of implementation structures for security management measures, for the prevention of leakage, loss or damage, and for other management of security of the personal data that it handles. Further, it is prescribed in these guidelines that these measures must include 'systematic', 'human-related' and 'technical' security management measures, which are laid out according to the respective levels of acquisition, usage and retention of personal data.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Article 15 of the Basic Act on Cybersecurity provides for the state's obligation to promote awareness of the importance of cybersecurity and to provide necessary information, advice and other necessary measures to private business operators and educational and research institutions to protect the intellectual property information held by them, in view of the importance of the information for the reinforcement of Japan's international competitiveness.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

To provide stable and proper services, critical infrastructure operators are obligated to have a deeper understanding and should know the significance of cybersecurity. They are further required to make voluntary and active efforts to ensure cybersecurity and to cooperate in putting in place cybersecurity measures prescribed by the state or local authorities (article 6 of the Basic Act on Cybersecurity). Moreover, the Basic Act on Cybersecurity prescribes that the government must develop basic schemes concerning cybersecurity (cybersecurity strategy) to further cybersecurity measures in an effective manner. It also provides that cybersecurity strategies must contain matters relating to strengthening cybersecurity in critical infrastructure operators (article 12, paragraph 2, item 3). In addition to the Basic Act on Cybersecurity, which is of a general nature, specific provisions on cybersecurity have been prescribed in related laws, such as the:

- Personal Information Protection Act;

- Penal Code;
- Unauthorised Computer Access Prohibition Act;
- Unfair Competition Prevention Act;
- Copyright Act;
- Telecommunications Business Act;
- Specially Designated Secret Protection Act;
- Basic Act on the Formation of a Digital Society (renamed from 'Basic Act on the Formation of an Advanced Information and Telecommunications Network Society' on 1 September 2021);
- Act on Electronic Signatures and Certification Business; and
- Act on Facilitation of Information Processing.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In Japan, it is construed that the spirit of article 13 of the Japanese Constitution guarantees privacy in general. The Personal Information Protection Act also deals with some aspects of privacy; however, there are no privacy-specific cybersecurity laws or regulations.

In terms of private communications, article 21, paragraph 2 of the Japanese Constitution guarantees the secrecy of communications, stating that: 'No censorship shall be maintained, nor shall the secrecy of any means of communication be violated'. It is prescribed in the Telecommunications Business Act that secrecy of communications handled by telecommunications business operators shall not be violated (not only by telecommunications business operators but also by any other person). The Radio Act similarly protects the secrecy of private communications.

As an exception to the above, the Act on Wiretapping for Criminal Investigation permits, as a special investigation method for serious crimes, the wiretapping of telecommunications for criminal investigations, based on strict requirements and subject to a warrant issued by a judge, with an observer being present throughout the process, limited to cases where it would be difficult to reveal the truth through normal investigative means. However, subject to the necessary technical measures (eg, encryption of communications) being taken, it is no longer necessary for the personnel of telecommunications carriers to act as observers and to seal the wiretapped communications. Further, procedures for enabling wiretapping at police facilities are also available for such a purpose.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

Cybercrimes are regulated by the Penal Code, the Unauthorised Computer Access Act and other laws, as outlined below.

Penal Code

The following types of conduct were prescribed as crimes in the 1987 amendment to the Criminal Code:

- unauthorised creation of electronic or magnetic records (article 161-2): the act of creating electronic or magnetic records relating to rights, duties or certification of facts that was previously covered by the crime of forgery of documents became punishable;
- obstruction of business by damaging a computer (article 234-2): obstruction of business by way of damaging a computer was newly added as a type of obstruction of business that is subject to punishment;
- computer fraud (article 246-2): an act of fraud using a computer became punishable; and
- damage to an electronic or magnetic record (articles 258 and 259): an act of damaging an electronic or magnetic record in use by a public office, or an act of damaging another person's electronic or magnetic records relating to rights or obligations, became punishable.

The following types of conduct were added as crimes in the 2001 amendment to the Criminal Code:

- unauthorised creation of electromagnetic records of payment cards (article 163-2);
- possession of payment cards with unauthorised electromagnetic records (article 163-3);
- preparation for unauthorised creation of electromagnetic records of payment cards (article 163-4); and
- attempts to engage in the crimes prescribed above (article 163-5).

Articles 168-2 and 168-3 were added as crimes in the 2011 amendment to the Criminal Code to punish the conduct of creating, providing, obtaining and storing a computer virus.

Unauthorised Computer Access Act

This act prohibits and punishes criminal conduct, such as the following:

- unauthorised access;
- promoting any unauthorised computer access (ie, an act of providing another authorised person's identification code (eg, ID and password) without that person's permission); and
- wrongfully obtaining another authorised person's identification code (eg, ID and password), wrongfully storing another authorised person's identification code or wrongfully requesting another authorised person to input an authorised person's identification code.

'Unauthorised access' as used here refers to the following types of conduct (article 2(4) of the Computer Access Act):

- spoofing (ie, inputting another authorised person's identification code (eg, ID and password) without that person's permission); and
- attacking security holes (ie, inputting unique data, avoiding access control features and using computer functions that are restricted by identification codes by utilising computer programs to engage in cyberattacks).

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Globalisation of corporate activities has facilitated cloud services and other cross-border distribution of information. To ensure smooth cross-border distribution of information, the amended Personal Information Protection Act is aimed at creating a better structure in line with the systems being used overseas as well as the prevailing circumstances in international society. For that purpose, the amended Personal Information Protection Act includes:

- a provision prescribing protective measures to be taken when transferring information to other countries (ie, article 24, which, in principle, requires the obtaining of prior consent from the data subject in the event of such an individual's personal information being provided to a third party located overseas); and
- a provision allowing the application of Japanese laws to foreign business operators in the event of cross-border distribution of information (ie, article 75, pursuant to which many of the obligations prescribed in the Personal Information Protection Act will be directly applicable to any business operator handling personal information, who has acquired the personal information of an individual in Japan in connection with the provision of goods or services to such individual, and who handles, outside of Japan, any such personal information or any de-identified information created using it).

Further, the 2020 amendments to the Personal Information Protection Act prescribe equality between foreign and domestic business operators, such that, in the case that the Act is applicable to a business operator located outside of Japan, all provisions of the Act will be applicable thereto, including provisions concerning the collection of reports, on-site inspections, and orders and emergency orders by the PPC. Moreover, under the amended Act, when personal information is provided to a third party in a foreign country, the data subjects must be informed in advance of the legislative system for protection of personal information in the foreign country; the personal information protection measures to be taken by the third party; and other matters that would serve as a reference to the data subjects.

12 | How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Obligations under Japanese laws and regulations applicable to foreign corporations engaging in business in Japan are the same as those applicable to domestic corporations in Japan.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Under the Basic Act on Cybersecurity, the obligations for critical infrastructure operators, cyber-related business operators, universities and other educational and research institutions may be prescribed in a more concrete manner by the promulgation of specific laws and regulations in the future. These may also include guidelines for strengthening cybersecurity. For example, on 28 September 2021, the Cabinet adopted a revised Cybersecurity Strategy. Furthermore, the Cyber Security Strategy Headquarters published The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) on 18 April 2017, which was subsequently revised on 25 July 2018 and 30 January 2020 (the 4th Edition Policy is now being revised, with the next edition planned to be developed by 31 March 2022), whereby the following four measures have been promoted:

- developing security standards and raising awareness: continuously improve guidelines for cross-sectoral measures and sector-to-sector security standards in protecting critical information infrastructure;
- strengthening failure response frameworks: generally strengthen the frameworks for responding to service failures in critical infrastructure through drills, to be performed by way of public-private collaboration and coordination of various drills and training;
- managing and addressing risks: promote comprehensive risk management, including improvement of risk response capabilities, through risk assessment and the development of contingency plans; and
- strengthening the protection base: revise the scope for critical infrastructure protection, promoting public relations or public consultation activities and international collaboration, make necessary approaches to corporate senior management and promote human resource development, among other things.

Further, from the perspective of information security, the Personal Information Protection Commission has developed the following separate guidelines regarding the Act on the Protection of Personal Information: general rules; provision of personal information to third parties outside of Japan; confirmation and recording obligations in providing personal information to third parties; and anonymously processed information.

14 | How does the government incentivise organisations to improve their cybersecurity?

To ensure that critical infrastructure operators adhere to measures to strengthen cybersecurity, the Basic Act on Cybersecurity requires the state to take necessary measures, such as developing basic standards to be followed, providing drills, training and promoting information sharing and other voluntary efforts (article 14). In addition, the state is required to promote awareness regarding the significance of cybersecurity, hold consultations concerning cybersecurity, provide necessary information and advice and take other necessary measures (article 15).

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

With regard to information security, international standards ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27017 are principally used in the development of relevant guidelines.

To use the ISO standards for the applicable certification system in Japan, however, the contents of such ISO standards must be established anew as Japanese Industrial Standards (JISs). JISs refer to national standards that are established for the purpose of promoting industrial standardisation in accordance with the Industrial Standardisation Act. These are specially enacted for the purpose of furthering industrial standardisation in Japan. Among the ISO/IEC 27000 family relating to information security management systems (ISMSs), the following standards have been faithfully translated into Japanese to secure consistency with international standards and are recognised as being identical (IDT: IDENTICAL):

- ISO/IEC 27001: 2013 into JIS Q 27001: 2014;
- ISO/IEC 27002: 2013 into JIS Q 27002: 2014;
- ISO/IEC 27006: 2015 into JIS Q 27006: 2018;
- ISO/IEC 27014: 2013 into JIS Q 27014: 2015; and
- ISO/IEC 27017: 2015 into JIS Q 27017: 2016.

In 2017, JISQ15001, being a standard used for privacy mark certification, was revised. JISQ15001 is not an international standard but rather a national standard that partly overlaps with ISO/IEC 27001 in terms of information protection; however, the two standards greatly differ in that, while information held by an organisation is generally protected under ISO/IEC 27001, only personal information is protected under JISQ15001.

16 | Are there generally recommended best practices and procedures for responding to breaches?

In the event of an accidental information leak at a company resulting from a cybersecurity incident, although the measures to be taken by the company may vary depending on each case, examples of possible measures generally include the following:

- immediately verify the facts concerned, including the causes of the accident and the information that has been leaked, and announce accurate facts at an early stage, expressing sincere apologies;
- continuously announce facts that may be revealed through subsequent investigations;
- perform investigations not only by a team of internal members but also, where necessary or appropriate, organise a third-party committee consisting of legal specialists (including attorneys and technical specialists, etc) who are in neutral positions to

perform investigations and report the results of the investigations performed; and
- develop and adopt measures to prevent recurrence based on the accidental information leak concerned.

Information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

There is no particular legal incentive with regard to the voluntary sharing of information relating to cyberthreats. However, the revised Cyber Security Strategy (adopted by a Cabinet decision on 28 September 2021) stipulates as follows: '[T]he government will work to ensure that efforts to strengthen cybersecurity in line with digitalisation are visualised so that investors and other stakeholders who value sustainability will be aware of them, and that incentives are generated for such efforts'; 'Specifically, cybersecurity initiatives will be positioned in policies to promote digitalisation, including tax measures for digital-related investments and the selection and announcement of forward-looking companies that practice digital management guidelines and work on digitalisation. In addition, the use of tools and guidelines to visualise the status of initiatives to stakeholders in and outside companies will be advanced'; and 'Through such efforts, ... the promotion of practices such as ascertaining cybersecurity risks by executives and the disclosure of corporate information is expected'. The Policies state that the government will share information on best practices and create guidelines while working to continually grasp and evaluate information dissemination and disclosure status. For example, from the perspective of information security, in the event of an accidental information leak at a company, it would be practically advantageous for the company to make an accurate announcement at an early stage and to take the necessary measures to reduce the deterioration of goodwill among its customers. In the Japanese market, there have been cases of huge business losses incurred by companies as a result of deterioration in their corporate image due to improper handling of information leaks. Risk to reputation must, therefore, be considered a significant business risk that should never be ignored.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The Basic Act on Cybersecurity provides the basic philosophy for cybersecurity and basic measures that are required to be taken 'for facing threats to cybersecurity, through coordination of various entities such as the state, local authorities, critical infrastructure operators, etc' (article 3). To realise such coordination, the Basic Act on Cybersecurity requires the government or the state to take the following measures, in addition to the measures mentioned in 'Increased protection':
- necessary legal, financial or tax measures and other measures to be taken by the government to adhere to the policies concerning cybersecurity under the Basic Act on Cybersecurity (article 10); and
- necessary measures to be taken by the state to reinforce coordination among relevant governmental agencies and ministries, and to enable various entities such as the state, local authorities, critical infrastructure operators, etc, to mutually coordinate and work on cybersecurity-related measures (article 16).

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance products covering cyber risks, such as standard attacks from outside parties and unauthorised access committed internally, and providing coverage for damage arising from personal information leakage or system failure or similar issues, are generally available. However, most of these insurance products have limited the types of incidents for which insurance benefits can be claimed and have also limited the place of insured incidents to Japan.

In December 2012, a Japanese corporation belonging to an insurance company group based in the United States started selling insurance products that provide broader coverage for damage arising from cyberattacks, including accidents occurring outside Japan. Currently, insurance products that cover damages incurred in cybersecurity incidents are being sold by leading Japanese insurance companies.

ENFORCEMENT

Regulation

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Government agencies that are the competent authorities concerning cybersecurity are the nodal authorities for ensuring implementation of the laws, such as by providing their interpretations as relevant administrative organs and developing guidelines (provided, however, that the interpretation of laws by the administrative organs shall not be binding upon judicial organs).

For example, the National Police Agency, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry are the competent authorities in the case of the Unauthorised Computer Access Prohibition Act, and the Ministry of Justice has competency over laws pertaining to cybercrimes, including the Penal Code, and, as such, are in charge of the implementation of those laws. The Personal Information Protection Commission (PPC) has competency over the Personal Information Protection Act and, as expressly prescribed in said Act, is entitled to require the submission of reports and materials from personal information-handling business operators, as well as being entitled to enter their business premises for inspection purposes (article 40 of the Act). Furthermore, the PPC provides necessary guidance and advice (article 41 of the Act) or recommendations or orders (article 42 of the Act) to personal information-handling business operators. A personal information-handling business operator shall be punished (Chapter 7 of the Act) if it fails to comply with an order. Since the PPC must ensure the proper handling of personal information in an urgent and focused manner, it is entitled to delegate the power to collect reports from, and to enter and inspect the business premises of, a personal information-handling business operator, among others, to the authority having jurisdiction over the business concerned, whenever the PPC considers it necessary to do so to effectively provide recommendations or orders (article 44, paragraph 1 of the Act).

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

With regard to cybersecurity, there are, to date, no laws or regulations directly and expressly prescribing the power of any administrative organ to monitor or investigate private business operators for their compliance with regard to the implementation of measures to strengthen cybersecurity. The obligations imposed on those other than the state or the local authorities under the Basic Act on Cybersecurity are obligations to make efforts, and the Basic Act on Cybersecurity itself will not be grounds for the authorities' power over private sectors. Therefore, no administrative organ has the power to prosecute any private business operator in the event of a violation of these obligations.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Administrative organs do not have the power to impose, by way of penalties or by any other means, any mandatory obligations on private business operators to ensure cybersecurity. The Basic Act on Cybersecurity is preconditioned on the fact that the obligations of parties, other than the state and local authorities, are limited to carrying out best efforts, and the voluntary efforts of private business operators will be furthered by the state by taking necessary measures. This being the case, there is a huge issue in terms of whether or not the voluntary efforts of private business operators can be effectively furthered based on measures taken by the state.

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

In terms of information security, some of the guidelines prepared in accordance with the Personal Information Protection Act carry an obligation that a leakage of personal information be reported to the supervisory authority and the data subject informed. For example, the Guidelines for Personal Information Protection in the Financial Field developed by the PPC and the FSA set forth that: 'If an accident involving leakage, etc of personal information occurs, an entity handling personal information must immediately report the same to the supervisory authority' (article 17, item 1); and 'If an accident involving leakage, etc of personal information occurs, an entity handling personal information in the financial field must promptly notify the facts, etc thereof to the person whose personal information has been leaked' (article 17, item 3). In addition, as described above, an entity handling personal information may be subject to punishment if it fails to comply with any order given by the PPC in accordance with article 42 of the Personal Information Protection Act (Chapter 7).

Pursuant to article 17 of the Basic Act on Cybersecurity, the Cybersecurity Council was established in April 2019 to promote an information-sharing system. The Council has a total of 265 various members (as of 4 October 2021) from both the public and private sectors and different industries, and is planning to continue accepting applications for membership hereafter. The Council may request its members to provide cooperation whenever necessary, including submission of information, and a member who receives such request is obliged to comply with the same, unless it has a just cause not to do so (article 17, paragraph 3 of the Basic Act on Cybersecurity).

However, with regard to sharing personal information prescribed in the Personal Information Protection Act; trade secrets prescribed in the Unfair Competition Prevention Act; material facts that may affect stock prices as prescribed in the Financial Instruments and Exchange Act; and malware, etc, which may constitute a crime under the Penal Code, due consideration must be given to regulations under applicable laws, as well as to the disadvantages that may arise from such requests. Therefore, with a view to preventing abuse of requests for provision of information, the Council Rules set forth that the Council may request general members to provide cooperation such as provision of information, only in the following cases:

- whenever a special need to request cooperation such as provision of information is recognised, such as a large-scale cyberattack having occurred, or in the event that circumstances similar thereto are recognised to exist; or
- whenever members have consented to receiving cooperation requests from the Council.

In addition, although private business operators do not have any regulatory notification obligations in general, the National Center of Incident Readiness and Strategy for Cybersecurity is working on mutual sharing of information regarding system failures, etc, in cooperation with ministries and agencies managing critical infrastructure, ministries and agencies related to information security, and principal infrastructure business operators, as one of the measures to be taken in accordance with The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) published by the Cyber Security Strategy Headquarters. Such efforts are made in line with critical infrastructure business operators' duties of 'endeavouring independently and actively to ensure cybersecurity' and 'endeavouring to cooperate in the implementation of the cybersecurity policy' as set forth in article 6 of the Basic Act on Cybersecurity. Furthermore, there are several other information sharing systems.

In terms of information security, some of the guidelines that have been prescribed in accordance with the Personal Information Protection Act set forth the obligation to report any information leakage, etc to regulatory authorities, etc, or to notify data subjects of the same. For example, the Guidelines for Protection of Personal Information in the Finance Sector developed by the PPC and the Financial Services Agency (FSA) stipulate that '[i]n the event of the leakage of any personal information … a personal information handling business operator in the finance sector is to immediately report that incident to the supervisory authority, etc' (article 17, paragraph 1 of the Guidelines). In addition, with regard to notification to data subjects, these guidelines stipulate that '[i]n the event of the leakage of personal information or other related incident, a personal information handling business operator in the finance sector is to promptly inform the person in question involved in the relevant incident of the facts concerning the incident' (article 17, paragraph 3 of the Guidelines). Furthermore, punishment may be imposed on a business operator handling personal information if it fails to comply with an order issued by the PPC in accordance with article 42 of the Personal Information Protection Act (Chapter 7 of the Act).

On the other hand, according to the PPC's general guidelines applicable to all business fields (Guidelines Concerning Measures to be Taken upon Personal Data Leakage Incidents, Etc), private business operators are merely obliged to make efforts to report information leakages to the PPC, among others. In addition, with regard to notification to data subjects, these guidelines stipulate that a desirable measure would be to either promptly notify the data subjects of information such as the facts involved in the incident in question or to keep such information in a status that allows for data subjects to easily become aware of the same, depending on the content of each data leakage incident, principally from the perspective of preventing any secondary damage or similar incidents.

Under the amended Personal Information Protection Act (amended in 2020 and due to come into force on 1 April 2022), personal information-handling business operators will be required to report to the PPC and, in principle, notify the data subjects, in the event of any leakage, loss or damage of personal data or other security-related situations that are prescribed by the PPC as highly likely to harm the rights and interests of the data subjects (article 22-2 of the amended Act).

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

To date, there is no penalty under law imposed on victims of cyberattacks, solely by reason of having failed to implement sufficient measures for cybersecurity other than information security. It is, however, set forth in the Unauthorised Computer Access Prohibition Act that an administrator of a computer connected to telecommunication lines, who has

added an access control feature to the computer by way of an ID or password, has the obligation to always verify the effectiveness of the ID or password and endeavour to promptly take appropriate measures to protect the computer concerned from acts of unauthorised computer access, such as enhancement of the function of the access control feature concerned, whenever deemed necessary (article 8).

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

With regard to cybersecurity, there is, to date, no law or regulation directly and expressly obliging a private business operator to report any cyberattack sustained by it, and no penalty is imposed on it in the event of a failure to make a report. On the other hand, in terms of information security, some of the guidelines prepared in accordance with the Personal Information Protection Act set forth an obligation to report any information leakage to the competent authority. Under the amended Personal Information Protection Act (amended in 2020 and due to come into force on 1 April 2022), personal information-handling business operators will be required to report to the Personal Information Protection Commission (PPC) and notify the data subjects in the event of any leakage, loss or damage of personal data, or other security-related situations that are prescribed by the PPC as highly likely to harm the rights and interests of the data subjects. Under the amended Act, the PPC will issue a recommendation or order concerning any action to be taken in respect of any failure to report (article 42, paras 1 and 3), and a violation of such order shall be subject to imprisonment for up to one year or a fine of up to ¥1,000,000 (newly prescribed in article 83), or if such violation relates to the business of a juridical person (corporation), such juridical person (corporation) shall be subject to a fine of up to ¥100,000,000 (newly prescribed in article 87, paragraph 1, item 1).

26 | How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

If cybersecurity is regarded as a contractual obligation, compensation may, as a general rule, be claimed against a party who has the obligation, within the scope of a reasonable cause-effect relationship. It is, however, possible to restrict the scope of the damage compensation obligation, based on the mutual agreement of both parties to a contract, as long as the restrictions do not conflict with any mandatory laws and regulations. If the restriction is set forth in a contract, this merely means that compensation for damage may be made within the scope of the contract.

In internet-based businesses, however, contracts could be entered into with consumers (ie, individuals, excluding those who become a party to a contract in the course of, or for the interest of, any business (article 2 of the Consumer Contract Act)). In this case, according to the Consumer Contract Act, any clause that totally exempts a business operator from its liability to compensate a consumer for damage arising from default by the business operator is void (article 8), and the provision of the Act is a mandatory statute (ie, any clause of a contract in conflict therewith will be void). In this regard, according to the 2018 amendments to the Act that came into force on 15 June 2019, any clause in which a business operator attempts to set its own liability, etc, will also be void.

THREAT DETECTION AND REPORTING

Policies and procedures

27 | What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

In terms of the Personal Information Protection Act, as serious infringement will be caused to data subjects where there is a leakage, etc of personal data, personal information-handling business operators are required to take concrete security management measures, as appropriate, concurrent to the risks involved, such as the size and nature of the business, the personal information-handling status, and the nature of the media on which personal data is recorded. The Personal Information Protection Commission (PPC)'s guidelines, etc prescribe concrete approaches for developing basic policies and personal information-handling rules, as well as human-related, physical and technical security management measures.

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

To date, there are no rules directly and expressly prescribing such obligations under any laws or regulations.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

To date, there are no laws or regulations directly and expressly requiring private business operators to make regular reports concerning their cybersecurity breaches. On the other hand, in terms of information security, certain guidelines prescribed under the Personal Information Protection Act require that reports be made to the supervisory authority, etc, and that the data subjects be informed in the event of leakage, etc of personal information.

The Personal Information Protection Act was amended in 2020 (due to come into force on 1 April 2022) and personal information-handling business operators will be required to report to the PPC and notify the data subjects in the event of any leakage, loss or damage of personal data, or other security-related situations that are prescribed by the PPC as highly likely to harm the rights and interests of the data subjects (article 22-2 of the amended Act).

Time frames

30 | What is the timeline for reporting to the authorities?

To date, there is no law or regulation directly and expressly prescribing the obligation of a private business operator to make regular reports concerning cybersecurity.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

In terms of information security, some of the guidelines, etc established in accordance with the Personal Information Protection Act set forth matters relating to public announcements or notices to be provided in the event of any leakage of information. For example, in the public notice given pursuant to the Guidelines Concerning Measures to be Taken upon Personal Data Leakage Incidents, Etc, prepared by the Personal Information Protection Commission (PPC), prescribe that: 'It is desirable for a business operator handling personal information to

take necessary measures concerning (1) through (6) below', and, with regard to (6) ('Publication of facts involved and recurrence prevention measures'): 'Facts involved and recurrence prevention measures should be promptly publicised based on the details of such leakage incident, etc, so as to prevent any secondary damage or the occurrence of similar incidents'.

Furthermore, it is provided in the Guidelines for Personal Information Protection in the Financial Field that, in the event of an accidental leak, or similar, of personal information, an entity handling personal information in the financial field must 'promptly publicise the facts involved in such incident and the recurrence prevention measures, so as to prevent secondary damage or the occurrence of similar incidents' (article 17, paragraph 2) and must 'notify the facts of such incident promptly to the person whose personal information has been leaked' (article 17, paragraph 3).

The Personal Information Protection Act was amended in 2020 (due to come into force on 1 April 2022), whereby personal information-handling business operators will be required to report to the PPC and, in principle, notify the data subjects in the event of any leakage, loss or damage of personal data, or other security-related situations that are prescribed by the PPC as highly likely to harm the rights and interests of the data subjects (article 22-2 of the amended Act).

UPDATE AND TRENDS

Key developments of the past year

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Most of the critical infrastructure business operators are private entities and, accordingly, there is an issue in relation to the possibility of excessively strict obligations being imposed on those entities, resulting in pushback from them owing to the huge expenses and manpower required from them in ensuring cybersecurity. In this regard, it can be said that this issue has been resolved by the Basic Act on Cybersecurity being preconditioned on the furtherance of the voluntary efforts of private business operators, while limiting their obligations merely to making an effort to improve the security of their systems. In addition, pursuant to the Basic Act on Cybersecurity, the position of the Cyber Security Strategy Headquarters (the Chief Cabinet Secretary acting as the head of the Headquarters) as an organisation demonstrating a control tower function extending across ministries and agencies has been made legally clear, allowing for the Cyber Security Strategy Headquarters to fulfil its role in a more effective manner (as outlined in Chapter 4 of the Basic Act on Cybersecurity). Much attention continues to be paid to the effective measures to be taken hereafter by the state in relation to cybersecurity under the leadership of the Cyber Security Strategy Headquarters.

To fundamentally reinforce the countermeasures to be taken by the national administrative organs, etc in response to increasing threats to cybersecurity, the Basic Act on Cybersecurity was partly amended and came into force on 21 October 2016. Under the amended Act, the scope of parties to be evaluated by the national government in terms of cybersecurity measures has been expanded to cover special corporations and authorised corporations, in addition to the central government and incorporated administrative agencies. Moreover, the scope of parties whose information systems will be monitored unanalysed by the national government to deal with wrongful activities targeting them has been expanded to cover incorporated administrative agencies, special corporations and authorised corporations, in addition to the central government. These amendments have been triggered by an incident made public in June 2015 when there was a cyberattack on the Japan Pension Service (a special and authorised corporation) resulting in the leakage of approximately 125 million items of personal information. In relation to the amendments, the Act on Facilitation of Information Processing was also amended, and a national qualification system of cybersecurity specialists (registered information security specialists) has been established.

Subsequently, in preparation for the Tokyo Olympic and Paralympic Games which were originally planned for 2020, the Basic Act on Cybersecurity was amended and came into force on 1 April 2019, to include, for example, provisions concerning a council to be established by the government and major infrastructure operators to share information on preventing the spread of damage caused by cyberattacks.

In addition, governmental investigations have revealed that, as well as high-level cyberattacks on major defence-related companies, small to medium-sized companies (SMEs) have also been targets of cyberattacks in Japan in recent years. The Ministry of Economy, Trade and Industry (METI) has therefore compiled a report concerning basic directions for future efforts concerning such issues, suggesting the following three actions to be taken by companies:

- closely sharing information among supply chain companies;
- reporting to the METI if there is any concern about the leakage of sensitive technical information; and
- making public announcements whenever there is a risk of damage spreading, not only within a supply chain but also to third parties.

To reinforce cybersecurity measures within supply chains, including SMEs thereof, the METI has decided to consider means of visualising SMEs' efforts regarding cybersecurity measures. Subsequently, on 1 November 2020, the Supply Chain Cybersecurity Consortium was established under the initiative of METI, the purpose of which is to promote cybersecurity measures throughout respective supply chains, with large companies and SMEs from various fields working as one. The consortium considers and promotes efforts to reinforce cybersecurity measures throughout respective supply chains, including duly motivating SMEs whose cybersecurity systems are insufficient.

Furthermore, the following amendments have been made to related laws and regulations in the past year.

First, the 'Cybersecurity Strategy', which is formulated every three years pursuant to the Basic Act on Cybersecurity, was newly formulated on 28 September 2021. This new strategy sets out the major direction of 'Cybersecurity for All; with no one left behind', as well as policies for the measures to be taken by the government, in light of environmental changes and awareness of threat perceptions that we are currently facing, such as the development of DX (digital transformation); the increasingly public nature of cyberspace; and the escalating threat from cyberattacks including suspected state involvement, from the perspective of Japan's national security.

Further, the Basic Act on the Formation of a Digital Society was enacted and abolished the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, and the Digital Agency was established based on the said new Act (1 September 2021). There is an obligation to develop the 'measures to be taken by the government rapidly and with priority in connection with securing cybersecurity, etc' as one of the matters set out in the 'priority policy program on the formation of a digital society' which the government is required to develop pursuant to the Basic Act on the Formation of a Digital Society. For the development of the said program, it is prescribed that the government shall consult with the Cyber Security Strategy Headquarters and the Personal Information Protection Commission.

The Digital Agency aims at promoting DX and rapidly establishing public-private infrastructure in the digital age in the next five years. In

addition, with respect to the administrative functions related to cybersecurity, it is stipulated that the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) shall establish a series of unified standards for the government, while it is provided that the Digital Agency shall use the said series of standards to propose basic principles for cybersecurity within the basic development principles for information systems and shall promote the implementation thereof. Moreover, the Digital Agency shall recognise cybersecurity as an important issue and respond thereto, such as the Agency being equipped with a dedicated team for cybersecurity to conduct verification and auditing principally of the systems to be developed and operated by such Agency. The NISC shall complement the Digital Agency's system by reinforcing the cybersecurity system of the NISC itself, and shall perform security auditing, etc against the systems of national administrative organs, etc including the systems to be developed and operated by the said Digital Agency, with the aim of ensuring security.

In addition, principally in relation to information security, the Personal Information Protection Act has been amended (due to come into force on 1 April 2022, except for provisions concerning strengthened penalties, etc). It should be noted that such amendments relate to increased penalties (ie, in addition to increasing the statutory penalties as a whole, the maximum fine to be imposed on a juridical person (corporation) will be increased to ¥100,000,000, which is higher than the fine to be imposed on the offender (natural person); the increased penalties came into force on 12 December 2020, prior to the other amendments); and legal extra-territorial applications and cross-border transfers (such as foreign business operators that handle personal information, etc) relating to persons located within Japan being subject to the collection of reports and orders by the Personal Information Protection Commission.

Masaya Hirano
masaya_hirano@tmi.gr.jp

Kazuyasu Shiraishi
kshiraishi@tmi.gr.jp

23F Roppongi Hills Mori Tower
6-10-1 Roppongi, Minato-ku
Tokyo 106-6123
Japan
Tel: +81 3 6438 5511
www.tmi.gr.jp

Singapore

Lim Chong Kin
Drew & Napier LLC

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The primary cybersecurity legislation in Singapore is the Cybersecurity Act 2018 (Cybersecurity Act). The Cybersecurity Act came into effect on 31 August 2018, with the exception of Part 5 (sections 24 to 35) and the Second Schedule, which concerns the licensing of cybersecurity service providers. Subsidiary legislation includes the Cybersecurity (Critical Information Infrastructure) Regulations 2018 and Cybersecurity (Confidential Treatment of Information) Regulations 2018.

The Cybersecurity Act:

- creates a framework for the protection of designated critical information infrastructure (CII) against cybersecurity threats;
- provides for the appointment of the Commissioner of Cybersecurity (Commissioner) and other officers for the administration of the Cybersecurity Act;
- authorises the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore; and
- establishes a licensing framework for providers of licensable cybersecurity services in Singapore – specifically, managed security operations centre monitoring services and penetration testing services.

Under the Cybersecurity Act, the Commissioner is empowered to issue codes of practice and standards of performance to ensure the cybersecurity of CII. Pursuant to these powers, the Commissioner has issued the Cybersecurity Code of Practice for Critical Information Infrastructure as of 1 September 2018.

In addition, the Cybersecurity Agency of Singapore (CSA) has also introduced supplementary references to assist CII owners in compliance, including the Security-by-Design Framework (a framework developed to guide CII owners in addressing cyber protection considerations throughout their system's life cycle) and the Security-by-Design Framework Checklist (a quick reference guide assisting cybersecurity practitioners in adopting the Security-by-Design Framework).

The Cybersecurity Act will operate alongside the patchwork of existing legislation and various self-regulatory or co-regulatory codes that promote cybersecurity, including but not limited to the following:

- the Computer Misuse Act 1993 (CMA), which criminalises certain cyber activities, such as hacking, denial-of-service attacks, infection of computer systems with malware, the possession or use of hardware, software or other tools to commit offences under the CMA, and other acts preparatory to or in furtherance of the commission of any offence under the CMA;
- the Personal Data Protection Act 2012 (PDPA), which governs the processing of individuals' personal data by private sector organisations, and which is administered and enforced by the Personal Data Protection Commission (PDPC);
- the Strategic Goods (Control) Act 2002, which governs the transfer and brokering of strategic goods and strategic goods technology, including 'information security' systems, equipment and components (ie, designed or modified to use cryptography for data confidentiality having in excess of 56 bits of symmetric key length or equivalent);
- sector-specific codes of practice, such as the Telecommunication Cybersecurity Code of Practice formulated by the Infocomm Media Development Authority, the converged telecommunications and media regulator in Singapore, which is imposed on major internet service providers in Singapore and includes security incident management requirements;
- other sector-specific regulatory frameworks, such as the Notice on Technology Risk Management (and the related Technology Risk Management Guidelines) (TRM Notices and Guidelines) formulated by the Monetary Authority of Singapore (MAS), Singapore's central bank and the regulator responsible for overseeing the financial sector in Singapore, which imposes certain requirements relating to technology risk management for MAS-regulated financial institutions; and
- in respect of public sector agencies, the Business Continuity Readiness Assessment Framework and the Infocomm Security Health Scorecard, which were put in place to assess the level of security readiness and preparedness of Singapore's public sector agencies.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The Cybersecurity Act provides for the regulation of CII in 11 critical sectors. CII is defined as a computer or computer system that is necessary for the continuous delivery of an essential service, the loss or compromise of which will lead to a debilitating effect on the availability of the essential service in Singapore. The 11 critical sectors containing essential services from which CII may be designated are:

- energy;
- info-communications;
- water;
- healthcare;
- banking and finance;
- security and emergency services;
- aviation;
- land transport;
- maritime;
- government; and
- media.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The CSA has launched a certification scheme known as the Singapore Common Criteria Scheme (SCCS). The SCCS is based on the international standard ISO/IEC 15408 for computer security certification, otherwise known as the Common Criteria for Information Technology Security Evaluation. The SCCS aims to provide a cost-effective regime for the info-communications industry to evaluate and certify that their IT products conform to an accepted protection profile under the SCCS.

In addition, the government has publicly stated that, in the implementation of the Cybersecurity Act, it will take reference from internationally recognised standards when developing codes of practice and standards of performance for different sectors.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Personal liability may in certain circumstances be imposed on certain individuals for offences committed by their organisations under the Cybersecurity Act. Such offences include, among others, the failure of a CII owner to notify the Commissioner of certain cybersecurity incidents within the prescribed period of becoming aware of such occurrence under section 14, and the failure of a CII owner to conduct regular cybersecurity audits and risk assessments under section 15.

Section 36 of the Cybersecurity Act imposes personal liability on officers, members (where the affairs of a corporation are managed by its members) and individuals involved in the management of the corporation and who are in a position to influence its conduct, for offences committed by the corporation under the Cybersecurity Act, where such person: consented or connived, or conspired with others to effect the commission of the offence; is in any other way knowingly concerned or party to the commission of the offence; or knew or ought reasonably to have known that the offence by the corporation would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence.

In relation to offences committed by an unincorporated association or a partnership under the Cybersecurity Act, section 37 of the Cybersecurity Act imposes personal liability on officers of unincorporated associations and members of their governing bodies, partners in a partnership, and individuals involved in the management of the unincorporated association or partnership and who are in a position to influence its conduct, in circumstances similar to those set out under section 36 of the Cybersecurity Act.

Under general company law, a director's failure to adequately manage an organisation's cybersecurity arrangements may amount to a breach of his or her directors' duties, for example, under section 157 of the Companies Act (Cap. 50), which requires a director to use reasonable diligence in the discharge of the duties of his or her office.

The Code of Corporate Governance, which applies to listed companies in Singapore on a comply-or-explain basis, establishes the principle that the board of directors is responsible for the governance of risk and should ensure that management maintains a sound system of risk management and internal controls to safeguard the interests of the company and its shareholders.

5 How does your jurisdiction define cybersecurity and cybercrime?

'Cybersecurity' is defined under section 2 of the Cybersecurity Act to mean the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state:

- the computer or computer system continues to be available and operational;
- the integrity of the computer or computer system is maintained; and
- the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

The Cybersecurity Act, which provides for the protection of CII and establishes powers for the investigation and prevention of cybersecurity threats and incidents, falls under the purview of the Commissioner as supported by the CSA.

There is no statutory definition of the term 'cybercrime'. In general, cybercrime issues are dealt with under the CMA, which criminalises activities such as the unauthorised access to computer material and the unauthorised modification of computer material. The enforcement and investigation of offences under the CMA fall under the purview of the Singapore Police Force.

The protection of personal data falls under the purview of the PDPA, which is administered and enforced by PDPC.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The Cybersecurity Act does not prescribe detailed protective measures to be taken. Instead, it imposes a set of general duties on owners of CII, including:

- a duty to comply with notices issued by the Commissioner for the CII owners to provide information (ie, to provide the Commissioner with information on the technical architecture of the CII (section 10));
- a duty to comply with codes of practice, standards of performance or written directions in relation to the CII as may be issued by the Commissioner (sections 11 and 12);
- a duty to notify the Commissioner of any change in ownership of the CII (section 13);
- a duty to report prescribed cybersecurity incidents (ie, to notify the Commissioner of any prescribed cybersecurity incident relating to the CII (section 14));
- a duty to conduct audits (ie, to cause regular audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance, which are to be carried out by an auditor approved or appointed by the Commissioner (section 15));
- a duty to conduct risk assessments (ie, to regularly conduct risk assessments of the CII as required by the Commissioner (section 15)); and
- a duty to participate in cybersecurity exercises as required by the Commissioner (section 16).

More detailed measures for the protection of CII may be prescribed in codes of practice, standards of performance or directions issued directly to CII owners.

Within the financial sector, the TRM Notices and Guidelines issued by the MAS stipulate that financial institutions shall establish frameworks and processes for the identification of critical systems (as defined in the Notices), and shall implement IT controls to protect customer information from unauthorised access or disclosure. Such critical systems include, among others, automated teller machine systems,

systems that support payment, clearing or settlement functions, and online banking systems. The TRM Guidelines were most recently updated on 18 January 2021.

The MAS has issued the Cyber Hygiene Notices, which is a set of requirements legally binding upon financial institutions relating to the mitigation of cyberthreat risks (Cyber Hygiene Notices). The Cyber Hygiene Notices consist of separate notices that apply respectively to financial institutions such as banks, licensed financial advisers and credit card or charge card licensees.

The Cyber Hygiene Notices build upon the requirements contained in the TRM Notices and Guidelines and make it mandatory for financial institutions to:

- establish and implement robust security for IT systems;
- ensure that updates are applied to address system security flaws in a timely manner;
- deploy security devices to restrict unauthorised network traffic;
- implement measures to mitigate the risk of malware infection;
- secure the use of system accounts with special privileges to prevent unauthorised access; and
- strengthen user authentication for critical systems as well as systems used to access customer information.

Broadly summarised, the Cyber Hygiene Notices require financial institutions to implement a set of cybersecurity measures to protect and secure systems from cyberattacks. A non-exhaustive list of key measures is provided below:

- administrative accounts must be secured so as to prevent unauthorised access or use – this includes the granting of access rights on a 'need-to-use' basis, the establishment of procedures to assess and approve such grants, periodic reviews to verify their appropriateness, and other preventive controls such as password complexity, expiration, dual control and system administration duty segregation;
- security patches must be applied to address system vulnerabilities within a time frame commensurate with the risk posed by such vulnerability (including the system's criticality, the security severity of the patches and any existing controls in the IT environment). If no security patch is available, controls could be instituted to reduce risk (eg, the use of network security devices to detect and intercept malicious payloads, where a zero-day vulnerability has been identified and no patch is available);
- a written set of security standards must be available for every system – guidance in formulating these may be drawn from internationally recognised industry best practices. The system must conform to such standards, and where this is not possible controls should be put in place to reduce any resulting risk (including processes to seek dispensation from senior management);
- network perimeter defence controls must be implemented to restrict all unauthorised network traffic;
- one or more malware protection measures (eg, antivirus solution) must be implemented on every system to mitigate the risk of malware infection (where such protection measures are available and can be implemented); and
- multi-factor authentication must be implemented in respect of all administrative accounts of operating systems, databases, applications, security appliances or network devices that are critical systems, as well as all accounts used to access customer information over the internet.

Where an entity is unable to comply with any requirement by reason of being unable to exercise direct control over the system; or unable to exercise indirect control over the system by requiring the service provider to ensure compliance, and it is not reasonable to procure an alternative system provider over whom indirect control can be exercised, then compliance is not necessary to the extent that control cannot be exercised.

The Cyber Hygiene Notices came into effect on 6 August 2020, after a one-year transition period from its issue date of 6 August 2019, save for requirements pertaining to multi-factor authentication, which instead came into effect on 5 February 2021 (subject to the satisfaction of certain conditions).

Scope and jurisdiction

7 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Pursuant to the Copyright Act 2021, there are prohibitions on the circumvention of technological access control or protection measures applied to copyrighted work or other subject matter under Part 7, Division 4 of the Copyright Act 2021, the contravention of which may constitute an offence under section 439 of the Copyright Act 2021.

In addition, the provisions of the CMA, while not specifically targeted at addressing threats to intellectual property, may apply to cybercrime activities that involve threats to intellectual property.

8 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Yes. The Cybersecurity Act regulates designated CII in 11 critical sectors containing essential services such as energy as well as banking and finance. It imposes general duties on owners of CII to report prescribed cybersecurity incidents and to comply with prescribed codes of practice, standards of performance or written directions in relation to the CII, among others.

9 | Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There is no general restriction against the sharing of cyberthreat information. However, section 43 of the Cybersecurity Act provides that persons who are or who have been the Commissioner, the Minister and certain other specified officers must not, except in limited circumstances, disclose certain information that has come into such persons' knowledge in the performance of their functions or discharge of their duties under the Cybersecurity Act. Such information includes matters relating to a computer or computer system.

Other general legislation aimed at preserving the confidentiality or secrecy of certain matters may also apply to prevent the sharing of cyberthreat information in certain circumstances. For example, information that relates to official secrets may also be protected from communication under the Official Secrets Act 1935.

10 | What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following is a non-exhaustive list of cyberactivities that are criminalised in Singapore:

- it is an offence for any person to knowingly cause a computer to perform any function for the purposes of securing unauthorised access to any program or data held in any computer (eg, by hacking or using another person's login details without authority) (section 3 of the CMA);
- it is an offence for any person to cause a computer to perform any function for the purpose of securing access to a computer (whether

authorised or unauthorised) with the intent to commit or facilitate the commission of an offence involving property, fraud or dishonesty or which causes bodily harm (eg, identity theft or identity fraud) (section 4 of the CMA);
- it is an offence for any person to do any act that the person knows will cause an unauthorised modification of the contents of any computer (eg, deliberately infecting computer systems with malware and viruses) (section 5 of the CMA);
- it is an offence for any person to knowingly secure unauthorised access to any computer for the purpose of obtaining any computer service, or to perform unauthorised use or interception of any computer function (section 6 of the CMA);
- it is an offence for any person to knowingly cause unauthorised interference or obstruction of the use of a computer or of the usefulness or effectiveness of any program or data stored within a computer (eg, denial-of-service attacks) (section 7 of the CMA);
- it is an offence for any person to disclose without authority access codes for wrongful gain, unlawful purposes or with the knowledge that it is likely to cause wrongful loss (section 8 of the CMA);
- it is an offence for any person to illegally obtain, retain or supply personal information about another individual from a computer in contravention of certain provisions under the CMA (eg, selling identity card numbers or credit card information without legitimate purpose) (section 9 of the CMA);
- it is an offence for any person to obtain or retain any item with the intent to using it to commit or facilitate the commission of an offence (eg, buying or dealing in hacking tools) (section 10 of the CMA); and
- it is an offence for an organisation or individual to evade requests made by individuals to access or correct their personal data by disposing of, altering, falsifying, concealing or destroying records containing personal data or information about the collection, use or disclosure of personal data (section 51 of the PDPA). This may constitute a cyberactivity if the records were kept on a computer.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Recognising the increasingly common cross-border nature of cybersecurity threats, the Singapore government has signed a number of Memoranda of Understanding (MOUs) with foreign countries, to promote information exchange and sharing as well as to collaborate on cybersecurity capacity building. MOUs signed by Singapore include those with Australia, Canada, France, India, Korea, the Netherlands, the United Kingdom and the United States. In addition, Singapore has signed a Joint Declaration on Cybersecurity Cooperation with Germany, and a Memorandum of Cooperation on Cybersecurity with Japan.

Locally, the Singapore authorities have also introduced a number of initiatives to enhance the security standards of cloud service providers. Legislative initiatives include the Cybersecurity Act, which aims to enhance cybersecurity among essential services in 11 critical sectors. Other initiatives include the Multi-Tier Cloud Security Standard for Singapore (SS 584) issued by the Information Technology Standards Committee for voluntary adoption by cloud service providers (CSPs). The SS 584 standard provides for three tiers of security certification (Tier 1 being the base level and Tier 3 being the most stringent). Although adoption of the SS 584 standard is voluntary, certification under the SS 584 standard may be a requirement to participate in government tenders for public cloud services.

The IMDA has also issued a set of Cloud Outage Incident Response Guidelines (COIR Guidelines) for voluntary adoption by CSPs. The COIR Guidelines guide CSPs in planning for and responding to cloud outages, with a focus on operational mistakes, infrastructure or system failure and environmental issues (eg, flooding, fire).

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The Cybersecurity Act and the PDPA may be applicable to foreign organisations doing business in Singapore. The frameworks generally do not impose differing standards of regulatory obligations on the foreign organisations to which they apply, as compared with local organisations.

The framework for the protection of CII under the Cybersecurity Act applies to any CII located wholly or partly in Singapore (section 3 of the Cybersecurity Act). Moreover, section 7 of the Cybersecurity Act allows computers or computer systems that are located wholly or partly in Singapore to be designated as CII. Hence, owners of CII that are partly located in Singapore would need to comply with the requirements of the Cybersecurity Act.

Similarly, the term 'organisation' is defined under the PDPA to include any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the law of Singapore, or resident or having an office or a place of business in Singapore. Therefore, the PDPA may be applicable to foreign entities that fall under this definition of 'organisation'.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes. The Singapore authorities have introduced various non-legislative initiatives aimed at enhancing cybersecurity standards. For instance, the authorities have introduced standards and guidelines to promote security among cloud service providers.

The Cybersecurity Agency of Singapore (CSA) has also published supplementary references to help owners of critical information infrastructure (CII) proactively secure and build resilience into their systems, such as its Security-by-Design Framework, which was developed to guide CII owners through the process of incorporating security into their systems development lifecycle process.

The Singapore Computer Emergency Response Team (SingCERT), which is part of the CSA, facilitates the detection, resolution and prevention of cybersecurity-related incidents on the internet. It publishes alerts, advisories and recommendations from time to time, detailing procedures or mitigating measures for organisations to respond to new cyberthreats.

On 31 May 2019, the Personal Data Protection Commission (PDPC) issued its Guide to Data Protection by Design for ICT Systems (Design for ICT Systems Guide), which aims to assist organisations in applying Data Protection by Design principles in designing and building information and communications technology (ICT) systems, by recommending best practices to adopt at each stage of the software development lifecycle.

A non-exhaustive list of measures recommended in the Design for ICT Systems Guide includes the following:
- prior to development, a data protection impact assessment should be conducted;
- the collection of personal data by ICT systems that is not used or necessary should generally be avoided;
- when developing bespoke solutions through ICT vendors, organisations should spell out to them their data protection and security requirements, document these and ensure their fulfilment;

- prior to utilising ready-made solutions (whether purchased or open source), organisations should understand what it does to personal data entrusted to it, and should satisfy themselves that such data is adequately protected (including whether there is adequate developer support);
- updates and security patches should be applied to ICT system components as soon as possible;
- https instead of http should be utilised;
- a Web Application Firewall should be deployed; and
- code reviews, vulnerability assessments, penetration testing and user acceptance testing should be conducted.

On 25 November 2021, the CSA, in collaboration with the PDPC and Singapore Police Force, published an e-handbook, Overview of Legislations on Cybersecurity, Personal Data Protection & Computer Misuse, to explain the differences between the Cybersecurity Act, the Computer Misuse Act and the Personal Data Protection Act. The e-handbook provides an introduction to the aforementioned statutes with some case studies and also includes resources from the three agencies to assist organisations and individuals in better securing their computer systems.

14 How does the government incentivise organisations to improve their cybersecurity?

The government has publicly stated that it does not intend to provide funding to offset the costs of CII obligations that are regulatory requirements under the Cybersecurity Act. However, the government has established several schemes to enhance the cybersecurity capabilities of organisations, particularly small and medium enterprises (SMEs).

For instance, the Infocomm Media Development Authority (IMDA) has established an SME Digital Tech Hub, a dedicated hub that provides specialist digital technology advice to SMEs on areas including, but not limited to, data analytics and cybersecurity. It also works with SME Centres and Trade Association & Chambers to provide assistance in connecting SMEs with digital technology vendors and consultants, as well as conducting workshops and seminars to improve the digital capabilities of SMEs. The CSA has also tailored SG Cyber Safe cybersecurity toolkits for SME owners and employees for awareness and cybersecurity training.

The CSA and the IMDA have also established partnerships with private organisations through the Critical Infocomm Technology Resource Programme Plus, Cybersecurity Professional Scheme, Cyber Security Associates and Technologists programme and the Tech Skills Accelerator initiative. These partnerships help to train and up-skill professionals with ICT or engineering disciplines, enabling them to take on cybersecurity job roles through company-led, on-job training.

In the area of certifications and accreditations, the government has also announced that it will allow small service providers to apply for government funding to cover a proportion of the costs to become member companies of CREST. The CREST Singapore chapter has been established in collaboration and partnership with the CSA, the Association of Information Security Professionals, the Monetary Authority of Singapore (MAS), the Association of Banks in Singapore and the IMDA, and offers various certifications for cybersecurity services in Singapore.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The following publicly available industry standards and codes of practice may be accessed at the links provided:

- the Cybersecurity Code of Practice for Critical Information Infrastructure may be accessed on the CSA website at: https://www.csa.gov.sg/legislation/codes-of-practice;
- the TRM Notices and Guidelines (Notice on Technology Risk Management, and the related Technology Risk Management Guidelines) may be accessed on the MAS website at: http://www.mas.gov.sg;
- the Cyber Hygiene Notices may be accessed on the MAS website at: https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&page=1&q=cyber%20hygiene;
- the PDPC's various advisory guidelines and guides may be accessed on the PDPC website at: http://www.pdpc.gov.sg; and
- the Association of Banks in Singapore's industry guidelines on cybersecurity can be accessed on the ABS website at: http://www.abs.org.sg.

16 Are there generally recommended best practices and procedures for responding to breaches?

In the case of certain breaches involving personal data, there may be a need to notify the authorities.

The recent amendments to the Personal Data Protection Act 2012 (PDPA), which came into effect on 1 February 2021, have introduced a mandatory data breach notification obligation (Part 6A of the PDPA). In the event of a data incident, an organisation has a duty to conduct, in a reasonable and expeditious manner, an assessment of the incident to determine if it is a 'notifiable data breach'. If the data incident is a 'notifiable data breach', the organisation has an obligation to notify the PDPC of such a data breach as soon as practicable, but in any case no later than three calendar days from when the organisation makes the assessment.

A data breach is classified as a 'notifiable data breach' if the data breach results in, or is likely to result in, significant harm to the individual; or is, or is likely to be, of a significant scale (read with the Personal Data Protection (Notification of Data Breaches) Regulations 2021).

In addition, organisations are also required to notify the affected individuals of the 'notifiable data breach' in a reasonable manner, unless an exception applies. The two exceptions are: if, on or after assessing that the data breach is a 'notifiable data breach', the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data breach will result in significant harm to the affected individual.

Apart from the mandatory data breach notification obligation, PDPC's Guide on Managing and Notifying Data Breaches under the PDPA contains a number of recommendations that organisations may consider in responding to a data breach, including that an organisation should act as soon as it is aware of a data breach and consider the following measures, where applicable:

- shutting down the compromised system that led to the data breach;
- establishing whether steps can be taken to recover lost data and limit any damage caused by the data breach;
- isolating causes of the data breach in the system, and where applicable, changing the access rights to the compromised system and removing external connections to the system;
- rerouting or filtering network traffic, firewall filtering, closing particular ports or mail servers;
- preventing further unauthorised access to the system, and resetting passwords if accounts and passwords have been compromised;

- notifying the police if criminal activity is suspected and preserving evidence for investigation;
- putting a stop to practices that led to the data breach; and
- addressing lapses in processes that led to the data breach.

Information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Section 45 of the Cybersecurity Act protects the identities of informers of certain offences relating to CII. Generally, no witness in any proceedings for an offence under Part 3 of the Cybersecurity Act is obliged or permitted to:

- disclose the name, address or other particulars of an informer who has given information with respect to that offence, or the substance of the information received; or
- answer any question if the answer would lead, or tend to lead, to the discovery of the name, address or other particulars of the informer.

In addition, the court must also order any entries containing the informer's name or descriptions, which may lead to the discovery of the informer's identity, to be concealed from documents in evidence, or those available for inspection in such proceedings as mentioned in section 45(1) of the Cybersecurity Act.

Beyond the Cybersecurity Act, the Ministry of Communications and Information and CSA have stated that they intend to explore implementing administrative arrangements and partnerships to facilitate and encourage information sharing.

In the telecommunications sector, IMDA has also published a Cyber Security Vulnerability Reporting Guide to facilitate and encourage the reporting of cybersecurity vulnerabilities that the cybersecurity researcher community has detected in the public-facing applications and networks of telecommunication service providers, such as internet access, mobile and fixed-line voice and data service providers, broadcast, print (newspaper) and postal service providers.

In the financial sector, MAS has partnered with the Financial Services Information Sharing and Analysis Centre to set up a regional centre in Singapore to share information on cybersecurity threats among financial institutions.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In practice, it is not uncommon for the government to consult industry players and relevant private sector parties in developing legislative and regulatory standards. For instance, prior to the introduction of the Cybersecurity Act, the government had conducted several rounds of consultations with potential CII owners, industry associations and cybersecurity professionals. The government has also announced its intent to continue working with the industry and professional association partners to establish accreditation regimes for cybersecurity professionals.

The Singapore government has actively promoted cybersecurity through research-and-development (R&D) collaborations between government, academia and industry. In 2013, the Singapore government launched the National Cybersecurity R&D Programme to promote such research collaboration, with a total of S$190 million in funding having been made available to support the programme until 2020. The government has also kick-started other initiatives, such as the Cybersecurity Consortium with S$1.5 million in funding over three years from 2016, and the National Cybersecurity R&D Laboratory.

Grant schemes such as the Co-Innovation and Development Proof-of-Concept Funding Scheme are also available to Singapore-registered companies or overseas firms that partner with Singapore-registered companies. The scheme aims to support the co-development of innovative cybersecurity solutions that help to meet national cybersecurity needs, with potential for commercial application.

The Computer Emergency Response Teams (CERTs) overseeing specific sectors also issue advisories to the operators in their respective sectors. For example, the Info-communications Singapore CERT, or ISGCERT, issues alerts to operators in the telecommunications and media sector to enhance their cyber readiness, and advisories on cybersecurity vulnerabilities pertaining to this sector.

SingCERT also works with the sectoral CERTs, where necessary, to inform local companies and affected customers on cybersecurity threats and incidents.

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Yes, various insurance solutions covering cyber risks are offered by several insurers in the Singapore market. Such insurance solutions remain relatively new to the Singapore market, with AXA being reported to be the first insurer to commence such an offering in 2014.

ENFORCEMENT

Regulation

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Commissioner is responsible for the enforcement of the Cybersecurity Act. At present, the Chief Executive of the Cybersecurity Agency of Singapore has been appointed as the Commissioner. The Cybersecurity Act also provides for the appointment of a Deputy Commissioner and Assistant Commissioners to assist the Commissioner. The government has publicly stated that Assistant Commissioners will be appointed from officers of sector regulators, as they understand the unique contexts and complexities in their sectors.

The Singapore Police Force, which is overseen by the Ministry of Home Affairs, working together with the Public Prosecutor, is generally responsible for investigating and prosecuting criminal offences, such as those under the Computer Misuse Act 1993 (CMA).

In relation to data protection, the Personal Data Protection Commission (PDPC) is the authority responsible for administering and enforcing the Personal Data Protection Act 2012 (PDPA).

Sector regulators, such as the Monetary Authority of Singapore, which regulates the finance sector, and the Infocomm Media Development Authority, which regulates the info-communications sector, are responsible for enforcing their individual sector-specific frameworks.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Commissioner has broad powers under the Cybersecurity Act to require critical information infrastructure (CII) owners to furnish information relating to CII, including information to ascertain the level of cybersecurity of CII. The Commissioner also has broad powers to investigate cybersecurity threats or incidents generally, including those that involve non-CII, by requiring the production of documents and examining relevant persons.

Section 15 of the Cybersecurity Act requires CII owners to conduct cybersecurity risk assessments of CII and cybersecurity audits of the compliance of the CII with the statute and the applicable codes of

practices and standards of performance, and to furnish reports to the Commissioner.

With respect to investigations of cybersecurity threats or incidents, section 19 of the Cybersecurity Act sets out the powers of the Commissioner and authorised officers, which include powers to investigate cybersecurity threats or incidents for the purposes of: assessing the impact or potential impact of the cybersecurity threat or incident; preventing any or further harm arising from the cybersecurity incident; or preventing a further cybersecurity incident from arising from that cybersecurity threat or incident.

Section 20 of the Cybersecurity Act is similar to section 19, save that it sets out the powers of the Commissioner with respect to 'serious' cybersecurity threats or incidents, namely, those that satisfy the severity threshold specified in section 20(3) of the Cybersecurity Act.

Under section 19(2) of the Cybersecurity Act, the powers that are to be exercised against persons affected by the cybersecurity threat or incident include the powers to:

- require the person to attend at a specified place and time to answer questions or to provide a signed statement concerning the cybersecurity threat or incident;
- require the person to produce any record or document, or provide any relevant information;
- inspect, copy or take extracts from such records or documents; and
- examine orally the person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident.

Under section 20 of the Cybersecurity Act, the powers that may be exercised against persons affected by the cybersecurity threat or incident that satisfies the severity threshold include the powers to:

- exercise any power mentioned above in section 19(2) of the Cybersecurity Act;
- direct the person to carry out such remedial measures, or to cease carrying on such activities, in relation to the affected computer or computer system, to minimise cybersecurity vulnerabilities;
- require the person to take any action to assist with the investigation, including but not limited to: preserving the state of the affected computer or computer system by not using it; monitoring the affected computer or computer system; performing a scan of the affected computer or computer system to detect cybersecurity vulnerabilities and to assess the impact of the cybersecurity incident; and allowing the incident response officer to connect any equipment to, or install any computer program on, the affected computer or computer system as necessary;
- after giving reasonable notice, enter the premises where the affected computer or computer system is reasonably suspected to be located;
- access, inspect and check the operation of the affected computer or computer system, or use the computer or computer system to search any data contained in or available to that computer or computer system;
- perform a scan of the affected computer or computer system to detect cybersecurity vulnerabilities;
- take a copy of or extracts from any electronic record or computer program affected by the cybersecurity incident; and
- with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

Under section 40 of the Cybersecurity Act, notwithstanding any provision to the contrary in the Criminal Procedure Code 2010, a District Court of Singapore has jurisdiction to try any offence under the statute and has the power to impose the full penalty or punishment in respect of the offence.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The Cybersecurity Act is relatively novel and there have yet to be any published reports of significant enforcement actions thereunder.

In relation to data breaches involving personal data, the PDPC has been active in its enforcement of the PDPA. As of 4 December 2021, the PDPC has issued a total of 195 decisions, with a significant percentage of these decisions relating to breaches of the protection obligation, namely the requirement imposed on organisations to make 'reasonable security arrangements' to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks with respect to personal data held or processed by those organisations, and the loss of any storage medium or device on which personal data is stored (under section 24 of the PDPA).

Notably, the largest penalty the PDPC has imposed on an organisation to date (S$750,000) arose from the organisation's failure to take sufficient security steps or make the necessary arrangements to protect the personal data from unauthorised access (see *Re Singapore Health Services Pte Ltd and another* [2019] SGPDPC 3).

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

Section 14 of the Cybersecurity Act provides that the owner of a CII must notify the Commissioner within the prescribed period in the prescribed form and manner upon becoming aware of the occurrence of any of the following events:

- a prescribed cybersecurity incident in respect of a CII;
- a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with a CII; and
- any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the owner.

For this purpose, the prescribed cybersecurity incidents are set out in the Cybersecurity (Critical Information Infrastructure) Regulations 2018 and include:

- the unauthorised hacking of a CII;
- the installation or execution of unauthorised software or code on a CII;
- man-in-the-middle attacks, session hijacks or other unauthorised interception of communication between a CII and an authorised user; and
- denial of service attacks.

In relation to data breaches, recent amendments to the PDPA (which came into effect on 1 February 2021) include the introduction of a mandatory data breach notification regime. Organisations will be required to notify the PDPC of a data breach that:

- results, or is likely to result, in significant harm to the affected individuals (ie, where the compromised personal data falls within certain prescribed categories set out in the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or
- is of a significant scale (ie, 500 or more individuals).

Under this new regime, where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable

and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

Organisations will then have to notify the PDPC as soon as practicable, but in any case no later than three calendar days after determining that the breach meets the notification criteria.

Where the data breach results, or is likely to result, in significant harm to the affected individuals (ie, data subjects), organisations will also be required to notify affected individuals on or after notifying the PDPC, unless any of the stated exceptions apply, namely:

- the organisation, on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual;
- the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure that rendered it unlikely that the notifiable data breach would result in significant harm to the affected individual;
- the organisation is instructed by a prescribed law enforcement agency, or directed by the PDPC, not to notify the affected individual; or
- the PDPC, on the written application of the organisation, waives the requirement, subject to any conditions that the PDPC thinks fit.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The Cybersecurity Act provides for a number of offences, including the following:

- an owner of a CII who fails, without reasonable excuse, to comply with the duty to furnish information relating to the CII pursuant to a notice by the Commissioner, shall be liable upon conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years or to both, and in the case of a continuing offence, to a further fine not exceeding S$5,000 for every day or part of a day during which the offence continues after conviction (section 10(2));
- an owner of a CII who fails, without reasonable excuse, to comply with the duty to notify the Commissioner within 30 days of making a material change to the design, configuration, security or operation of the CII after any information has been furnished to the Commissioner pursuant to a notice given, shall be liable on conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding 12 months or to both (section 10(7));
- any person who, without reasonable excuse, fails to comply with a direction issued by the Commissioner, shall be liable upon conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years or to both, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction (section 12(6));
- any owner of a CII who fails, without reasonable excuse, to comply with the duty to conduct cybersecurity risk assessments and cause an audit of the compliance of the CII by an auditor approved or appointed by the Commissioner, and other requirements under the same provision (such as to comply with the Commissioner's directions under subsections (3), (5)(a) or (6), or obstructs or prevents an audit mentioned in subsection (4) or a cybersecurity risk assessment under subsection (5)(b) from being carried out), shall be liable upon conviction to a fine not exceeding S$100,000 or to imprisonment for a term not exceeding two years or to both, and in the case of a continuing offence, to a further fine not exceeding S$5,000 for every day or part of a day during which the offence continues after conviction (section 15(7));
- any owner of a CII who, without reasonable excuse, fails to furnish a copy of the report of the audit or cybersecurity risk assessment within 30 days after completion of such audit or assessment, shall be liable upon conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding 12 months or to both, and in the case of a continuing offence, to a further fine not exceeding S$2,500 for every day or part of a day during which the offence continues after conviction (section 15(8));
- any person who, without reasonable excuse, fails to comply with the duty to participate in a cybersecurity exercise if directed to do so by the Commissioner, shall be liable on conviction to a fine not exceeding S$100,000 (section 16(3));
- any person who, without reasonable excuse, fails to comply with a Magistrate's order under section 19(5), or who wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required by an incident response officer under section 19(2) in the investigation of a cybersecurity incident, shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding six months or to both (section 19(8)); and
- in the case of an investigation into serious cybersecurity incidents, any person who, without reasonable excuse, fails to comply with sections 19(2) or 19(5) as mentioned above, or who fails to comply with a direction, requirement or lawful demand of an incident response officer made in the discharge of the officer's duties under section 20, shall be liable on conviction to a fine not exceeding S$25,000 or to imprisonment for a term not exceeding two years or to both (section 20(7)).

In the case of a breach of the data protection provision of the PDPA, the PDPC is empowered to direct organisations to: stop collecting, using or disclosing personal data in contravention of the PDPA; destroy personal data collected in contravention of the PDPA; provide access to or correct personal data, or reduce or make a refund of any fee charged for any access or correction request; or pay a financial penalty.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Section 14 of the Cybersecurity Act provides that an owner of a CII who, without reasonable excuse, fails to comply with the duty to report any prescribed cybersecurity incident within the prescribed period shall be liable on conviction to a fine not exceeding S$100,000, or to imprisonment for a term not exceeding two years, or to both.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The Cybersecurity Act does not confer any private rights on parties to seek redress for unauthorised cyberactivity or failure to adequately protect systems and data.

Under the CMA, a court may order an offender to pay compensation to a victim of the offence. The victim may separately pursue a civil remedy against the offender, and the compensation ordered under the CMA will not prejudice the victim's right to recover more than the amount compensated under the CMA.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Sections 11 and 12 of the Cybersecurity Act impose duties on owners of critical information infrastructure (CII) to comply with the codes of practice or standards of performance, or directions either of a general or specific nature issued by the Commissioner, which may contain provisions with respect to the measures to be taken by them to ensure the cybersecurity of the CII. On 1 September 2018, the Commissioner of Cybersecurity issued the Cybersecurity Code of Practice for CII. Although its detailed requirements are not published in the public domain, the Cybersecurity Agency of Singapore (CSA) has introduced various supplementary references as additional resources to help CII owners in complying with this.

In relation to the obligation to put in place reasonable security measures to protect personal data, the Personal Data Protection Commission (PDPC) does not prescribe any 'one-size-fits-all' solution to compliance as it recognises that each organisation will need to address its own unique circumstances. For instance, PDPC's Advisory Guidelines on Key Concepts in the PDPA (revised 1 October 2021) sets out security arrangements (including administrative, physical and technical measures) that organisations may use to protect personal data.

The PDPC has also published the Guide to Securing Personal Data in Electronic Medium (Securing Personal Data Guide) to provide greater clarity on the obligation to provide 'reasonable security arrangements' in respect of personal data held or controlled by organisations.

In particular, the Securing Personal Data Guide sets out a series of good practices that organisations should undertake, including but not limited to:

- providing clear direction on information and communications technology (ICT) security goals and policies for personal data protection within the organisation;
- establishing, enforcing and periodically reviewing ICT security policies, standards and procedures;
- instituting a risk management framework to identify security threats, assessing the risks involved and determining the controls to remove or reduce them; and
- designing and implementing an internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type, etc.

The Securing Personal Data Guide also sets out a series of enhanced practices which organisations may consider, including but not limited to:

- disabling unused network ports;
- monitoring LAN and Wi-Fi regularly and removing unauthorised clients and Wi-Fi access points;
- using network proxies to restrict employee access to known malicious websites;
- using two-factor authentication and strong encryption for remote access;
- disallowing remote network administration; and
- logging database activities, such as any changes to the database and data access activities to track unauthorised activities or anomalies.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There are currently no provisions in the Cybersecurity Act or the Personal Data Protection Act 2012 (PDPA) expressly requiring organisations to keep records of cyberthreats or attacks. It may, however, be prudent for organisations to consider the need to keep records to ensure compliance with other regulatory requirements, for example, in the case of CII owners, to fulfil audit requirements, or in the case of a breach of personal data, to keep records so that they may be provided to the PDPC if it conducts an investigation into a data breach.

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Where the owner of a CII is required to notify the Cybersecurity Commissioner of a cybersecurity incident in respect of the CII, the report must be submitted within two hours of the owner becoming aware of its occurrence and must include the following details:

- the CII affected;
- the name and contact number of the owner of the CII;
- the nature of the cybersecurity incident, whether it was in respect of the CII or an interconnected computer or computer system, and when and how it occurred;
- the resulting effect that has been observed, including how the CII or any interconnected computer or computer system has been affected; and
- the name, designation, organisation and contact number of the individual submitting the notification.

Within 14 days after the initial submission, the owner of the CII must submit in writing, via the CSA's website and to the fullest extent practicable, the following supplementary details in writing:

- the cause of the cybersecurity incident;
- its impact on the critical information infrastructure, or any interconnected computer or computer system; and
- what remedial measures have been taken.

In relation to the reporting of data breaches to the authorities, the amendments to the PDPA have introduced a new mandatory data breach notification regime. If the organisation forms the view, following its assessment of a potential data breach, that the breach is 'likely to result in significant harm or impact to the individual to whom the information relates' or 'the data breach is of a significant scale' (ie, involving personal data of 500 or more individuals), the organisation must notify the PDPC and, subject to certain exceptions, would also be required to notify affected individuals.

Under the Personal Data Protection (Notification of Data Breaches) Regulations 2021, the notification to the PDPC must contain the following information:

- the date on which and the circumstances in which the organisation first became aware that the data breach had occurred;
- a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment that the data breach is a notifiable data breach;
- information on how the notifiable data breach occurred;
- the number of affected individuals affected by the notifiable data breach;
- the personal data or classes of personal data affected by the notifiable data breach;
- the potential harm to the affected individuals as a result of the notifiable data breach;

- information on any action by the organisation, whether taken before or to be taken after the organisation notifies the PDPC of the occurrence of the notifiable data breach:
  - to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and
  - to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
- information on the organisation's plan (if any) to inform, on or after notifying the PDPC of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach; and
- the business contact information of at least one authorised representative of the organisation.

The notification to the PDPC must also be in the form and manner specified on the PDPC's website at: www.pdpc.gov.sg.

As for notification to individuals, the notification must contain the following information:

- the circumstances in which the organisation first became aware that the notifiable data breach had occurred;
- the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach;
- the potential harm to the affected individual as a result of the notifiable data breach;
- information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual:
  - to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and
  - to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
- the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the individual's personal data affected by the notifiable data breach; and
- the business contact information of at least one authorised representative of the organisation.

Apart from the PDPC, where criminal activity (eg, hacking, theft or unauthorised system access by an employee) is suspected, organisations should consider alerting the police and preserving evidence for police investigation. Where a case of cyberattack is suspected, organisations should also consider alerting the CSA through the Singapore Computer Emergency Response Team.

Within the financial sector, the Notice on Technology Risk Management issued by the Monetary Authority of Singapore (MAS) requires financial institutions to notify MAS as soon as possible, but not later than one hour, upon the discovery of a relevant IT incident. The Notice also requires the financial institution to submit a root-cause and impact analysis report in respect of the IT incident to MAS within 14 days or such longer period as MAS may allow, from the discovery of the relevant IT incident.

Time frames

30 | What is the timeline for reporting to the authorities?

Section 14 of the Cybersecurity Act sets out that the owner of a CII must notify the Commissioner within the prescribed period upon becoming aware of the occurrence of the cybersecurity breaches described above.

The prescribed period is set out in regulation 5 of the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (CII Regulations), which sets out that a CII owner must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in the required form within two hours after becoming aware of the occurrence, and provide, within 14 days of the initial submission, the following supplementary details:

- the cause of the cybersecurity incident;
- its impact on the CII, or any interconnected computer or computer system; and
- what remedial measures have been taken.

In relation to the reporting of personal data breaches to the authorities, the recent amendments to the PDPA (which took effect on 1 February 2021) have introduced a new mandatory data breach notification regime. Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. If the organisation determines that the data breach is notifiable, it must then notify the PDPC as soon as practicable, but in any case no later than three calendar days after determining that the breach meets the notification criteria.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no provisions within the Cybersecurity Act that expressly require organisations to report threats or breaches to others in the industry, to customers or to the general public.

In relation to notification of data breaches involving personal data to the public, the amendments to the PDPA (which came into effect on 1 February 2021) require organisations to notify affected individuals of the data breach, unless an exception applies. Specifically, organisations must, on or after notifying the PDPC, notify the individuals affected by a notifiable data breach, if the data breach results in, or is likely to result in, significant harm to an affected individual. The notification should be in the form and manner as prescribed and contain information to the best of the knowledge and belief of the organisation at the time.

However, there are exceptions to this requirement. Organisations do not need to notify the affected individuals if one of the stated exceptions applies, namely, if the organisation:

- takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- has implemented, prior to the occurrence of the notifiable data breach, any technological measure that rendered it unlikely that the notifiable data breach would result in significant harm to the affected individual.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Significant amendments to the Personal Data Protection Act 2012 (PDPA) have recently been introduced under the Personal Data

Protection (Amendment) Bill 2020 (PDP (Amendment) Bill 2020), which was passed in Parliament on 2 November 2020. This marks the first comprehensive review of the PDPA since its enactment in 2012. Most of the provisions of the PDP (Amendment) Bill 2020 came into effect on 1 February 2021.

The amendments under the PDP (Amendment) Bill 2020 seek to: strengthen the accountability of organisations in respect of the handling and processing of personal data; enhance the legal framework for the collection, use and disclosure of personal data; provide individuals with greater autonomy over their personal data; and enhance the enforcement powers of the Personal Data Protection Commission (PDPC).

Key amendments include new provisions on mandatory data breach notification, data portability, processing of personal data for legitimate purposes and a new offence relating to unauthorised re-identification of anonymised information. The PDP (Amendment) Bill 2020 also increases the maximum financial penalty that may be imposed for a contravention to 10 per cent of the organisation's annual turnover in Singapore or S$1 million, whichever is higher.

While most of the provisions of the PDP (Amendment) Bill 2020 have already come into effect, certain provisions will only come into effect at a later date. The provisions that have yet to come into effect include provisions relating to data portability, and provisions increasing the maximum financial penalty for a contravention of the obligations under the PDPA to up to 10 per cent of the organisation's annual turnover in Singapore or S$1 million, whichever is higher.

In September 2021, the CSA conducted a public consultation to seek industry feedback on the proposed licence conditions and draft subsidiary legislation under the licensing framework for cybersecurity service providers found in Part 5 of the Cybersecurity Act. The CSA stated that it will license only two types of service providers: those providing penetration testing and managed security operations centre monitoring services. The public consultation commenced on 20 September 2021 and closed on 18 October 2021. The licensing framework for cybersecurity service providers is expected to be implemented by early 2022.

Lim Chong Kin
chongkin.lim@drewnapier.com

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315
Tel: +65 6531 4110
www.drewnapier.com

Switzerland

Michael Isler, Jürg Schneider and Hugh Reeves

Walder Wyss Ltd

LEGAL FRAMEWORK

Legislation

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

No overarching cybersecurity legislation has been adopted in Switzerland to date, and there are also no plans to comprehensively address the issue in a bespoke legal instrument. Rather, cybersecurity is and will remain regulated by a patchwork of various acts and regulatory guidance. Currently, the sole clear exception to this rule is the Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV) of 27 May 2020, which entered into force on 1 July 2020. The CyRV governs the organisation of the federal administration from a cyber risks protection standpoint. It therefore regulates the tasks of federal cybersecurity bodies, provides for a competence centre – the National Cyber Security Centre (NCSC) – and moreover regulates various compliance aspects regarding external service providers that contract with the federal administration. On 18 December 2020, Parliament approved a draft Information Security Act the aim of which is to bolster proper information security practices within all levels of the federal government.

The pertinent legislative and policy landscape has been analysed in a report concerning the national strategy on the protection of Switzerland from cyber risks, which was first approved by the federal government in 2012 and was updated in April 2018 for the 2018–2022 period. In summary, the April 2018 report outlines the existing cybercrime defence scheme, defines the main goals for enhancing protection against cyber risks and is based on the headway achieved between 2012 and 2017. After identifying the risks that originate from cyberthreats, the report identifies major weaknesses and resolves how the various stakeholders should proceed. The strategy focuses on seven objectives:

- Switzerland's disposal of the necessary skills, knowledge and capabilities to identify and evaluate cyber risks;
- the preparation and enforcement of measures to mitigate cyber risks;
- capabilities and structural organisations that can rapidly identify and address cyber incidents;
- ensuring Switzerland's IT resilience;
- a clear definition of the respective responsibilities and competencies of the various actors;
- involvement in the international dialogue to increase cybersecurity; and
- learning the lessons from cybersecurity incidents in Switzerland and abroad.

The report ultimately proclaims 29 measures (up from 16 in the 2012 report) aimed at minimising cyber risks and enhancing cybersecurity. Several of these measures are dedicated to the validation and implementation of the existing and prospective legal and regulatory instruments. The report acknowledges that the existing scattered legal framework is inconsistent and incomplete, but also opines that the adoption of a comprehensive cybersecurity regime would be inappropriate for addressing cyber risks. Rather, the existing legislative framework will be subject to continuous adjustment by taking into account the specific exposure to cyber risks within the relevant scope of application of each statute. Moreover, the report expresses the intent to reach minimum standards in terms of cybersecurity that should be coordinated at the international level. In May 2019, the Federal Council adopted the implementation plan for the national cybersecurity strategy for 2018–2022. This plan, in particular, sets out more precisely the timeline for the roll-out of the various steps and measures.

The aforementioned national cybersecurity strategies (for 2012–2017 and 2018–2022 respectively) partially overlap with another governmental initiative, the Digital Switzerland strategy, which was first adopted in spring 2016 and replaced in September 2018. The Digital Switzerland strategy is reviewed on a biennial basis and addresses any topic relevant to digitalisation, not just cybersecurity. The associated action plan features, inter alia, an increase of cybersecurity in the fields of automated vehicles and aviation security.

The following list sets out the most relevant legislative instruments dealing explicitly or implicitly with cybersecurity in the private sector (ie, excluding the CyRV, as it pertains to the federal administration).

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime (CCC) entered into force in Switzerland on 1 January 2012 and imposes the following main obligations on member states with respect to cybercrime:

- harmonisation of substantive criminal laws;
- adoption of expedient investigation and prosecution measures; and
- establishment of a fast and effective regime of international cooperation.

Switzerland's adherence to the CCC brought about some light amendments to the Swiss Penal Code (SPC) and the Federal Act on International Mutual Assistance in Criminal Matters to render domestic law compliant with the prerequisites of the convention.

Federal Data Protection Act

The Federal Data Protection Act (FDPA) governs the protection of personal data, which encompasses information pertaining to identified or identifiable natural persons and legal entities. Pursuant to article 7 of the FDPA, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Enforcement of the data security principles is largely left to self-control by the concerned organisations and, eventually, civil courts; regulatory oversight by the Federal Data Protection and Information Commissioner in the area of data security, therefore, only exists in isolated cases and is

non-existent on a large scale. In the wake of the adoption of the General Data Protection Regulation within the European Union, a fundamental revision of the FDPA and its implementing ordinance took place.

On 25 September 2020, Parliament approved the draft revised FDPA. On 23 June 2021, Parliament published a preliminary draft of the revised implementing ordinance. Entry into force should occur during the second half of 2022, though no exact date has yet been communicated. This revised legislation will bring about wide-ranging changes not only to the FDPA itself but also to various other laws insofar as they touch upon data protection issues. In particular, legal entities will no longer benefit from dedicated data protection, transparency will be strengthened, data breaches will have to be notified in most cases and the criminal sanctions for offences against the FDPA will be bolstered. As far as data security is concerned, however, the matter has not been specifically or exhaustively addressed as a standalone subject and, rather, will remain part of the subject matter of the revised FDPA and its ordinance (as is the case under current law).

Federal Telecommunications Act

Pursuant to article 48a of the Federal Telecommunications Act (TCA) and article 96 of the corresponding Ordinance on Telecommunications Services (OTS), the Federal Office of Communications (OFCOM) is responsible for implementing the administrative and technical requirements pertaining to the security and availability of telecommunications services, which includes notification of the regulator in the event of security incidents. This body of laws was also revised to render it more compliant with the current technological landscape. The revised TCA, OTS and other implementing and technical ordinances entered into force on 1 January 2021. In particular, rules against unsolicited messaging and spamming are reinforced, though it can also be noted that the revised provisions on addressing resources seek to minimise risks of cybercriminality. Moreover, the Federal Act on the Surveillance of Postal and Telecommunications Traffic of 6 October 2010 governs information requests and real-time and retroactive monitoring of postal and telecommunications traffic and has been revised, with the new law having entered into force on 1 March 2018.

In addition, the Federal Act on the Intelligence Service has also been revised, having entered into force on 1 September 2017. This Act governs the monitoring of data streams to and from Switzerland to fulfil antiterrorism and national security objectives. In this respect, on 25 September 2020, Parliament adopted a new act on police measures for combatting terrorism. This law, which grants the authorities extensive powers – including online surveillance – to combat terrorism, was approved during a nationwide referendum in June 2021, though it has not yet entered into force.

Further, pursuant to article 15 of the Ordinance on Internet Domains (which has been revised, with entry into force of the revised text on 1 January 2021 – see above), the registry for the '.ch' top-level domain (currently the SWITCH foundation) is required, if requested by an OFCOM-accredited body, to combat cybercrime or to block domain names if there are reasonable grounds to suspect that they are being used to access sensitive data using illegal methods (phishing) or to distribute harmful software (malware). The only organisation entitled to accomplish this task is the NCSC, as it now incorporates the former Reporting and Analysis Centre for Information Assurance (MELANI).

Federal Act on Financial Market Infrastructure

The Federal Act on Financial Market Infrastructure (FinMIA), which entered into force on 1 January 2016, regulates the organisation and operation of financial market infrastructures, such as stock exchanges, multilateral trade systems, central deposits and payment systems. Article 14 of the FinMIA demands robust IT systems that are capable of deploying effective emergency responses and ensuring business continuity. The obligations are further detailed in article 15 of the implementing ordinance of the FinMIA. The systems must be designed to:

- ensure availability, confidentiality and integrity of data;
- enable reliable access controls; and
- provide features to detect and remedy security incidents.

Financial market infrastructures are under the regulatory surveillance of the Swiss Financial Market Supervisory Authority (FINMA).

The FinMIA is the first sector-specific federal act applicable to private undertakings that expressly acknowledges the high dependency of essential infrastructure on information technology and the vulnerability to which it is exposed owing to the interconnectivity of the market players' systems.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The focal zone of regulatory activity in the area of cybersecurity in Switzerland is the financial sector. In the aftermath of the financial crisis, the banking sector suffered from severe data leaks, albeit not primarily as a result of cyberattacks, which have greatly increased awareness of the importance of data security in general. Consequently, FINMA amended its Circular 2008/21 on the operational risks of banks by adding a new chapter on the security of electronic data. Annex 3 to the Circular now sets forth a number of principles and guidelines on proper risk management related to the confidentiality of client-identifying data stored electronically. FINMA makes it clear that state-of-the-art data security standards and procedures, as well as proper incident management, are pivotal. The main message conveyed is that cybersecurity must become a matter of top management attention. FINMA further enhanced the required security standards through an amendment of Circular 2008/21, with effect from July 2017. Specifically, management is required to implement a cyber risk management concept, which also entails regular vulnerability assessments and penetration tests.

Another important instrument of financial sector oversight relevant to cybersecurity is FINMA Circular 2018/3 regarding outsourcing at banks and insurance companies. It increases the transparency of the outsourced tasks by introducing an inventory of these tasks. Further, the (financial) institution and the service provider must draw up a security framework to ensure that the outsourced function can continue to be performed in an emergency. In contrast to prevailing trends in regulatory activity and contrary to the previous version of the Circular, the Circular does not contain provisions on data protection, to avoid duplication with the FDPA.

Both FINMA Circulars 2008/21 and 2018/3 have been slightly amended to include more pragmatic provisions for small banks. These revised texts entered into force on 1 January 2020.

Another emphasis lies on the protection of critical infrastructure from cyberthreats, such as in the electricity, transportation and telecommunications sectors. The healthcare sector has also received increasing attention recently, in particular, regarding the vulnerability of medical devices connected to the internet as well as in relation to the implementation of the electronic patient record. In this respect, it has been pointed out that a decentralised approach as adopted in Switzerland, despite its apparent disadvantages in terms of efficiency and interconnectivity, reduces the risk of a single point of failure and as such enhances data security. However, in small and medium-sized enterprises cybersecurity has not made it to the agenda of many board meetings as an item of strategic importance, but continues to be treated as a mere technicality. Nevertheless, there is a growing awareness among these enterprises that cybersecurity should become a top-level concern and must be addressed on a permanent and dynamic basis.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Adherence to international standards related to cybersecurity (such as ISO 27001:2013) is not mandatory in Switzerland. However, many undertakings are undergoing certification voluntarily, and those standards also serve as a benchmark when it comes to compliance with best practices as, for example, imposed by the regulator in the financial sector or by customers outsourcing their information and communications technology operations to third parties.

Further, pursuant to article 11 of the FDPA, the manufacturers of data processing systems or programs, as well as private undertakings that process personal data, may submit their systems, procedures and organisations to be evaluated by an accredited independent certification body on a voluntary basis. If they do so (which is very rare), abidance by the standards of ISO 27001:2013 is a prerequisite for this certification.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

As a matter of principle, responsibility for cybersecurity lies with the data processing organisation and not with the individuals entrusted with the task. Failure to comply with the data security requirements enshrined in article 7 of the FDPA does not constitute a criminal offence and, therefore, solely provides civil (tort) remedies to the persons (including legal entities) affected by a breach. It must, however, be noted that this situation is likely to change after the entry into force of the revised FDPA. Indeed, the revised FDPA criminalises intentional violations of basic data security requirements.

However, the ultimate responsibility for the overall strategy as regards cybersecurity, particularly the determination of the appropriate internal organisation as well as the adoption of the necessary directives, processes and controls, is vested in the board of directors of the company. This is certainly the case with respect to cyber risks that may have an impact on the accuracy of the company's financial statements and, therefore, need to be monitored by an internal control system, which forms part of the statutory audit scope but may arguably be extended beyond that. Given the increasing importance and awareness of cybersecurity, the problem can no longer be simply delegated to the IT department. In this context, pursuant to article 754 of the Swiss Code of Obligations, the members of the board of directors and other executive directors are personally liable both to the company and to the individual shareholders and creditors for any loss or damage arising from any intentional or negligent breach of their duties. Hence, personal liability of the responsible individuals may materialise if a company suffered loss because of a severe data breach that resulted from a lack of appropriate internal cybersecurity controls and procedures.

5 How does your jurisdiction define cybersecurity and cybercrime?

The CyRV, which is not an overarching law but rather targets structural and organisational matters within the federal administration, defines 'cybersecurity' as follows in article 3a: 'The situation in which the processing of data, in particular the exchange of data between persons and organisations via information and communication infrastructures, operates as intended' (authors' translation).

Traditionally, because Swiss legislation is technologically neutral and instead mostly relies on general rules and definitions, cybersecurity is usually closely associated with the notion of data security, being specified that data security is not a comprehensively defined notion and should rather be seen as an evolving concept.

The national strategy reports on cyber risks adopted by the federal government in 2012 and 2018 define cybersecurity as protection from disruptions of and attacks against information and communication infrastructures. Hence, the term would embrace both pertinent operational reliability and extraneous vulnerability concerns.

In line with the scope of application of the CCC, it can be argued that, outside heavily regulated sectors, the inclusion of cybersecurity provisions in legislation is equated with defence against cybercrime, namely repressive sanctions and procedures in relation to crimes committed via the internet, whereas preventive security measures are dealt with as a secondary concern of data privacy.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Pursuant to article 7 of the FDPA, personal data (namely, all information relating to an identified or identifiable person) must be protected against unauthorised processing through adequate technical and organisational measures, commensurate with the type of personal data being processed. Given these vague requirements, and even though the FDPA stipulates minimum protective measures, there is a large margin of discretion as to what these minimum requirements would precisely entail. This picture will remain fundamentally unchanged under the revised FDPA as it follows the same logic in terms of technical and organisational requirements.

Even in heavily regulated sectors, such as critical infrastructures, the minimum protective measures are rarely defined. The organisations running the infrastructure are deemed best positioned to assess and implement the actual level of cybersecurity needed for their specific operations and risk exposures. The government would only intervene where self-regulation fails. However, the national cyber risk strategy acknowledges a desire and need to devise more authoritative cybersecurity standards. An interesting observation is that the competitive landscape would not allow the adoption of more stringent (and costly) security requirements on a national level without simultaneous international harmonisation.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no specific legislation in Switzerland that deals with cyberthreats to intellectual property. Nevertheless, article 39a of the Swiss Federal Copyright Act prohibits the circumvention of effective technological measures for the protection of works and other protected subject matter (digital rights management (DRM)). DRM refers to technologies and devices such as access control, copy control, encryption, scrambling and other modification mechanisms intended and suitable for preventing or limiting the unauthorised use of intellectual property. It is unlawful to manufacture, import, offer, transfer or otherwise distribute, rent, give for use and advertise; possess for commercial purposes, devices, products or components; or provide services that purport the circumvention of DRM.

These prohibitions may not be enforced against persons who are permitted to circumvent DRM by virtue of statutory permission, such as the use of copyrighted work for private purposes or other statutory fair use limitations. It is against this background that the federal government established a surveillance office that monitors and reports on the effects of DRM and acts as a liaison between user and consumer groups. Given its mandate, the surveillance office focuses on the abusive use of

DRM systems by the industry rather than on cyberthreats to intellectual property.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The regulation of cybersecurity in critical infrastructure is fragmented and inconsistent. Although some legislative instruments deal with protection against cyber risks, they generally lack a precise definition of the required security measures. The same conclusion was reached by a report dealing with the national strategy for the protection of critical infrastructure, which was endorsed by the government in 2012 and revised in 2017 for the years 2018 to 2022, though the latter revised report does note a positive legislative trend towards better resilience and clearer security measures.

The primary responsibility to establish suitable controls and procedures lies with the organisations operating critical infrastructure. In the case of the need for governmental intervention, it would, in the majority of cases, be the competent regulator's task to define the appropriate measures. For instance, OFCOM may issue technical and administrative regulations concerning the handling of information security, the obligation to report faults in the operation of networks and other measures that make a contribution to the security and availability of telecommunications infrastructures and services (article 96, paragraph 2 OTS). In the financial sector, it is up to FINMA to adopt the necessary measures by way of circulars and regulatory notices (article 7 of the Financial Market Supervision Act).

The regulatory activities are seconded by the NCSC, which is a multidisciplinary body sponsored by the federal government and, inter alia, responsible for counselling a closed circle of roughly 140 operators of critical infrastructure in cybersecurity issues by:

- informing them of cyber incidents and threats;
- providing analyses for early detection and evaluation of cyberattacks and incidents; and
- examining malicious code.

In June 2019, the Swiss Federal Council appointed a Cyber Security Delegate, who now leads the newly created National Cyber Security Centre. The primary purposes of the NCSC and the Cyber Security Delegate are to provide dedicated competencies and skills in the cybersecurity area, serve as a contact point for the government, the media and the general public and raise awareness around matters of cybersecurity and the related risks.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Pursuant to telecommunications secrecy governed by article 43 of the TCA, any person who is or was entrusted with providing tasks pertaining to telecommunications services must not disclose information relating to subscribers' communications or give anyone else the opportunity to do so. The range of addressees of telecommunications secrecy is very broad and encompasses not only telecommunications operators but also all stakeholders that are active in the delivery of telecommunications services, including any auxiliaries entrusted in full or in part with the provision of telecommunications services on behalf of service providers.

Telecommunications secrecy prohibits not only disclosure of communications content (including peripheral data) to third parties but also the interception of such content by the addressees of the telecommunications themselves, subject to the following limitative exemptions:

- lawful interception in accordance with the prerequisites of the Federal Act on the Surveillance of Postal and Telecommunications Traffic;
- filtering of malicious content causing damage to the telecommunications network (viruses, etc) and unsolicited mass advertising; and
- processing of peripheral data for billing and debt collection purposes.

Telecommunications secrecy does not provide for a clear exemption with respect to filtering of malicious content. However, according to article 321-ter, paragraph 4 of the SPC, breach of telecommunications secrecy for the sake of preventing damage is justified and, therefore, not subject to prosecution. However, pursuant to article 49 of the TCA, the falsification or suppression of information by a person involved in the provision of telecommunications services constitutes a criminal offence. In a synthesis of these two partially contradicting provisions, the following conditions will apply:

- the filtering must be carried out in an automatic manner to the effect that no individual is capable of taking notice of the content of the information; and
- the objective of the filtering process must be confined to the suppression of the malicious code.

Suppression of the entire message is only permissible if:

- there are no other means of preventing the malicious code from being transmitted; and
- the sender and the intended recipient of the message are informed about the suppression.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following cybercrimes are sanctioned pursuant to the SPC:

- unauthorised obtaining of data (article 143);
- unauthorised access to a data processing system (article 143-bis);
- damage to data (article 144-bis);
- computer fraud (article 147);
- breach of secrecy or privacy through the use of an image-carrying device (article 179-quater);
- obtaining personal data without authorisation (article 179-novies);
- industrial espionage (article 273); and
- breach of the postal or telecommunications secrecy (article 321-ter).

Further, the TCA stipulates criminal sanctions where private information received through means of a telecommunication device is used or disclosed to third parties without permission (article 50 TCA), or of the establishment or operation of a telecommunications installation with the intention to disturb telecommunications or broadcasting (article 51 TCA). In addition, the processing of data on external devices by means of transmission using telecommunications techniques without informing users thereof is prohibited (article 45c TCA) and constitutes a misdemeanour. Lastly, the transmission of mass advertising through telecommunication channels (spam) constitutes an act of unfair competition and is criminalised as such.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Although cloud services have become increasingly popular in Switzerland, there are no specific hard-law provisions with regard to the security requirements of cloud computing. Accordingly, the general data protection provisions apply. If personal data is processed in the cloud by a provider, the processing regularly qualifies as data processing by a third party on behalf of the principal in accordance with article 10a of

the FDPA. Pursuant to this provision, the processing of personal data may be outsourced to a cloud provider by agreement or by law if the data is processed only in the manner permitted for the principal itself and the outsourcing is not prohibited by a statutory or contractual duty of confidentiality. Moreover, the principal must ensure that the provider guarantees appropriate data security. Depending on the sensitivity of the data processed in the cloud, this may entail an obligation of the principal to conduct security audits, which will often be unrealistic in a cloud setting. In practice, principals will largely rely on the cloud providers' data security certifications; however, they provide no guarantee that the provider in practice heeds these respective security controls and procedures.

Additionally, cloud computing will frequently entail cross-border disclosure of personal data. According to article 6 of the FDPA, personal data must not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular owing to the absence of legislation in the country of import that guarantees an adequate level of data protection. However, even in the absence of comparable privacy legislation, cross-border disclosure through cloud services is generally permissible if sufficient alternative safeguards (in particular, contractual clauses) substitute for an adequate level of data protection. Given that in Switzerland data pertaining to legal entities is, in contrast to many foreign (including European) data protection laws, qualified as personal data, outsourcing to the cloud in a cross-border setting may often trigger the obligation to enter into contractual guarantees; however, the revised FDPA does away with the qualification of legal entities as data subjects, and the divergence between Swiss and EU law is thus expected to be evened out in this respect with the entry into force of the revised FDPA.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

There are no particular cybersecurity regulations specifically applicable to foreign organisations doing business in Switzerland. Under Swiss conflict of law rules, a foreign organisation generally needs to observe the provisions of the FDPA if it processes personal data in Switzerland or if data subjects resident in Switzerland are affected, even if the organisation is domiciled abroad. As a general rule, sectorial regulatory requirements pertaining to data security must be observed by Swiss branches or representations of foreign organisations.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The National Cyber Security Centre (NCSC) and its precursor, the Reporting and Analysis Centre for Information Assurance (MELANI), adopted recommendations for small and medium-sized enterprises with regard to best practices for removing malware, cleaning up websites, protecting industrial control systems and content management systems, securing e-banking and countering distributed denial-of-service attacks. They are partially based on recommendations issued by the US Industrial Control Systems Cyber Emergency Response Team.

14 How does the government incentivise organisations to improve their cybersecurity?

Apart from the services provided by the Cyber Security Delegate and the NCSC, the government also has a stake in the public-private partnership Swiss Cyber Experts, which is an alliance of cybersecurity experts in the information and communications technology and sciences industries and the public and private sectors. The Swiss Internet Security Alliance is a similar project that aims to reduce the infection rate of devices within Switzerland. Further, cybersecurity projects occasionally receive a grant from Innosuisse, which is a federal innovation promotion agency responsible for encouraging science-based innovation in Switzerland by providing financing, professional advice and networks. Moreover, the government has set up a 'cyber defence campus' at the federal technology institutes (namely, ETH in Zurich and the EPFL in Lausanne).

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The pertinent industry norms, such as ISO 27001:2013, can be obtained from the Swiss Association for Standardisation (www.snv.ch). Further, the NCSC provides some additional guidance (www.ncsc.admin.ch).

16 Are there generally recommended best practices and procedures for responding to breaches?

Victims of cyberattacks are encouraged to share information and to report incidents to the supporting units maintained by the federal government (to the NCSC, which issues alerts and helps to coordinate the response to cyberattacks).

Information sharing

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Victims of cyberattacks are encouraged to notify incidents to the NCSC. The report can be made by a simple message on the NCSC's website and may be submitted anonymously. The NCSC looks to be a central point of contact in all matters relating to cybersecurity and is therefore the primary (federal) governmental body in this respect.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The national strategy for the protection of Switzerland against cyber risks, which was first adopted by the government in 2012 and updated in 2018, has identified a desire within the industry for intensified cooperation between the public authorities, the private sector and operators of critical infrastructure to mitigate cyber risks. Stakeholders expect increased consistency in the elaboration of standards and procedures to be devised in a cooperative manner. The government also holds that the primary responsibility to fight cyberattacks lies with each responsible organisational unit individually, and the authorities are only supposed to interfere if public interests are at stake or if the relevant risks cannot be addressed at the competent subordinate level. In line with this strategy, the government is a stakeholder in private initiatives dedicated to the enhancement of cybersecurity awareness and defence schemes.

Insurance

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

At the beginning of 2013, the first insurance company started to offer insurance for cybersecurity in Switzerland. Since then, several Swiss insurance companies have followed this example and offer coverage for cyber risks. The risks covered by this insurance vary and include, for

example, the loss or theft of data, unwanted publication of data, damage resulting from hacking and malware, or costs ensuing from investigations or crisis management as a result of cybercrime.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

On a general scale, the following authorities are primarily responsible for enforcing cybersecurity regulations affecting the private sector:

- the Federal Data Protection and Information Commissioner (FDPIC), who is responsible for the supervision of private undertakings with regard to their compliance with the Federal Data Protection Act (FDPA); and
- the Cybercrime Coordination Unit Switzerland, which forwards cases of incoming reports to the appropriate prosecution authorities in Switzerland and abroad (namely the police and public prosecutors in charge of prosecuting cybercrimes), it being specified that the Cyber Security Delegate and the National Cyber Security Centre also serve as valuable contact points for matters pertaining to cyber security and cyber risks.

On a sectoral level, the authorities entrusted with regulatory oversight are also responsible for enforcing compliance of the regulated undertakings with cybersecurity rules. In crisis situations affecting critical infrastructure, the special task force for information assurance would intervene. It is composed of decision-makers from the public and private sectors dealing with critical infrastructures. The latter are involved in power supply, emergency and rescue services, banks and insurance companies, telecommunications, transport and traffic, and public health (including water supply), as well as the government and public administrations.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

A distinction must be drawn between the general economy and regulated sectors.

On a general level, the FDPIC is endowed with powers to investigate cases on his or her own initiative or at the request of a third party if methods of data processing are capable of breaching the privacy of a larger number of persons (conceptual systemic failures). This could, for instance, be the case if a specific undertaking processing a large volume of sensitive personal data is suspected of neglecting data security obligations. However, the investigative powers would not extend to the examination of data breaches. In the performance of his or her duties, the FDPIC is empowered to request files, obtain information and investigate data processing mechanisms. The FDPIC does not, however, have enforcement powers; he or she may only issue recommendations. If these recommendations are not complied with, the FDPIC may institute proceedings before the Swiss Federal Administrative Court. By contrast, the text of the revised FDPA gives the FDPIC the authority to issue binding decisions and take the administrative measures that he or she deems necessary.

In regulated sectors, the authorities do have extended investigative powers within their field of competence. By way of example, the Swiss Financial Market Supervisory Authority (FINMA) may appoint independent experts to conduct audits of supervised persons and entities, which must provide the experts with all the information and documents required to carry out their tasks.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

Switzerland has experienced increased exposure to cyber incidents in recent years, with ransomware and identity theft being among the top issues. More specifically, the Reporting and Analysis Centre for Information Assurance (MELANI) – now part of the National Cyber Security Centre (NCSC) – observed an increase of incidents concerning ransomware, including the expansion of ransomware as a service, as well as usurpation of the names of various federal authorities or companies (such as the Swiss Post and Swisscom). Since 2018, MELANI has been flagging the widespread use of ransomware affecting not only private actors but governmental bodies as well. Over the course of 2019, MELANI highlighted the propagation of the latest generations of ransomware, namely Ryuk, GandCrab, Dharma, LockerGoga, MegaCortex and RobbinHood. MELANI moreover noted that sports organisations based in Switzerland (which is a hub for the sports world) have been the targets of numerous cyberattacks, and CEO fraud has been another frequent occurrence.

A noteworthy event in 2019 occurred when, on 6 June 2019, an important share of European mobile internet traffic transited through the network of China Telecom. This was the result of an error attributed to the Swiss data centre Safe Host and affected the services of several European providers and, most importantly, Swisscom. The most notable event, however, surfaced in spring 2016, when it was revealed that the Swiss defence technology company RUAG had been the victim of cyber-espionage since 2014, resulting in a loss of approximately 23 GByte of data. The government decided to have the report of the technical analysis conducted by MELANI published to give organisations the chance to check their networks for similar infections and to show the modus operandi of the attacker group.

On a judicial level, the expectations of expedited international cooperation in combatting cybercrime propagated by the Budapest Convention on Cybercrime (CCC) suffered a setback by a landmark decision handed down by the Swiss Federal Supreme Court in January 2015: the judges ruled that cantonal prosecutors were not empowered to bypass judicial assistance and order Facebook to release the IP history of its users by virtue of article 32 of the CCC. With respect to cybersecurity regulations, new rules on the treatment of electronic client data by banks adopted by FINMA entered into force at the beginning of 2015, with a revision tightening the rules entering into force in July 2017. These amendments have enhanced cybersecurity awareness in the financial sector. More recently, in a July 2020 decision, the Federal Supreme Court ruled that, in a client-bank relationship, clients bear the (contractually allocated) risk of being hacked, save for cases of the bank's gross negligence. This specific matter involved a situation where a third party hacked into the client's email accounts and sent inaccurate transfer orders.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

Switzerland currently does not have a general duty to notify cybersecurity breaches; any reporting is currently done on a voluntary basis, typically via the NCSC. The Swiss government is nevertheless contemplating introducing this obligation in the context of its 2018–2022 national cybersecurity strategy. Consequent to a 13 December 2019 report, the Federal Council initiated a consultation period, ending on 14 April 2022, regarding the introduction of reporting duties for cyber incidents affecting critical national infrastructures. Under the contemplated setup, operators of critical infrastructures would need to notify

the NSCS of certain cyber attacks; the NCSC would then provide support, information and coordination duties.

The revised FDPA also contains a duty to report violations of data security that have a likelihood of inducing a high risk for the personality or the fundamental rights of a data subject. This duty to report would not systematically call for the data subjects to be informed but would be applied only if the FDPIC orders it or if it is necessary to protect the data subject.

Sector-specific regulations may nonetheless call for notification, as is the case in the banking sector where FINMA Circular 2008/21 requires that banks implement a clear communication strategy in case of grave incidents pertaining to the confidentiality of client-identifying data.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

If a recommendation made by the FDPIC in the course of an investigation (referred to in 'Regulation') is not complied with or is rejected by the affected entity, the matter may be referred to the Swiss Federal Administrative Court for a decision. There is also the right to appeal against the decision before the Swiss Federal Supreme Court. However, there are no penalties associated with this. The revised FDPA contains provisions under which failure to follow the basic data security requirements may lead to a criminal fine.

Failure to comply with rulings of regulatory authorities may constitute a criminal offence or entail administrative sanctions depending on the applicable statute.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In the absence of a general obligation to report cyberthreats and data breaches, there are no criminal or administrative penalties associated with a failure to do so. In regulated sectors, failure to submit a required report to the regulatory authority may be prosecuted as a crime or entail administrative sanctions depending on the applicable statute. However, the text of the revised FDPA calls for data breaches to be notified to the FDPIC, unless an exception applies (see 'Policies and procedures' for further details on the notification of data breaches). This reporting obligation, if not heeded, may lead to criminal penalties. Moreover, failure to implement the minimal requirements for data security is criminally sanctioned by a fine.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Victims of cyberattacks may seek redress in a civil action against the tortfeasor. This may be the cybercriminal or the entity that has failed to comply with appropriate data security standards and procedures. Since class actions do not exist in Switzerland, private individuals whose data have been hacked will, in most cases, be incapable of asserting financial damages in an amount that merits a claim. The revised FDPA provides that if the basic data security measures were not implemented, a criminal complaint may be filed by the injured party, which may lead to a criminal fine.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Personal data must be protected against unauthorised processing through adequate technical and organisational measures. These measures are set forth in more detail in articles 8 to 12 of the implementing Ordinance to the Federal Data Protection Act (DPO). Any system in which personal data is processed must live up to appropriate state-of-the-art technical standards in terms of protection against the risk of unauthorised or accidental destruction or loss, technical flaws, forgery, theft or unlawful access, copying, use, alteration and other kinds of unauthorised processing. More specific requirements are imposed on systems that feature automated processing of personal data. Those systems must, in particular, ensure appropriate access, disclosure, storage and usage controls. In the context of the revision of the FDPA, the DPO was also overhauled; compared to the current DPO, the revised ordinance contains some bolstered requirements around data security, but it does not, however, define specific technical requirements.

Sector-specific regulations and guidance may contain more detailed technical requirements or recommendations.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

To date, Swiss law does not expressly prescribe such recording obligations. Under the text of the revised FDPA, in particular, as certain data breaches will have to be notified, this would imply recording cyberthreats to the extent these resulted in a breach.

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The current FDPA does not provide for an explicit obligation to notify data breaches. Switzerland is finalising the steps towards ratification of the revised Council of Europe Treaty 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) as the Federal Council ratified it in December 2019 and Parliament is expected to give its formal approval in the near future. Under the revised Council of Europe Treaty 108, a notification obligation in the case of data breaches would have to be included in local law. Pursuant to article 7, paragraph 2 of the revised Treaty, the data controller is obliged to notify, without delay, at least the competent supervisory authority of data breaches that may seriously interfere with the rights and fundamental freedoms of data subjects. Consequently, and in anticipation of the ratification, the revised FDPA provides for a duty to notify data breaches to the Federal Data Protection and Information Commissioner (FDPIC). The revised rules call for data controllers to notify the FDPIC as soon as possible if a data breach has occurred and when the breach is likely to result in a high risk to the privacy or the fundamental rights of the data subject. Conversely, the data processors must notify all breaches of data security to the data controller as soon as possible. This breach notification mechanism will not systematically require informing the data subjects, as this step shall only be required when necessary for the protection of the data subject or if requested by the FDPIC.

Notification duties specific to certain sectors and critical infrastructures include the following:

- financial services sector: mandatory notification to the Swiss Financial Market Supervisory Authority without delay regarding

events of material relevance for the supervision of the relevant supervised entity;
- telecommunications sector: notification to the Federal Office of Communications of faults in the operation of telecommunications networks that affect a significant number of customers;
- aviation sector: notification to the Federal Office of Civil Aviation in the event of safety-related data breaches;
- railway industry: notification to the Federal Department of the Environment, Transport, Energy and Communications in the event of severe incidents; and
- nuclear sector: notification to the Swiss Federal Nuclear Safety Inspectorate in the event of safety-related data breaches.

Time frames

30 | What is the timeline for reporting to the authorities?

Sector-specific provisions may require the affected entity to report any relevant cybersecurity incidents without delay.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Scholarly opinion holds that article 4, paragraph 2 of the FDPA, which enshrines the principle of good faith, entails the rule that data subjects must be informed of unauthorised access to their data. However, such notification duty depends on the gravity of the breach in question. Further, specific contractual obligations may impose on organisations a duty to report threats or breaches. The revised FDPA contains rules on the notification of data breaches. Pursuant to these rules, the data controller may be required to inform the data subjects of the breach if the information should prove necessary for the protection of the data subject or if it is requested by the FDPIC.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

One main challenge to the development of cybersecurity regulations is the speed at which cyberthreats evolve. This renders legislating on the subject rather difficult for Parliament. The international dimension of cybersecurity (eg, the involvement of foreign operatives) would also constitute an obstacle to the implementation of the criminal provisions contained in any dedicated cybersecurity law.

The current Swiss approach relies to a broad extent on providing private actors with helpful contact points and resources, with the ultimate aim of mitigating to the greatest extent possible the impact of any cyberthreat on national infrastructures, local businesses and the general public. This is leading the government to bolster its resources, both financially and in terms of personnel. Across-the-board sharing of information and interaction with the science and research domains should also occur on a more regular basis, paving the way for a transversal and interdisciplinary approach to cybersecurity. If not already the case, companies should make a habit of ensuring they implement proper cybersecurity practices and train their personnel accordingly. They should also interact with the ad hoc bodies, in particular the National Cyber Security Centre and the Cyber Security Delegate, to promptly share any relevant information.

walderwyss attorneys at law

Michael Isler
michael.isler@walderwyss.com

Jürg Schneider
juerg.schneider@walderwyss.com

Hugh Reeves
hugh.reeves@walderwyss.com

Seefeldstrasse 123
8034 Zurich
Switzerland
Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
www.walderwyss.com

Turkey

Stéphanie Beghe Sönmez and Mert Karakaşlar
Paksoy

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Turkey does not have any dedicated cybersecurity laws. The data protection legislation, including the Personal Data Protection Law No. 6698 (PDPL), however, contains general requirements with regard to the security of personal data. Cybersecurity breaches can therefore lead to a breach of data protection law.

Following the previous version for the periods between 2013–2014 and 2016–2019, the Ministry of Transport, Maritime Affairs and Communication prepared the 2020-2023 National Cybersecurity Strategy and Action Plan (the National Action Plan), under which definitions, principles, cybersecurity risks and strategic cybersecurity purposes and actions were presented. This plan aimed to shape Turkey's cybersecurity legislation in accordance with international standards and establish a public authority that ensures coordination in the field of cybersecurity.

The 11th Development Plan of the Turkish Republic for the 2019–2023 period (the Strategy Plan for 2019–2023) states that to mitigate national security and ensure technological transformations in primary sectors (eg, chemical industry, medicine and medical equipment, electronics, automotive and rail system equipment), Turkey must enhance its ability to develop cybersecurity and data privacy technologies, fill the gap in the number of qualified persons, further develop its administrative structures and keep its legislation in pace with ever-developing technology. Various plans and strategies are expected to be implemented within the period covered by the Strategy Plan for 2019–2023, including the establishment of new public organisations and committees dealing with cybersecurity. On the other hand, the Turkish Presidency's Digital Transformation Office (DTO), which was established in 2018, has been carrying out a series of studies and projects in the area of cybersecurity and data security for the purpose of ensuring digitalisation in public services and increasing public awareness thereof.

The Presidential Circular on Information and Communication Security Measures (the Circular), which was published by the Presidency on 6 July 2019, sets forth a series of measures aimed at increasing the security of critical data, including requirements for the domestic localisation of data and limitations on the use of cloud services. The Circular primarily concerns public institutions and organisations, but also private organisations that provide services in critical infrastructure sectors, namely banking and finance, electronic communications, transportation, energy, water management and critical public services. The Circular also provided that the DTO had to prepare an Information and Communication Security Guide (the Guide) to be implemented by public institutions and organisations, as well as organisations providing critical infrastructure services. The current information systems of these institutions shall be gradually aligned with the principles determined in the Guide. The Guide, which entered into force on 24 July 2020, lists a series of security measures to be implemented by institutions within the scope of the Circular and provides a 24-month timeline for actions to be taken. In addition, the DTO addressed some of the issues arising under the Circular in the form of frequently asked questions published on its website. On 27 October 2021, the DTO published the Information and Communication Security Audit Guide (the Audit Guide), which provides the methodology to be followed in planning the audits, implementing the audit procedures and reporting the audit results within the scope of mandatory annual periodic audits.

Despite the lack of general legislation to date, certain sector-specific pieces of legislation apply. The Electronic Commerce Law No. 6563 and the Banking Law No. 5411 are the most important. In the banking sector, the Regulation on the Information Systems of Banks and Electronic Banking (the Electronic Banking Regulation), published on 15 March 2020, brought a renewed focus on data protection and cybersecurity issues. The Electronic Banking Regulation contemplates at least 90 hours per year of mandatory training for bank personnel and the carrying out of annual penetration tests by independent firms. It puts in place a gradual transition system, with most provisions becoming effective on 1 July 2020, while six provisions in relation to identity authentication came into force on 1 January 2021. The Electronic Banking Regulation is meant to repeal the Communiqué on the Principles Applicable to the Information Systems of Banks (the Communiqué) issued by the Banking Regulation and Supervision Agency (BRSA) in 2007.

In the health and insurance sectors, the data protection legislation imposes stricter requirements in terms of cybersecurity to the extent that healthcare providers and health insurers process health personal data, which qualifies as a special category of data and requires enhanced protection. These two sectors also have their own legislation with regard to confidentiality obligations, thus making cybersecurity even more critical. In the telecommunications sector, the Information and Communication Technologies Authority (ICTA) has detailed regulations with regard to technical precautions to be taken by telecommunications providers.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

As the PDPL is of general application, companies in all sectors have to comply with data protection law to the extent they process personal data. In addition, the banking, insurance, e-commerce, telecommunications and health sectors have sector-specific legislation and are thus more affected by cybersecurity issues. Owing to their data-intensive nature, these sectors have shown faster progress than other sectors in the field of cybersecurity.

In the telecommunications sector, for instance, the ICTA published a decision on 28 March 2019 with regard to localisation requirements

for remote programmable SIM technologies (eg, eUICC, e-SIM) used in devices that are manufactured to be used in Turkey, imported into the country or brought by passengers from abroad. The decision sets forth that where remote programmable SIM technologies are used in Turkey, SIM modules embedded in these devices must be programmed in such a way that they can be managed by authorised operators, and that only local operator profiles must be installed on the devices. One of the grounds for this decision is to maintain cybersecurity and prevent possible security breaches.

The issuance of additional rules specific to the telecommunications sector is also expected according to the NATO Cooperative Cyber Defence Centre of Excellence's National Cybersecurity Organisation: Turkey report. Developments are also expected in the military sector. The DTO has numerous projects in this field and is soon expected to become more active. On the other hand, under the modernisation programme of the Cyber Defence Command, a new military computer emergency response team and dedicated cyber defence training laboratory has been launched. This will bring a new set of rules for cyber defence.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

For the Turkish Armed Forces, cybersecurity and defence standards are prepared in accordance with those of NATO. As Turkey is a member of the International Organization for Standardization (ISO), the requirements set out under the ISO/IEC 27001 standard must be complied with in the field of data security. ISO/IEC 27001 is a common standard that is also applicable and mandatory under Turkish law for entities providing electronic communication services, electronic networks and infrastructure, and energy facilities.

Pursuant to the Regulation on Independent Audit of Information Systems and Business Processes issued by the BRSA on 31 December 2021, institutions in the banking sector must comply with control objectives in accordance with the principles determined by the BRSA to ensure data security and integrity. The previous issue of this regulation made reference to COBIT standards, but these have been removed in the new version. Although the ISO/IEC 23001 and ISO/IEC 19790 standards have been used with respect to sustainability and cryptography of data, they are not mandatory.

In practice, payment system providers that support the e-commerce industry comply with the Payment Card Industry Data Security Standard, imposed by international credit card institutions to keep online payment records and sensitive data, such as credit card numbers, secure.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The PDPL does not regulate the concept of data protection officer. Although the Turkish Data Protection Authority (DPA) has issued rules for the certification of data protection officers on 10 December 2021, these are solely aimed at certifying a level of knowledge in data protection law and do not define any position with specific duties or responsibilities under the PDPL. As per the PDPL and the guidelines on necessary technical and organisational measures published by the DPA, organisations that act as a data controller or data processor must use and implement the necessary technical and organisational measures listed therein to ensure an appropriate security level to prevent data breaches. In the event of a breach, if the behaviour that led to the breach can be characterised as a crime, a sanction can only be imposed on the natural person perpetrator, meaning the person who actually committed the act defined as an offence by the law. If an offence is committed upon the instruction of another person, the person who committed the act will be charged as the offender, while the person who instructed the perpetrator will be considered an abettor. Both will be exposed to the applicable sanction for the offence at hand. Where the breach leads to an administrative penalty under the PDPL, the organisation itself can be fined. The liability of responsible personnel and directors will thus not be directly triggered under the provisions of the PDPL unless they personally took part in the behaviour that led to the breach. On the other hand, directors can find themselves liable to their company under the provisions of the Turkish Commercial Code if their failure to adequately manage and supervise the company, including by ensuring that the organisation's networks and data are adequately protected against cyberthreats, amounts to a breach of their fiduciary duties. This could lead to their dismissal and to actions for compensation against individual directors. Responsible personnel on the company's payroll could face consequences under labour law, including termination without severance.

More specific precautions in terms of cybersecurity are imposed on organisations active in regulated sectors. In the banking sector, the primary and secondary systems of banks, payment service providers and electronic money institutions should be located within the Turkish territory for data security purposes. In the event of a breach, a disaster recovery plan must be used to ensure data integrity. In addition, the Regulation on Bank Cards and Credit Cards states that institutions that issue credit cards must keep all personal data in confidence, refrain from using such data for marketing activities, and take all necessary precautions to keep records safe. Banks have a general obligation to supervise their information systems and ensure their secrecy, integrity and accessibility. Otherwise, administrative fines may be imposed by the BRSA. As per the Electronic Banking Regulation, it is mandatory to establish a cyber incident response team that is responsible for cybersecurity issues and incident management, and to ensure that the contact details of the team members are notified to the BRSA. In the event of a data breach or cyberattack, this team will be responsible for informing the relevant departments and the BRSA immediately. If such a breach or cyberattack results in the breach or disclosure of sensitive data or personal data, banks must notify their customers following an internal assessment.

Similar rules were issued by the ICTA for the telecommunications sector.

In terms of individual liability of responsible personnel or directors in the banking and telecommunications sectors, under the current state of the legislation, the rules are the same as under the data protection legislation (ie, criminal liability would require personal involvement in the offence), while inadequate cybersecurity that leads to administrative fines for the organisation could ultimately trigger the directors' liability for breach of fiduciary duty under the Turkish Commercial Code.

5 How does your jurisdiction define cybersecurity and cybercrime?

There is no clear definition of cybersecurity under Turkish law. Although cybersecurity as a concept is used in several regulations, it has not been specifically defined yet, whether by statute or through case law. The distinction between cybersecurity and data privacy has not been made by any authority, and cybersecurity requirements remain largely defined in terms of complying with data privacy obligations.

Various definitions have, however, been used by regulatory authorities. The ICTA has adopted the following definition: 'Cybersecurity aims to ensure that the security features of institutions, organisations and users' assets are created and maintained in a way that they are able to withstand the security risks of cyber environments. The main objectives of cybersecurity are accessibility, integrity (fidelity and undeniable logs) and confidentiality'. In the National Action Plan, cybersecurity is

defined as 'activities that consist in protecting the information systems that shield the cyber space from attacks, securing the confidentiality, integrity and accessibility of the information/data processed in this environment, detecting attacks and cyber incidents, activating reaction mechanisms against these detections, and then returning the systems to their pre-existing state before cyber events'; and cybercrime is defined as 'crimes targeting the security of an information system and/or the data and/or user connected to it and committed by using the information system'.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Data controllers have the obligation to implement the technical and organisational measures necessary to ensure an appropriate security level to prevent personal data from being processed or accessed unlawfully and to ensure its protection. The PDPL does not explicitly specify the technical and organisational measures to be taken, and these should be evaluated on a case-by-case basis.

The DPA has published guidelines on technical and organisational measures that are not binding. These guidelines recommend several steps to be taken by those who process personal data. A proper firewall should be put in place. All applications and software should be protected against cyberattacks, which implies that they need to be kept up to date. Access to the systems that contain personal data should be limited. Employees should only be able to access information on a need-to-know basis. The use of brute force algorithms, the requirement to use strong passwords and limitations on the number of password entry attempts to ensure protection against the most common attacks are also suggested. Anti-spam products that periodically review the system and detect malware should be used. The integration of data leakage programs would also count as a protective measure. The guidelines further suggest pseudonymisation, micro merging, global coding, differentiated password systems, partial hiding and extraditing variables as technical methods to protect data.

Furthermore, in the banking sector, the Communiqué makes it mandatory to use a two-factor authentication method to protect data and requires that risk analysis be carried out by the relevant department of the bank. As per the Electronic Banking Regulation, providing cybersecurity training is also a requirement.

Scope and jurisdiction

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Turkey does not have any specific law addressing cyberthreats to intellectual property. Intellectual property rights are generally protected under the Intellectual Property and Artistic Works Law No. 5846, which provides for sanctions in case of infringement, regardless of the environment in which it is committed.

On the other hand, it is a crime for any person to produce, put up for sale, sell or possess for non-private use programs or technical equipment that aim to circumvent additional programs developed to prevent the illegal reproduction of a protected work. This offence is punishable by six months to two years' imprisonment, which may in some cases be converted into a corresponding judicial fine.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

While Turkey does not have any specific legislation addressing cyberthreats to critical infrastructure, the Circular sets forth a general framework for security measures applicable to such infrastructures. Although the Circular does not expressly specify its scope of application, it primarily concerns public institutions and organisations. It also extends to private organisations that provide services in the following critical infrastructure sectors: banking and finance, electronic communications, transportation, energy, water management and critical public services. In addition, sector-specific regulations lead to the protection of critical infrastructure in the relevant sectors, such as financial services systems. Finally, the use of the ISO/IEC 27001 standard is mandatory for entities providing electronic communication services, electronic networks and infrastructure, and energy facilities.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Turkish Criminal Code makes it a crime to access or record telephone communications, or intercept and open private mail. While this should, in principle, extend to electronic communications, there are no express provisions in this respect in the legislation. It is, however, generally admitted that the confidentiality of electronic communications is protected as well, and this is expected to be expressly provided under the new cybersecurity law.

The only exception to the confidentiality of private communications is provided under the Turkish Code of Criminal Procedure No. 5271, under which the communications of persons suspected of illegal activities can be accessed and recorded for the needs of an investigation, with the permission of the public prosecutor. There is no law allowing access to private communications for the purpose of protecting networks or data against cyberthreats.

There are no laws governing access to metadata.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following cyberactivities are criminalised under the Turkish Criminal Code No. 5237:

1. providing unlawful or unauthorised access to information systems, blocking or destroying information systems and altering or destroying data;
2. improper use of bank or credit cards;
3. creating or putting together devices, software, passwords or other security codes to commit the crimes listed in points (1) and (2); and
4. producing, importing, delivering, transporting, storing, accepting, selling, supplying, purchasing or carrying the same.

These offences can lead to sanctions ranging from one to three years' imprisonment.

The PDPL provides for a number of criminal sanctions in the event of a breach of its provisions. Persons who illegally collect personal data are subject to one to three years' imprisonment. If the data is sensitive personal data, the offender is subject to one-and-a-half to four-and-a-half years' imprisonment. Persons who illegally transfer personal data or make personal data available to the public are subject to two to four years' imprisonment. Finally, persons who are responsible for deleting data following the expiry of the retention period but fail to do so are subject to one to two years' imprisonment.

11 | How has your jurisdiction addressed information security challenges associated with cloud computing?

Turkish Law has not yet specifically addressed security challenges associated with cloud computing. An informative note was issued in 2013 by the ICTA, leading to the publication of draft standards for cloud computing systems by the Turkish Standards Institution in 2014. These have not been finalised yet and are thus not binding. The Strategy Plan for 2019–2023 prepared by the ICTA mentions that necessary legal and administrative arrangements will be made for the development and expansion of cloud computing services.

The use of cloud services is indirectly regulated under the PDPL to the extent that the storage of personal data processed by a Turkish organisation on cloud servers located outside Turkey will be considered as an international transfer of data, even if the data cannot be accessed by persons located in the third country. The PDPL rules with regard to the transfer of personal data outside Turkey will thus have to be complied with. Under the PDPL, personal data cannot be transferred to foreign countries unless the explicit consent of the data subject is obtained, or the organisation can rely on one of the exceptions set out by the law. In addition, if the recipient is located in a country that is not considered to provide adequate protection, the transfer is subject to the execution of a written undertaking by the sender and the recipient, as well as the prior approval of the DPA. The list of adequate protection countries has not been published to date.

The DPA's non-binding guidelines on technical and organisational measures also mention cloud computing systems. These mostly warn data controllers of the data protection risks associated with the use of cloud technology.

In the banking sector, the Electronic Banking Regulation provides that banks are obliged to have their primary and secondary systems within Turkish territory. Likewise, they will be able to benefit from private cloud computing services only if the servers of the cloud services provider are located within Turkish territory.

12 | How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Regulatory obligations are the same for all organisations doing business in Turkey, whether they are Turkish organisations with Turkish or foreign capital or foreign organisations doing business through a local branch. Turkish organisations with foreign capital and foreign organisations doing business in Turkey are, however, more likely to need to consolidate data generated in Turkey in jurisdictions outside Turkey, for which they will face restrictions under the PDPL.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The Information and Communication Technologies Authority (ICTA), as the telecommunications regulatory and supervisory authority of Turkey, is authorised to regulate cybersecurity issues. While the ICTA's decisions are directly binding upon companies, the authority also publishes recommendations and guidelines. As per the recommendations of the ICTA, each organisation dealing with data should conduct annual penetration tests to identify weaknesses in its information systems. The aim of the test is also to evaluate incident management methods. This test is already required in the banking sector, but under the Regulation on the Information Systems of Banks and Electronic Banking, it is mandatory to have the test be conducted annually by an independent firm. The ICTA also recommends data classification, data governance projects and cryptology methods to be adopted to increase data security and minimise the risk of data leakage.

Furthermore, a series of security measures to be implemented by institutions within the scope of the Presidential Circular on Information and Communication Security Measures (ie, public institutions and organisations, as well as private organisations that provide services in critical infrastructure sectors) are provided in the Guide to ensure network and system securities, application and data security, portable device and platform security, internet of things device security, personnel security and physical place security.

14 | How does the government incentivise organisations to improve their cybersecurity?

The Turkish government does not currently provide any form of incentive for organisations to improve cybersecurity. It is, however, working on increasing cybersecurity standards and awareness within public institutions. In this respect, the Turkish Cyber Security Cluster was established in 2017 to develop the Turkish cybersecurity ecosystem with the contribution of all public agencies, academia and private sector representatives under the leadership of the Presidency of Defence Industries. This platform has a number of objectives, which include: increasing the number of cybersecurity companies in Turkey; supporting the development of the member companies' technical, administrative and financial capabilities; improving the branding of products and services; improving the standards of the cybersecurity ecosystem; increasing the competitiveness of member companies in the national and global market; increasing human capital in the field of cybersecurity; and increasing awareness of cybersecurity throughout society.

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There are sector-based standards applicable in Turkey, the most common being ISO/IEC 27001. It is a legal requirement for energy companies, licensed operators in accordance with ICTA regulations and certified operators in accordance with customs law to obtain ISO/IEC 27001 certification. Companies providing payment systems services must comply with the Payment Card Industry Data Security Standard (PCI DSS), which is imposed in practice by international credit card institutions. At points where classified information is processed by public institutions and organisations, dissemination security (TEMPEST) or similar security measures must be taken.

16 | Are there generally recommended best practices and procedures for responding to breaches?

The Turkish Data Protection Authority (DPA) has not published any guidance with regard to best practices and procedures for responding to personal data breaches. Under the Personal Data Protection Law No. 6698, the retention of third-party data forensic firms is not required but may be useful to respond to the questions of the DPA, which is likely to request all available information related to the breach. There are no generally recommended best practices as regards communications to employees or with the media, which will be devised on a case-by-case basis.

The ICTA has published guidelines regarding general and sectoral best practices and procedures for responding to breaches in the telecommunications sector. These require operators affected by a breach to take certain technical measures immediately in compliance with

international standards. There is no requirement to retain third-party forensic firms. Operators should have incident management and disaster recovery policies in place.

In the banking sector, the Banking Regulation and Supervision Agency requires banks to comply with control objectives in accordance with the principles determined by the BRSA. Payment systems providers should comply with the practices and procedures set out under the PCI DSS.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Turkey does not have any regulated practices or procedures for voluntary sharing of information about cyberthreats. According to the 11th Development Plan of the Turkish Republic for the 2019–2023 period and the Strategy Plan for 2019–2023 issued by the ICTA, coordination and bidirectional information flow should be ensured between the National Cyber Incidents Response Centre (established under the ICTA) and public authorities, the private sector, universities, NGOs and cybersecurity volunteers to ensure coordination on cyberthreat intelligence with national and international stakeholders and to fight cyberthreats through rapid detection and early intervention.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The ICTA periodically convenes a meeting with cybersecurity professionals to obtain their input to determine cybersecurity standards and procedures. This is an ongoing process, and no such standards and procedures have been officially determined yet.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Although cybersecurity insurance is not an obligation, there are several insurance firms offering cybersecurity insurance policies in Turkey. Owing to the lack of reliable standards and parameters to detect the risk of a cybersecurity breach, the actuarial risk assessment is difficult to make and insurance companies in Turkey struggle to price this type of insurance product.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Information and Communication Technologies Authority (ICTA) is the regulatory body authorised to take decisions and actions regarding the protection of information systems. However, as the Personal Data Protection Law No. 6698 (PDPL) is the only general piece of legislation that currently imposes requirements in terms of cybersecurity, the Turkish Data Protection Authority (DPA) is the regulatory authority competent to conduct investigations, issue binding decisions and impose administrative fines. To the extent that cybercrimes are defined under the Turkish Criminal Code, public prosecutors and criminal courts are also competent to investigate, prosecute and impose sanctions in relation to such crimes.

The Digital Transformation Office (DTO), established in 2018, is the main body responsible for the digital transformation of public institutions and cybersecurity. As per Presidential Decree No. 1 on the organisation of the Presidency (of which the DTO is a department), the DTO is authorised to implement strategies and policies regarding cybersecurity and to coordinate the regulatory activities necessary for digital transformation and the harmonisation of national regulation with international standards.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Under the PDPL, the DPA has the right to audit data controllers and processors, including the right to conduct site inspections and request documents. In the banking sector, the Banking Regulation and Supervision Agency (BRSA) has the right to audit the banks' information systems. Pursuant to the Regulation on Independent Audit of Information Systems and Business Processes issued by the BRSA on 31 December 2021, banks must comply with control objectives in accordance with the principles determined by the BRSA and are subject to yearly audits conducted by certified independent firms at the request of the BRSA in accordance with the rules and principles set forth under the aforementioned regulation. The BRSA is also authorised to audit other financial institutions, including payment systems providers and e-money companies. In addition, institutions that hold a Payment Card Industry Data Security Standard (PCI DSS) certification and obtain credit card information can be audited and investigated by the PCI DSS auditors.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

The practice of regulators is generally to afford cure periods to organisations to remedy instances of non-compliance. If the DPA identifies deficiencies in the technical and organisational measures taken to protect personal data, it can give a 15-day period to cure the situation under the PDPL and eventually issue administrative fines. The ICTA and the BRSA also have the power to request that deficiencies be cured within a certain period of time and to issue administrative fines if the necessary measures are not taken. Where fines are imposed, they can be quite substantial, especially in the banking sector, where there is no statutory cap. There are market precedents in which fines well in excess of 10 per cent of the affected bank's revenue were imposed following a failure to take necessary measures against cyberthreats and report the breach immediately. On the other hand, it is difficult to have a clear picture of the enforcement environment because most regulatory decisions imposing fines are not made public; the lack of transparency in this respect is a recurrent issue in Turkey.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

In the event of a cybersecurity breach potentially affecting personal data, the data controller must notify the DPA without undue delay and, where feasible, no later than 72 hours after becoming aware of the data breach. Data subjects must also be notified via appropriate methods as soon as possible after determination of the persons affected by the data breach.

The following elements must be included in the notification made to the data subjects:

- date of the breach;
- information on the categories of personal data affected by the breach;
- possible consequences of the breach;

- measures taken or proposed to be taken to reduce or eliminate possible adverse effects; and
- the names and contact details of the persons who can provide information about the breach or the full contact details of the data controller.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The PDPL provides that the failure to comply with the obligation to ensure data security can result in a fine ranging from 40,179 Turkish lira to 2,678,863 Turkish lira (for 2022). In addition, failure to comply with the decisions of the DPA, which may include injunctions to comply with cybersecurity requirements, can result in a fine ranging from 66,965 Turkish lira to 2,678,863 Turkish lira (for 2022).

In the telecommunications sector, the ICTA has broad powers to impose fines of up to 3 per cent of the operator's net revenue in the previous year for failure to comply with laws, regulations and the ICTA's own decisions. In the banking sector, the BRSA also has the power to impose fines calculated by reference to the bank's revenue, but this is not subject to a formal cap and will be determined by the BRSA on a per breach basis.

If it is determined, following an inspection by mandated auditors of the International Organization for Standardization (ISO), that a company has failed to comply with the ISO 27001 standard, the company's certification may be suspended or cancelled. In the field of payment systems, if a company fails to comply with the PCI DSS twice, the certificate is taken away from the company. For companies that are required to comply with the ISO 27001 standard by their own regulatory authority, such as the Energy Market Regulatory Authority in the energy sector, administrative fines can be directly imposed by the competent regulator in case of failure to comply.

While this would only apply in extreme cases, Turkish regulatory bodies also have the power to suspend or cancel an organisation's operating licence in case of non-compliance with laws, regulations or regulatory decisions.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Under the PDPL, failure to report a data breach to the DPA and the data subjects can lead to administrative fines ranging from 40,179 Turkish lira to 2,678,863 Turkish lira (for 2022). In the telecommunications sector, the ICTA may impose fines of up to 3 per cent of the operator's net revenue in the previous year for the failure to report a security breach. In the banking sector, the BRSA also has the power to impose fines calculated by reference to the bank's revenue, but this is not subject to a formal cap and will be determined by the BRSA on a case-by-case basis.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Compensation lawsuits may be initiated on the basis of general principles of law, including by seeking liability in tort or in contract if there was a contractual relationship between the parties. If the data breach affects personal data, the PDPL expressly provides for the data subjects' right to compensation if their data has been processed in breach of the law. If the data breach resulted in the infringement of intellectual property rights, compensation can also be sought on the basis of intellectual property law. If a company has suffered damage as a result of its directors' failure to implement adequate cybersecurity measures within the organisation, this could qualify as a breach of fiduciary duties and form the basis of liability claims against the directors under the Turkish Commercial Code.

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Regulation on Deletion, Destruction and Anonymisation of Personal Data provides that data controllers that are obliged to register with the data controller registry should prepare a data retention and disposal policy based on the personal data processing inventory, and should include the technical and organisational measures to be provided by data controllers.

Organisations acting as data controllers have the obligation to implement the technical and organisational measures necessary to ensure an appropriate security level to prevent personal data from being processed or accessed unlawfully and to ensure its protection. The Personal Data Protection Law No. 6698 (PDPL) does not explicitly specify the technical and organisational measures to be taken, and these should be evaluated on a case-by-case basis.

As per Decision No. 2019/10 of the Turkish Data Protection Authority (DPA), dated 24 January 2019, data controllers should prepare and periodically review a data breach intervention plan. This plan should include matters such as the internal reporting line, responsible persons for disclosures and assessments of possible outcomes of data breaches.

The Information and Communication Technologies Authority (ICTA) has published guidelines regarding general and sectoral best practices and procedures for responding to breaches in the telecommunications sector. These require operators affected by a breach to take certain technical measures immediately, in compliance with international standards. There is no requirement to retain third-party forensic firms. Operators should have incident management and disaster recovery policies in place.

In the banking sector, the Banking Regulation and Supervision Agency (BRSA) requires banks to comply with control objectives in accordance with the principles determined by the BRSA. Payment systems providers should comply with the practices and procedures set out under the Payment Card Industry Data Security Standard. At points where classified information is processed by public institutions and organisations, dissemination security (TEMPEST) or similar security measures must be taken.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There is no general legal requirement to keep cyberthreat records, although it is strongly advisable to keep records of all activity affecting personal data in the event of an inspection by the DPA. Most companies will also have an obligation to keep internet log records for two years under the Internet Law No. 5651 and related regulations as long as they provide access to the internet, even if only to their own employees.

In the telecommunications sector, the Regulation on Network and Information Security in the Electronic Communications Sector, issued by the ICTA in 2014, requires that records regarding network and security breaches be kept for two years. In the banking sector, banks are obliged to keep records of data and logs, but it is currently unclear how long the records should be retained. In accordance with the Regulation on the Information Systems of Banks and Electronic Banking (the Electronic Banking Regulation), banks are under the obligation to keep records

of all transactions for three years. Banks and telecoms operators are also required to report breaches to the regulator in annual reports. The Internet Law also requires internet access providers to keep records of traffic information for one year, and organisations to keep logs of all e-commerce and call centre transactions, which can be later be used for evidence purposes.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

If the breach affects personal data, the PDPL provides that if personal data is illegally obtained by third parties, the data controller must inform the DPA and the relevant data subjects as soon as possible. The PDPL further states that the DPA may publish an announcement regarding the data breach on its website or by any other method it deems appropriate. The failure to comply with this obligation would expose the affected organisation to administrative fines.

In the telecommunications sector, a binding decision of the ICTA requires operators to notify any type of cybersecurity breach, including data leakage and cyberattacks, to the authority. Reports should include, among other things, logs, time stamps, the identification numbers of affected devices, a description of the lost data and the time at which the breach was discovered.

In the banking sector, banks currently have to prepare a form containing substantially the same information as listed above, as well as identification of potential harm to end users (such as affected transactions) and submit it to the BRSA. Under the Electronic Banking Regulation, it is mandatory to appoint a team responsible for cybersecurity issues, whose duties would include informing the departments of the bank and the relevant authorities in the event of a breach. Banks would also be obliged to report cyberthreats as well as breaches.

In addition, if a public company is affected by a cyberattack, it must notify the Capital Markets Board, which will make the information publicly available. In the insurance sector, even though it is not mandatory, it is strongly advisable for companies to notify the Undersecretariat of the Treasury, which is the insurance regulator.

Time frames

30 | What is the timeline for reporting to the authorities?

In the event of a cybersecurity breach potentially affecting personal data, the data controller must notify the DPA without undue delay and, where feasible, no later than 72 hours after becoming aware of the data breach. Data subjects must also be notified via appropriate methods as soon as possible after determination of the persons affected by the data breach. There is no requirement to report on cybersecurity on a regular basis under the PDPL.

Likewise, all the relevant regulatory authorities should be notified as soon as the breach is discovered. This could mean the ICTA, the BRSA and any other competent authority depending on the sector in which the affected entity operates.

Regular reporting obligations only exist in the banking and telecommunications sectors. Banks must submit an information system audit report to the BRSA in accordance with the rules and principles to be determined by the BRSA, and telecommunications companies must submit a report including an assessment of cyber risks, encountered cyberattacks and precautions taken against them, to the ICTA in the first three months of each year.

Paksoy

Stéphanie Beghe Sönmez
sbeghe@paksoy.av.tr

Mert Karakaşlar
mkarakaslar@paksoy.av.tr

Orjin Maslak
Eski Büyükdere Caddesi No. 27 K:11
Maslak
34485 Istanbul
Turkey
Tel: +90 212 366 47 00
Fax: +90 212 290 23 55
www.paksoy.av.tr

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

The PDPL requires that data breaches affecting personal data be notified to data subjects in addition to the DPA. There are no formal requirements to report threats or breaches to others in the industry or to the general public.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Together with the publication of various strategy and development plans that set promising goals for the government and regulatory authorities to develop cybersecurity and information technologies in several sectors, there has been an increasing trend towards digitalisation in the country. Turkish public authorities have started to use digital platforms to increase efficiency, integrity and sustainability. One example is the electronic online apostille services to be provided by the Post, Telegraph and Telephone Institution.

The Ministry of Environment and Urbanisation published its smart cities strategy and action plan for 2020–2023, which introduces various enhancements in the areas of data security, information technologies, smart infrastructures and so on. The Istanbul Municipality is working on a smart cities system and on the collection of data for payment systems in public transportation and vendor machines. The intent is to introduce a city card, the Kent Kart, for payments in public places. This will bring about the need for increased cybersecurity precautions. The establishment of an Istanbul Cyber Security Platform is also on the agenda. However, no official announcement has been made to date regarding the implementation of these projects. Another significant development concerns the land registry system, with land registries starting to keep

online records and to accept online payments for land registry transactions. A series of other formalities, such as trade registry applications or registration with the data controller registry, must now be made through online systems.

In view of this growing trend towards digitalisation, the Information and Communication Technologies Authority (ICTA) has started to draft a code regarding cybersecurity issues that should follow the approach taken in the EU Cybersecurity Act to introduce a new standardised cybersecurity framework and provide an EU-wide certification system identifying resilience to cyberattacks. Since the Personal Data Protection Law No. 6698 and the Payment Systems Law are largely modelled on EU legislation, Turkey's future cybersecurity code is expected to be similar to the EU Cybersecurity Act. In the meetings convened with cybersecurity experts, ICTA officials have largely referred to the EU Cybersecurity Act as an example.

Overall, the cybersecurity ecosystem in Turkey is developing as more strategies, plans and projects are being drawn up, in particular in the public sector and in critical private sectors, such as banking, health, telecommunications and energy. One obvious challenge for authorities devising legislation in this field is to keep up with fast-paced technological developments and the changing needs of private sector players. Turkish public authorities dealing with cybersecurity issues have, however, shown themselves to be quite open to seeking feedback from market players and involving them in the process to shape the new regulations. In this area, more than others, it is in the interest of market players to engage with regulatory authorities as early as possible in the process, make their needs known to these authorities and provide constructive feedback as to the proposed regulations.

United Kingdom

Robert Allen, Lawrence Brown, Neil Westwood, Russell Cowie and Emily May*

Simmons & Simmons

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The UK does not have a comprehensive cybersecurity law – instead, cybersecurity requirements and obligations are set out in various legislation:

- The Network and Information Systems Regulations 2018 (NISR) impose security and incident reporting requirements on organisations that are operators of essential services (OESs) and relevant digital service providers (RDSPs). An RDSP is an online marketplace, online search engine, or cloud computing service provider established in, or with a representative established in, the UK and which is not a micro or small enterprise. These organisations must have proportionate and effective security measures and procedures to ensure continuity of business services and effective incident reporting. The UK government is consulting on expanding the range of digital service providers affected by the NISR to include other types of digital services.
- The Communications Act 2003 (CA 2003) requires public electronic communications services (ECS) and electronic communications network (ECN) providers to ensure the security of their networks and services, including incident mitigation.
- The Telecommunications (Security) Act 2021 (TSA) amends the CA 2003 and will impose new legally binding security requirements on ECN and ECS providers. The provisions of the TSA that provide new powers to legislators and regulators are currently in force, with the provisions relating to the obligations on providers due to be introduced by way of statutory instrument.
- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) impose data security requirements on controllers and processors of personal data, and prescribe a risk-based approach to data security.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) place further obligations on ECS providers.

In respect of the financial services sector, the FCA Handbook also imposes a number of cybersecurity requirements on firms through its governance obligations.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Publicly listed companies and those within the financial services sector are subject to governance and security requirements which, either directly or indirectly, impose cybersecurity obligations upon them. The enforcement action that may be taken against such organisations can include significant fines and other sanctions, and there is significant reputational risk associated with such measures.

Operators of essential services (including in the energy, transport and health sectors) and digital service providers are subject to the additional cybersecurity and reporting obligations under the NISR. These organisations must implement appropriate technical and organisational measures to manage the cybersecurity risks to their networks and systems, and adopt measures that will enable them to mitigate the impact of incidents.

The UK government's National Cyber Strategy 2022 (the Strategy) highlights the interaction between established sectors of the economy and new and unregulated businesses (such as electric vehicle charging or those that provide microgeneration) as an area of potential concern, with the diversification of the business landscape likely to result in fundamental changes to the regulatory approach to cybersecurity.

There are not currently any cybersecurity obligations that apply explicitly to professionals in the legal sector; however, firms will be subject to broader data protection legislation such as the GDPR when conducting their business.

3 | Has your jurisdiction adopted any international standards related to cybersecurity?

There are no mandatory ISO standards in the United Kingdom. However, organisations may adopt standards such as ISO 27001:2013 to evaluate which security measures are required to meet their obligations under the NISR. Similarly, adherence to the standards is a means by which data controllers can demonstrate compliance with their obligations under the GDPR and DPA 2018.

Organisations also frequently elect to adopt ISO standards through contractual provisions, to demonstrate that their cybersecurity policies and procedures are sufficiently robust.

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

There is no legislation that imposes direct responsibility for cybersecurity compliance on personnel and directors. However, directors of organisations that fail to adequately ensure cybersecurity may be held responsible under the Companies Act 2006, which requires directors to exercise reasonable skill, care and diligence in the performance of their functions.

5 | How does your jurisdiction define cybersecurity and cybercrime?

The UK government's Strategy defines cybercrime as crime that can only be committed through the use of ICT devices, or which are changed

significantly (in scale and reach) by the use of ICT. The Strategy defines cybersecurity as the protection of internet-connected systems (including hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse.

The NISR relate to the security of network and information systems and therefore amount to cybersecurity obligations. However, information security requirements under the NISR also include other system and environmental considerations (such as management of system failure, human error, and natural events).

6 | What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The UK GDPR does not prescribe specific security measures that organisations must have in place; firms must implement appropriate technical and organisational measures to ensure the security of personal data, which may include measures such as encryption or pseudonymisation of data.

Organisations that fall within the NISR must also take appropriate and proportionate technical and organisational measures to ensure that risks to their systems are managed. In addition, the NISR provide for obligations relating to:

- the security of network and information systems and facilities;
- incident handling (including detection procedures and incident reporting);
- business continuity management (including disaster recovery capabilities);
- monitoring, auditing and testing (including processes to reveal flaws in the security mechanisms used to protect the network and information systems); and
- compliance with international standards relating to the security of network and information systems.

Scope and jurisdiction

7 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no legislation that specifically addresses cyberthreats to intellectual property. However, the Strategy specifically identifies the protection of intellectual property in critical cyber technologies as an objective, with a particular focus on the sectors mentioned in the National Security and Investment Act 2021 (NSIA), including artificial intelligence, communications, and cryptographic authentication.

8 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The NISR apply to operators of essential services in a number of sectors (including energy, transport and health) and provides that organisations must take appropriate and proportionate technical and organisational measures to manage risks posed to their network and information systems, including measures to mitigate the impact of incidents. The NISR also impose reporting standards on these organisations, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring. Compliance with the NISR is actively monitored by the designated authorities (including the Information Commissioner's Office (ICO)) and the UK has adopted an audit framework in respect of OESs and RDSPs to ensure compliance with the relevant requirements.

In respect of the financial services sector, the Senior Management Arrangement Systems and Controls (SYSC) section of the FCA Handbook applies to providers of financial services infrastructure, and requires firms to have effective and proportionate risk-based systems to combat financial crime.

9 | Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Investigatory Powers Act 2016 (IPA) criminalises the unlawful interception of communications within the UK. The IPA also limits the sharing of information lawfully obtained by UK law enforcement bodies and intelligence agencies via interception. It is a criminal offence under the IPA for communication service providers or public officials to disclose the existence and content of a warrant or authorisation where a government agency has, under a bulk or targeted warrant, intercepted communications in the interests of national security or for the prevention of serious crime.

The Counter-Terrorism Act 2008 covers disclosure of information to the intelligence services for the purposes of national security or the prevention of serious crime.

The UK GDPR and the DPA 2018 only permit personal data sharing to law enforcement authorities where it is necessary and proportionate. Except where the ICO determines that publication is in the public interest, the ICO is prohibited from publicising information disclosed to it via a personal data breach notification that relates to any identifiable individual or business that is not already in the public domain.

Article 8 of the Human Rights Act, which deals with an individual's right to privacy, can be interfered with by a public authority only where it can be shown that such interference is lawful, necessary, and proportionate to protect national security.

10 | What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The Computer Misuse Act 1990 (CMA) is the primary cybercrime legislation in the UK. The CMA criminalises unauthorised access to computer networks, such as hacking; intention to commit a cybercrime; modifying, removing, or ransoming data; and aiding computer misuses.

Section 3 of the IPA criminalises the unlawful interception of communications within the UK.

In relation to personal data processing, the DPA 2018 creates a number of offences, such as unlawfully obtaining personal data, knowingly or recklessly disclosing personal data without the consent of the data controller, and the sale of personal data obtained illegally. Fraud by false representation, which could cover certain phishing incidents, is punishable under the Fraud Act 2006.

11 | How has your jurisdiction addressed information security challenges associated with cloud computing?

The NISR specifically govern certain categories of digital services, including cloud computing services, and aim to establish a common level of security for network and information services.

The NSIA allows the government to scrutinise and intervene in acquisitions of control of companies involved in 17 'sensitive areas of the economy', where there is a potential impact on the UK's national security. One such area is cloud computing. The rules came into force on 4 January 2022, although they can be enforced retrospectively for deals that were completed on or after 12 November 2020. Completion of a notifiable acquisition without approval could lead to criminal or civil penalties.

The UK's National Cyber Security Centre (NCSC) offers a framework to organisations in the UK public sector built around 14 Cloud Security Principles that cover how organisations should configure, deploy, and use cloud services securely.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The NISR apply to OESs and RDSPs outside of the UK that offer services in the UK, and require these organisations to nominate a representative to the relevant competent authority for enforcement purposes.

The CMA has extraterritorial effect in relation to offences with a significant link to the UK (ie, where the accused was in the UK when the offence was committed, the unauthorised action was committed, or the target computer was located in the UK). The Serious Crime Act 2015 amended the CMA to provide for additional extraterritorial powers where there is a significant link. A significant link is established if the conduct in question caused serious damage of a material nature in the UK. Additionally, if the accused is a UK national and commits an offence while outside of the UK under the law of another country then a significant link is established.

The IPA also provides for extraterritorial application in respect of communications carried out in the UK (ie, where an individual in the UK is communicating with persons in other jurisdictions). UK law enforcement agencies may issue warrants under the IPA to overseas service providers for data, the interception of communications or the monitoring of computer equipment.

Foreign organisations will be subject to the UK GDPR, including its security requirements, if they offer goods or services to individuals in the UK. Personal data transferred from UK to organisations in third countries must be subject to appropriate safeguards, which typically involves the execution of standard data protection clauses, including provisions covering security measures, between the exporting and importing organisation. In February 2022, the ICO published a new form of International Data Transfer Agreement to be used for this purpose (subject to parliamentary approval). At the time of writing, further ICO guidance on use of the IDTA and the conduct of data transfer risk assessments is anticipated.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Enhanced cybersecurity protections, beyond those mandated by law, are recommended by a number of different authorities, with guidance notes and advice widely available.

The National Cyber Security Centre (NCSC) is an organisation within the UK government that provides advice and support for the public and private sector to promote cybersecurity. The central pillar of its advice is '*Cyber Aware*', which provides a set of guidelines built around six key actions. In addition, it also maintains '*10 Steps to Cyber Security*', guidance aimed at medium-sized to large organisations that employ cybersecurity professionals, and a *'Small Business Guide: Cyber Security*'. On top of this, the NCSC publishes various focused guides on passwords, ransomware, phishing, devices, personal data malware, operational security and the cloud.

Other authorities also recommend enhanced protections. The Global Cyber Alliance, Action Fraud, the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) are among other authorities that also recommend protections beyond those strictly mandated by law.

It should be noted that while industry and regulatory codes or guidance do not constitute protections mandated by law, failure to follow such codes may still give rise to adverse consequences. For example, the ICO states, in its Regulatory Action Policy, that failure to follow an approved or statutory code of conduct is an aggravating factor when it considers sanctions.

14 How does the government incentivise organisations to improve their cybersecurity?

Following a 2019 consultation, on 19 January 2022 the government published a policy paper entitled '2022 cyber security incentives and regulation review'. In that it noted that it was for the market to incentivise better security practices for organisations, but recognised that those incentives (such as consumer pressure and competitive advantage) have not yet formed effectively. To mitigate this, the government plans to take a more interventionalist approach through guidance, further market participations and strengthening of UK cyber legislation.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The NCSC publishes a guide dealing with issues such as cyber defence, threat and ransomware. The NCSC's *10 Steps to Cyber Security* sets out a number of key areas for medium-sized to large organisations to ensure that technology, systems and information are protected against cyberattacks. In doing so the guide emphasises the need to take a risk-based and proactive approach to cybersecurity.

Organisations operating within the regulated financial services sector are also guided by a range of materials produced by the FCA in order to achieve compliance with its Principles, and the standards set out in the SYSC sourcebook. One such example is the FCA's publication on *Good cyber security – the foundations*, which demonstrates the FCA's approach to working with other organisations (namely, the NCSC) in order to achieve effective levels of cybersecurity within the sector.

16 Are there generally recommended best practices and procedures for responding to breaches?

The best way to mitigate the impact of a data breach is to ensure you are properly prepared. A number of public organisations have published guidance for responding to data breaches (including the ICO and the NCSC). You should already have a detailed cybersecurity policy and within that should be a data breach response plan. Such a plan should be accessible to all employees and form part of standard onboarding training.

The first recommended step is to identify the extent of the breach and preserve relevant evidence. Although basic, it is important to document how the breach was identified and keep a careful note of steps taken. Such steps might include ensuring the correct internal stakeholders have been contacted (eg, HR, security), determining whether the breach contained personal data, and identifying

which jurisdictions may have been affected. Answering these questions will inform the scope of external bodies that need to be involved in the crisis response team (eg, forensic experts to track the extent of the breach).

Next, your focus should shift to analysis, that is, understanding the 'how'. For example, how did the breach occur and is it ongoing? If so, what steps need to be taken to fix (or 'patch') the breach? At this stage, you should consider whether stopping the breach might 'tip off' the attacker and lead to the destruction of evidence; this should be balanced against your data protection duties. You should also consider any external and internal communications. For example, you might want to consider a formal press release, or an internal notice reminding employees of the sensitivities of publicly discussing the breach with the media.

You should then consider the remedies and next steps available to you. Depending on the circumstance of the breach, this can range from initiating legal action to instigating a PR strategy.

Finally, you should consider your long-term response. If the breach identified any holes in your security system or staff training, these should be addressed as a matter of urgency. You should also reflect on whether you need to strengthen the relationships with necessary third parties; you may want, for example, to have forensic experts or legal counsel on retainer for data breaches.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

It is considered best practice to share information on cybersecurity threats, although this usually occurs after the threat has been properly resolved. You can share this information informally, for example through social media, or more formally on a voluntary basis to Action Fraud or the NCSC.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The UK government's Strategy sets out an aim for the UK to establish itself as a global cyberpower, which includes strengthening the UK cyber ecosystem between government, academia and industry. The Strategy intends to build on the existing relationships between NSCS and industry stakeholders, most notably the regional cyber clusters recently formalised by the UK Cyber Cluster Collaboration.

Industry experts have also organised to help direct the UK technology sector. In particular, techUK (the UK's technology trade association) brings together organisations to enhance government collaboration and accelerate innovation. techUK has over 800 members across the UK, from sector leaders, such as Amazon and DeepMind, to law firms and emerging start-ups.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance for cybersecurity breaches is available in the jurisdiction and has become more prevalent and available in the past five years, although the cyber insurance market has hardened significantly over the past year. Previously, insureds that suffered cyberattacks or were involved in cyber incidents would try to claim under their existing commercial insurance policies (such as, for example, those relating to property or commercial risks). While some of these 'silent' cyber risks could attach, many would not fall within cover. This state of affairs helped drive the 'affirmative' cyber insurance marketplace forward.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

A number of authorities share this responsibility. The National Cyber Crime Unit (which operates within the National Crime Agency) is responsible for responding to the most critical cyber incidents and also pursues longer-term activity against cyber criminals. The Information Commissioner's Office (ICO) enforces cybersecurity rules where they involve personal data (through the UK GDPR and Data Protection Act 2018), and enforces the NIS Regulations 2018. Industry-specific regulators (eg, the Financial Conduct Authority (FCA)) may enforce cybersecurity rules where a breach falls within their jurisdiction. Criminal prosecutions are (with some limited exceptions) carried out by the Crown Prosecution Service.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Authorities have relatively wide-ranging powers to monitor compliance, conduct investigations and support prosecutions. The ICO has statutory powers as set out in the DPA 2018 (Parts 5 and 6). Among other things, it is empowered to conduct compliance assessments, issue information requests, enter premises, call for documents and interview staff. It is a criminal offence to obstruct a person executing an ICO warrant. Sector-specific regulators have certain similar powers, which vary between regulators and are provided for by statute (eg, the FCA).

Where criminal proceedings are on foot or in contemplation, the power of authorities to monitor and investigate are the same as those for criminal investigations generally.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

According to the National Cyber Security Centre (NCSC), ransomware became the most significant cyber threat facing the UK in 2021. In addition, the UK government's Strategy makes clear that ransomware attacks continue to become more sophisticated and damaging. The government's *Cyber Security Breaches Survey (2021)* also highlights the increased risk level (due to the effects of the pandemic), and that businesses are finding it harder to administer cybersecurity measures than ever before. This reality, especially when coupled with increased enforcement actions, means that cybersecurity is likely to be an ongoing issue for the private sector and beyond.

In the UK, many will recall the ICO fining Ticketmaster £1.25 million in November 2020 following a data breach in 2018 that potentially compromised data of 9.4 million customers. While regulatory enforcement concluded in 2020, the separate private group action against Ticketmaster continued until February 2022, when it reportedly reached a confidential settlement.

The attack on Microsoft's Exchange servers, which was made public by the firm in March 2021, has not yet resulted in enforcement action by the ICO or otherwise. It remains to be seen whether direct action will be taken by regulators in response, although the recent increase in enforcement activity would suggest that an announcement is imminent.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A notification to the ICO is not required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business who is subject to the breach must also inform those affected individuals without 'undue delay', and, in practice, this should be done as soon as possible.

While the obligations under the UK GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation.

Penalties

24 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Cybersecurity law in the jurisdiction has not been centrally codified and instead is based on a legal framework comprised of a number of statutory enactments. It is therefore difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

By way of an example, however, the Network and Information Systems Regulations 2018 impose obligations on operators of essential services and relevant digital service providers. The former operate services that are deemed critical to the economy such as energy, water and transport. The latter operate (among others) online marketplaces and provide cloud computing services. The regulations require these entities to have sufficient security systems in place, and allow a competent authority (the ICO) to impose penalties for breaches of its provisions.

Where, for example, there has been a material contravention of the regulations, which is deemed to have caused (or could cause) an incident resulting in the disruption of service for a significant period of time, penalties of up to £8.5 million are capable of being imposed. If the disruption results in an immediate threat to life or a significant adverse impact on the economy, the penalty could be up to £17 million.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Again, the absence of a centrally codified cybersecurity law makes it difficult to discuss penalties for regulatory breaches in the round, as they apply to all businesses.

Most of the relevant regulations impose obligations to report either threats or breaches and in doing so, give competent authorities the power to issue penalties (usually in the form of enforcement notices). By way of an example, the Network and Information Systems Regulations 2018 require incidents to be reported without undue delay. If, however, a failure to do so amounts to a 'material contravention', the penalty could, in theory, be up to £17 million in certain circumstances. Where personal data is involved, the Data Protection Act 2018 and the UK GDPR will also be relevant.

26 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The GDPR gives you a right to claim compensation if you have suffered damage as a result of breach of data protection laws. 'Damage' includes material and non-material damage, meaning financial loss or suffering distress (an arguably low bar). In the first instance you should contact the individual or company who held your data at the time of the breach; they may agree to pay you without further action. If they don't, you might consider bringing formal proceedings (although you should take independent legal advice before doing so).

More recently we have seen a rise in group action claims for mass data breaches, although we expect this trend to plateau following the recent supreme court decision in *Lloyd v Google*, which refused a large-scale representative action (similar to US class actions).

THREAT DETECTION AND REPORTING

Policies and procedures

27 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

UK legislation does not mandate specific policies or procedures in this respect. The security principle set out in the UK GDPR requires organisations to process personal data securely by implementing appropriate technical and organisational measures. Similarly, the Network and Information Systems Regulations (NISR) require operators of essential services (OESs) and relevant digital service providers (RDSPs) to undertake measures to manage the risks posed to the security of their networks. Under the UK GDPR and the NISR, organisations should assess the security risk associated with their own operations and implement appropriate controls, which could be in the form of organisational policies, physical and technical measures and/or conducting risk analysis.

Organisations regulated by the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) will need to comply with the data security obligations set out in the Financial Services and Markets Act and are required to have in place adequate systems and controls to monitor, detect and prevent financial crime.

28 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the UK GDPR organisations are required to record all personal data breaches, regardless of whether they are reported to a regulator. There is no specific rule on format or timing for retaining the records, although the record must contain the facts relating to each data breach, its effect and the remedial action taken.

Under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), the Information Commissioner's Office (ICO) requires that communications network and service providers keep a log of any personal data breaches, and that they submit this to the ICO on a monthly basis. The log should contain the facts of the breach, the consequences and any remedial action taken.

Under the NISR, regulated entities must maintain records evidencing the appropriate and proportionate technical and organisational measures taken to manage risks to their systems. The NISR do not prescribe any format or retention period for these records. Records should be accurate and accessible to the competent authority.

29 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

For breaches that compromise network security, the NISR require OESs and RDSPs to notify the ICO of security incidents without undue delay. The government is consulting on changes to the NISR which would require enhanced cyber incident reporting to other regulators, such as Ofcom and Ofgem. The government also proposes a requirement to notify regulators of all incidents that pose a significant risk to resilience and security, not just those that directly impact services.

In relation to cybersecurity breaches that involve personal data, the UK GDPR and the DPA 2018 requires data controllers to notify the ICO without undue delay, and no later than 72 hours after becoming aware of the incident, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The notification must provide details of (1) the nature of the breach; (2) the organisation's Data Protection Officer (if relevant); (3) the likely consequences of the breach; and (4) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

The PECR require telecoms and internet service providers to notify the ICO if a personal data breach occurs within 24 hours of becoming aware of the facts of the breach. The notification must include the name of the service provider, circumstances of the breach, nature and content of the personal data and the technical and organisational measures applied to the affected personal data.

The ICO website provides links for the reporting of incidents under the UK GDPR, PECR, and NISR.

The FCA also requires regulated organisations to notify the FCA and PRA in the case of a data security breach.

Time frames

30 | What is the timeline for reporting to the authorities?

The UK GDPR places a legal obligation on all organisations to report cybersecurity breaches to the ICO within 72 hours of becoming aware of any given breach. The threshold for notification to the ICO will be met if the breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A notification to the ICO will not be required where the business can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the business that is subject to the breach must inform those affected individuals without 'undue delay'. In practice, the notification to the data subject will be required as soon as possible provided the breach is sufficiently severe to be considered high risk.

While the obligations under the GDPR have general application, additional notification obligations may arise depending on the nature of the organisation. For example, UK trust service providers must notify the ICO of a security breach that may include a personal data breach within 24 hours under the eIDAS Regulation.

The NISR also impose reporting standards on these organisations in essential services, with mandatory notification to the relevant authority within 72 hours of becoming aware of an incident occurring.

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no generally applicable requirements to reports threats or breaches to industry, customers or the general public.

In relation to cybersecurity breaches that involve personal data, the UK GDPR requires data controllers to inform affected individuals about breaches that are likely to result in a high risk to their rights, without undue delay, after becoming aware of the incident. The communication must provide details of (1) the organisation's data protection officer (if relevant); (2) the likely consequences of the breach; and (3) the measures taken, or proposed to be taken, to deal with or mitigate any possible adverse effects.

UPDATE AND TRENDS

Key developments of the past year

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Cybersecurity affects all internet-enabled businesses, but imposing the same regulations on all market participants is not practical. To date, UK regulations have focused on critical service providers, with the National Cyber Security Centre issuing guidance to sectors of the economy such as the self-employed and small and medium-sized enterprises.

Cybersecurity regulations must also allow for flexibility and be technology-agnostic to enable emerging threats to be countered. It is in this spirit that the UK government is consulting on changes to the Network and Information Systems Regulations 2018 (NISR) to create a process for the government to designate unregulated organisations as being 'critical' and therefore subject to the NISR's requirements.

The government is currently consulting on changing the scope of the NISR to encompass a broader range of service providers and incident types, among other developments.

* *The authors would like to thank Felix Zimmermann, Rachel Mahoney, Ryan Williams and Martin Murphy for their contribution to the chapter.*

simmons+simmons

Robert Allen
robert.allen@simmons-simmons.com

Lawrence Brown
lawrence.brown@simmons-simmons.com

Neil Westwood
neil.westwood@simmons-simmons.com

Russell Cowie
russell.cowie@simmons-simmons.com

Emily May
emily.may@simmons-simmons.com

Citypoint
1 Ropemaker Street
London, EC2Y 9SS
United Kingdom
Tel: +44 20 7628 2020
Fax: +44 20 7628 2070
www.simmons-simmons.com

United States

Edward R McNicholas, Fran Faircloth and Briana Fasone

Ropes & Gray LLP

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Several key federal criminal statutes promote cybersecurity, including the Computer Fraud and Abuse Act (CFAA), 18 USC section 1030, outlawing hacking and other computer crimes; the Economic Espionage Act of 1996; the Defend Trade Secrets Act of 2016; and the Electronic Communications Privacy Act (ECPA), 18 USC sections 2510, which prohibits certain access to information in transit or when held by a stored communications provider or remote computing service (including cloud providers). All states also have computer crime statutes that address unauthorised access and computer trespass, and many states have further statutes that address spyware, phishing, ransomware and other cyberattacks.

On the regulatory front, cybersecurity is governed by a patchwork of generally applicable federal laws, sector-specific federal laws, state statutes and common law norms. At the federal level, both the primary cybersecurity regulators have only indirect authority. The Federal Trade Commission (FTC) is a the primary regulator of data security, albeit indirectly through section 5 of the FTC Act, 15 USC section 45(a)(1), which prohibits 'unfair and deceptive acts or practices' affecting commerce. Under section 5, the FTC may bring civil enforcement actions against companies that fail to implement reasonable security controls for sensitive data if that inaction causes, or is likely to cause, substantial harm to consumers that they cannot reasonably avoid. The FTC can also use section 5 against deceptive statements, including when institutions contravene security standards to which they pledge adherence. The Securities and Exchange Commission (SEC) is also emerging as a significant regulator through its role in ensuring that participants in the public securities markets provide all material information to investors.

The Cybersecurity and Infrastructure Security Agency (CISA), created by the Cybersecurity Act of 2015, 6 USC sections 1501-1510, has clear authority to be an active participant in cybersecurity at the federal level. While CISA lacks formal regulatory authority over the private sector, it is charged with the vital task of coordinating information sharing within the government and with private entities.

Additionally, a range of sector-specific federal laws contain cybersecurity provisions and provide for regulatory enforcement of data security standards, including the Gramm-Leach-Bliley Act (GLBA), 15 USC sections 6801-6809, 6821-6827, for financial services and the Health Insurance Portability & Accountability Act (HIPAA) Security Rule, 45 CFR Part 160, 164(A), and 164(C), which applies to protected health information (PHI) processed by healthcare entities or their business associates.

Significant aspects of the United States cybersecurity regime are also subject to industry self-regulation. The Payment Card Industry's Data Security Standard (PCI-DSS), for example, outlines protections required for payment cards used by merchants or vendors.

At the state level, numerous laws impose cybersecurity obligations that protect information from unauthorised use. Every state has adopted some version of an unfair or deceptive act statute, and many states have also adopted statutes requiring some form of 'reasonable security'. The California Consumer Privacy Act, which will be expanded by the California Consumer Privacy Rights Act in 2023, creates a right of action with statutory damages of $100 to $750 per person for state residents if plaintiffs can prove that the impacted business failed to implement reasonable security protocols to protect personal information, which resulted in a breach of their personal information. Several states have also implemented sector-specific cybersecurity requirements. The New York Department of Financial Services (NYDFS), for example, has issued cybersecurity requirements for financial services companies licensed in New York. Its Cybersecurity Regulation has served as a regulatory model for the FTC and other state insurance agencies.

Finally, the United States cybersecurity framework includes applying common law norms, developed by both the federal and state judiciary, to complex data protection issues. Plaintiffs in cases involving tort theories of negligence and trespass, for instance, must be able to articulate whether there existed a duty to protect information and damage proximately resulting from a violation of that duty – and that inquiry may vary by state. While some state courts have found no common law duty to protect personal data, others have found such a duty under certain circumstances.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Cybersecurity law in the United States is very sector-specific, but it focuses on the 16 critical infrastructure sectors identified in the Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. The healthcare and financial services sectors are particularly subject to specific and detailed cybersecurity requirements. The primary regulator for healthcare is the Department of Health and Human Services, through its Office of Civil Rights (OCR), which sets standards for protecting electronic Protected Health Information (ePHI), including ePHI stored in electronic medical records. The security of medical devices that collect, store and transmit information, including ePHI, has also drawn the attention of federal agencies in recent years, including the Food and Drug Administration, which first issued guidance related to cybersecurity for these devices in 2014.

Numerous regulators oversee cybersecurity matters in the financial services sector, with the SEC wielding authority over certain registered advisors, broker-dealers and funds. The SEC, through its Office of Compliance Inspections and Examinations, has taken enforcement

actions against registrants and public companies that experience data breaches. Other financial services regulators include the FTC, the Commodity Futures Trading Commission, and the Consumer Financial Protection Bureau. Self-regulatory agencies such as the Financial Industry Regulatory Authority and the National Futures Association have also issued cybersecurity rules.

In response to the growing threat posed by cyberattacks to the United States government and private sectors, there has been increased focus on cybersecurity requirements applicable to defence contractors. In May 2021, President Biden issued an executive order on Improving the Nation's Cybersecurity, with the stated goals of strengthening the cybersecurity posture of both the federal government and its contractors. Many requirements – information sharing, incident reporting, contractual provisions related to cybersecurity and supply chain security – already applied to members of the defence industrial base (DIB), either through existing federal regulations, such as the Defense Federal Acquisition Regulation Supplement or contractual requirements. The Department of Defense's Cybersecurity Maturity Model Certification (CMMC) programme, codified in 2020, is a key component of the government's DIB cybersecurity effort.

Several other sectors have specific requirements. For instance, the Department of Energy has an office of Cybersecurity, Energy Security, and Emergency Response, which oversees energy grid security and has undertaken various efforts, such as the Cyber Testing for Resilience of the Industrial Control Systems programme. Similarly, the Chemical Facility Anti-Terrorism Standards programme requires the Department of Homeland Security (DHS) to establish risk-based cybersecurity performance standards for facilities that produce, handle or store chemicals considered to pose a high risk. And in the communications sector, the Federal Communications Commission has used its statutory authority under 47 USC section 151 et seq. to promote the security of information that is stored and transmitted on communications networks as well as to enhance the security of the networks themselves.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Although the United States has not formally adopted binding standards related to cybersecurity, the National Institute of Standards and Technology (NIST) developed an influential Cybersecurity Framework, initiated by an executive order issued by President Obama in February 2013, that builds on several international standards, including ISO/IEC 27001. The NIST security compliance standard, SP 800-53, is mandatory for all United States federal information systems except those related to national security, which must comply with higher standards. The NIST guidelines easily map to the International Organization for Standardization's ISO 27001:2013 for implementation of information security in either the public or private sector.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The Sarbanes Oxley Act of 2002 requires public companies to maintain appropriate governance of their key information systems so that officers can provide assurances of the integrity of material data as well as detect, mitigate and disclose material cybersecurity weaknesses. Officers and directors of corporations also owe common law fiduciary duties of care and loyalty to shareholders, which include an obligation to oversee cybersecurity risks. Failure to do so could lead to securities actions or shareholder derivative lawsuits. The standard for corporate oversight was established in *In re Caremark International Inc*, 698 A.2d 959 (Del. Ch. 1996). Under the *Caremark* standard, directors must 'exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility'. While *Caremark* was not a cybersecurity case, this standard has been applied in the wake of data breaches, where shareholder derivative suits have alleged that the board failed to implement a proper information security infrastructure, failed to investigate and remediate breaches after they occurred, or failed to disclose incidents to the public in a timely manner as required by law.

Cybersecurity governance standards are also outlined in various federal agency sectoral guidelines. For instance, the Federal Financial Institutions Examination Council has issued an Information Technology Handbook that details risk management strategies for corporate boards. Likewise, the Federal Reserve's Interagency Guidelines Establishing Information Security Standards features a section on board responsibilities, including, at a high level, the development, implementation, and oversight of a written security programme.

5 How does your jurisdiction define cybersecurity and cybercrime?

Definitions vary across federal and state laws. For instance, the CFAA, 18 USC section 1030, generally addresses cyber criminals as those who 'knowingly accessed a computer without authorization or exceeding authorized access'. The Department of Justice, in its manual on computer crime, broadly defines cybercrimes (a term used interchangeably with 'computer crimes') as 'any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution'.

The NIST Glossary defines cybersecurity as 'the process of protecting information by preventing, detecting, and responding to attacks'. It also defines a cybersecurity *event* as a 'cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)', which the institute distinguishes from a cybersecurity *incident*, defined as 'a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery'.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

While there does not exist a single set of mandatory protective measures at the federal level, NIST's Cybersecurity Framework, designed for private sector organisations, outlines best practices for cybersecurity compliance. Recently, the FTC announced an updated Safeguards Rule under GLBA requiring certain financial institutions to strengthen data security safeguards to protect consumer information. The FTC's new Safeguards Rule requires specific security controls and accountability measures (modelled after the NYDFS cybersecurity rule), including multifactor authentication for any individual accessing information systems storing customer information, encryption of all customer information (both in transit and at rest), and updates to record retention procedures. The revisions also dictate specific governance controls by requiring reporting to a senior officer about the institution's security posture and the adoption of a formal incident response plan.

Additionally, numerous state statutes include some kind of 'reasonable security' requirement. Massachusetts' cybersecurity regulations have long imposed specific security requirements regarding personal information, including the implementation of a written security programme and encryption of certain data. New York's SHIELD Act

requires reasonable security for personal information and specifies measures that may satisfy that standard.

Scope and jurisdiction

7 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The Computer Fraud and Abuse Act, the primary statutory mechanism for prosecuting cybercrime, provides a tool for entities seeking to protect intellectual property and computer systems from cyberthreats. The Economic Espionage Act of 1996 and the Defend Trade Secrets Act are additional sources of potential criminal and civil penalties against the cyber theft of trade secrets and other valuable intellectual property. The Digital Millennium Copyright Act of 1998 is designed to protect copyright holders from unlawful reproduction or distribution of their work and the act covers music, films, text – anything that can be copyrighted. Every state also has a computer crime statute.

8 | Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Yes, President Obama's Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience identified 16 areas of critical infrastructure and tasked the Secretary of Homeland Security to lead a unified national effort to protect these areas, in coordination with the relevant primary federal regulator for that sector. For instance, The Federal Energy Regulatory Commission is responsible for 'ensuring the reliability of the bulk power system of North America', and the North American Electric Reliability Corporation has enhanced cybersecurity in the energy sector by issuing alerts through the Electricity Information Sharing and Analysis Center and promulgating and enforcing Critical Infrastructure Protection Reliability Standards. The Transportation Security Administration can also promulgate regulations related to pipeline cybersecurity and has so far issued two directives about protecting against cyber intrusions. Likewise, the SEC, as well as several other agencies, addresses cyber threats to financial infrastructure. President Biden's recent Executive Order on 'Improving the Nation's Cybersecurity', aims to further enhance critical infrastructure cybersecurity.

9 | Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

President Clinton's Presidential Decision Directive-63 (PDD-63), signed on 22 May 1998, required the federal government to work with each critical infrastructure sector to establish sector-specific organisations to share information about threats and vulnerabilities. President Obama issued the 2015 Executive Order 13691 directing the Department of Homeland Security to encourage the development of similar Information Sharing and Analysis Organizations, while the Cybersecurity Information Sharing Act of 2015 provided guidance and substantial immunities to facilitate private entities sharing cyber threat indicators, but prohibited the sharing of personally identifiable information.

Various regulatory safeguards restrict the disclosure of certain information, including information related to cyberthreats, such as the Electronic Communications Privacy Act, and sector-specific privacy laws also restrict the sharing of information which can include sharing cyberthreat information. For instance, in the healthcare sector, the HIPAA Privacy Rule established national standards to protect the privacy of PHI and curtails unauthorised data disclosures.

10 | What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The Economic Espionage Act, CFAA, and computer crime laws in every state criminalise a wide variety of conduct. The CFAA imposes criminal and civil liability on anyone who, in short, receives information by intentionally accessing a 'protected computer' without authorisation or while exceeding authorised access. Hacking, unauthorised access, trespass, viruses, malware, denial of service attacks, ransomware, computer extortion, phishing and spyware are also criminalised under various laws, not to mention federal and state prohibitions on wire fraud, bank fraud and fraud schemes generally.

11 | How has your jurisdiction addressed information security challenges associated with cloud computing?

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide risk management programme that provides a standardised approach to conducting security assessments and monitoring cloud products and services. Under FedRAMP, to be eligible to provide services to federal departments and agencies, cloud service providers (CSPs) must agree to contractual clauses requiring that they implement baseline controls and capabilities, including two-factor authentication, code analysis scans, encryption protocols and the ability to process electronic discovery and litigation holds. The CSP must then directly apply or work with a sponsoring agency to obtain FedRAMP authorisation. If provisionally accepted into FedRAMP, the CSP must hire a third-party assessment organisation to independently assess its systems.

While there exists no overarching private-sector regulation specifically addressing cloud computing, various industries have generated their own requirements for CSPs. For example, under HIPAA, a CSP is considered a 'business associate'. Accordingly, a covered entity and CSP must enter into a HIPAA-compliant *business associate agreement* (BAA), with the CSP becoming both contractually liable for meeting the terms of the BAA and liable for compliance with applicable requirements of the HIPAA Rule. Additionally, government contractors may have to comply with the cloud security requirements of the DOD, which issues mandatory contractual clauses for DOD CSPs.

12 | How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations conducting business in the United States are generally subject to the same federal and state laws and regulatory obligations as domestic companies.

BEST PRACTICE

Increased protection

13 | Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

While the National Institute of Standards and Technology (NIST) Cybersecurity Framework is voluntary and aimed at critical infrastructure, it has evolved into a de facto standard for organisations and has inspired other sets of cybersecurity guidelines. The Federal Financial Institutions Examination Council adapts the NIST framework to financial services, and the Cybersecurity Maturity Model Certification (CMMC) provides a standard for the defence-industrial base, which is consistent with the NIST framework.

The NIST Cybersecurity Framework provides guidance to help organisations manage cybersecurity risks and is organised around an assessment of the five 'functions' of an effective cybersecurity programme:

- identification – the capacity to identify and understand organisational cyber risks;
- protection – the development and implementation of appropriate safeguards to secure critical infrastructure;
- detection – the activities and capabilities to detect cybersecurity intrusions and attempted intrusions;
- response – the capability to react and respond to a detected cybersecurity incident; and
- recovery – the activity of planning for resiliency and the capability to maintain or restore services that are impaired by a cybersecurity incident.

14 | How does the government incentivise organisations to improve their cybersecurity?

Although authorised under Executive Order by President Obama, the United States does not overtly use government incentives (grants, tax credits) to persuade companies to improve cybersecurity systems. President Biden's Executive Order has recently made clear that access to federal contractors will depend on private companies being able to comply with federal cybersecurity standards, and this approach has long been to incentivise federal defence contractors.

15 | Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework;
- Payment Card Industry's Data Security Standard (PCI-DSS): https://www.pcisecuritystandards.org/;
- Cybersecurity and Resiliency Observations: https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf;
- Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements: https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of; and
- Cybersecurity Maturity Model Certification: https://www.acq.osd.mil/cmmc/.

16 | Are there generally recommended best practices and procedures for responding to breaches?

Several agencies have produced guidelines – from comprehensive manuals to a single web page – that can be valuable when engaging in incident response. For example, the Federal Trade Commission has published a useful data breach response guide geared toward businesses and provides a separate resource for complying with its health breach notification rule. The Computer Crime and Intellectual Property Section of the Criminal Division in the United States Department of Justice released a revised version of its Best Practices for Victim Response and Reporting of Cyber Incidents and the Cybersecurity & Infrastructure Security Agency has developed a series of cybersecurity incident and vulnerability response playbooks.

Information sharing

17 | Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Since 2018, the Cybersecurity and Infrastructure Security Agency has led efforts to coordinate the United States approach to cybersecurity as well as government outreach to private companies. Many private companies participate in Information Sharing and Analysis Centers or Information Sharing and Analysis Organizations, which share threat intelligence, including from government sources. The Department of Homeland Security (DHS) has instituted a Cyber Information Sharing and Collaboration Program, through which it shares unclassified threat intelligence information via public-private networks in the critical infrastructure sector. The United States Computer Emergency Readiness Team provides national threat intelligence and works to assist critical infrastructure in responding to cybersecurity threats. The DHS also operates an Automated Indicator Sharing capability that shares real-time threat indicators and defensive measures.

18 | How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The government and private sector cooperate in developing regulatory cybersecurity standards through an informal notice-and-comment rulemaking process. Federal and state agencies use notice-and-comment rulemaking procedures for most rulemaking actions, including when creating new administrative regulations or repealing existing regulations.

Insurance

19 | Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance for cybersecurity incidents, which can help cover the costs of responding to a major security incident, is available in the United States and has become increasingly common for large companies with significant consumer information. Such coverage has become more difficult to obtain in adequate amounts at reasonable prices due to the rise in ransomware.

ENFORCEMENT

Regulation

20 | Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Federal Trade Commission (FTC) is the primary federal cybersecurity regulatory authority and has interpreted its authority under section 5 to require companies to implement security measures. Notably, however, section 5 does not apply to many not-for-profit organisations or institutions regulated by another federal agency, such as most financial services and much of the healthcare industry.

The Securities and Exchange Commission (SEC) has also increasingly taken on the mantle of a general cybersecurity regulator and overseer for public companies, issuing guidance on disclosure obligations for cybersecurity risks and incidents, and fining companies that fail to comply. The SEC has also been particularly aggressive in issuing guidance, conducting examinations and conducting market examinations of the cyber risks facing entities that it directly regulates, such as investment advisers.

In the healthcare sector, the Office of Civil Rights is the main regulatory authority as the primary Health Insurance Portability &

Accountability Act (HIPAA) enforcement body, but other regulators, including the FTC, play a role for entities that are not covered by HIPAA, including companies that collect health-related information from connected devices.

State attorneys general have broad authority regarding the enforcement of cybersecurity matters and often cooperate in multi-state groups to investigate companies experiencing data breaches. Additionally, state departments of insurance oversee the cybersecurity of their regulated entities.

21 | Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Both federal and state authorities wield wide-ranging authority – from investigating health information privacy complaints and data breaches with the potential to enforce civil and criminal penalties (OCI enforcing HIPAA) to imposing specific cybersecurity requirements on banks and credit unions (New York Department of Financial Services). This power often includes the ability to demand information related to cybersecurity incidents.

The FTC's assertion of authority over information security, however, is limited by its statutory powers under section 5 of the FTC Act to prohibit 'unfair or deceptive acts or practices' that injure consumers – an expansion of authority that has received close judicial review and approval. The FTC has used its section 5 authority to bring enforcement actions predicated on claims of 'deception' as well as claims alleging 'unfairness.' During such actions, the agency has the power to request or demand documents and information and enter settlements requiring payment of civil penalties and other injunctive measures.

Similarly, state attorneys general generally have the authority to prosecute businesses that fail to comply with state requirements to report cybersecurity incidents. This includes the power to investigate and request information related to the incident and to prosecute for damages and civil penalties.

22 | What are the most common enforcement issues and how have regulators and the private sector addressed them?

For many years, the most common cybersecurity enforcement issues have related to an organisation's failure to provide breach notifications in a timely manner or a general lack of reasonable or appropriate information security protections. Regarding the lack of information security protections, the private sector has sought additional guidance on what might be considered 'reasonable.' In some cases, regulators have responded. For example, the SEC, through the Office of Compliance Inspections and Examinations, has issued guidance on what it views as the components of an effective cybersecurity governance programme.

23 | What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

State data breach laws vary, but a security incident is generally reportable to consumers if there is acquisition of, or in some cases merely access to, personal information. The data elements covered by state-level breach vary. For example, while all states include sensitive identifiers like social security number in the definition of personal information, states vary on whether to include things like health data or fields without names. There are also various state sector-specific laws related to obligations to report heath and insurance-related data incidents.

Federal sector-specific laws also require notification for certain security incidents and may override state rules. HIPAA, for instance, generally requires notification in the event of a security incident impacting unsecured protected health information. HIPAA generally does not pre-empt state laws, but several state laws have an exception for compliance with HIPAA.

Penalties

24 | What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Common penalties for failure to comply with preventative cybersecurity regulations can include civil payments, cease-and-desist orders, criminal punishment or insurance termination. In California, for instance, a person can claim actual or statutory damages of $100–$750 per person for certain data breaches caused by a lack of reasonable information security.

25 | What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Penalties vary by statute and state. Civil penalties for unknowing HIPAA violations, for example, can range from $100 to $50,000 per violation, with the potential for greater criminal penalties as well. State laws allow for the Attorney General to prosecute companies that do not appropriately report breaches for civil penalties that can range from $10,000–$500,000 depending on the state statute and the severity of the breach.

26 | How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Many federal statutes, including HIPAA and the Gramm-Leach-Bliley Act, do not have private right of action. California's privacy law, the California Consumer Privacy Act, does provide a private right of action for individuals whose personal data is breached as a result of a failure of a business to provide reasonable security measures. Despite the lack of a private right of action in most cases, plaintiffs have sought to bring cases, sometimes successfully, claiming violations of, among other things, contractual rights, common law torts, and state and federal statutes with data-related provisions. The standing of plaintiffs to bring such cases often turns on whether the court determines that the parties have alleged an injury as a result of the incident.

THREAT DETECTION AND REPORTING

Policies and procedures

27 | What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Data protection requirements for organisations vary by business sector. In particular, the healthcare and financial services sectors are both subject to specific and detailed cybersecurity requirements. For example, in the healthcare sector, Health Insurance Portability & Accountability Act (HIPAA) covered entities must '[i]mplement policies and procedures to prevent, detect, contain, and correct security violations' and to restrict access to protected health information (PHI) only to authorised personnel.

State laws have also begun to develop policies and procedures that companies must put in place for cybersecurity protection. For example, Massachusetts' cybersecurity regulations have long imposed specific security requirements regarding personal information, including the implementation of a written security programme and encryption of certain data. New York's SHIELD Act similarly requires reasonable

security for personal information and specifies measures that may satisfy that standard. And California privacy law creates a right of action for state residents if plaintiffs can prove that the impacted business failed to implement 'reasonable' security protocols to protect personal information.

28 | Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There is currently no broad rule requiring organisations to maintain records of cybersecurity incidents, though record-keeping is required by certain states if an organisation determines that notification is not required because an incident does not pose a significant 'risk of harm' to individuals. Healthcare entities subject to HIPAA and organisations that process credit card information, subject to the Payment Card Industry's Data Security Standard, are required to maintain certain information, including records of incidents to facilitate reporting or audits.

29 | Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws. While these state laws are not uniform, they can generally be said to define a 'breach' as the unauthorised acquisition of or access to unencrypted computerised data that compromises the security, confidentiality or integrity of personal information. Most states also include a requirement that the incident is reasonably likely to cause harm to individuals. Organisations that experience a security breach may be required to notify affected individuals or state regulators (or both) of the incident. Under the state laws, the triggers for when regulatory authorities must be notified vary. While all states have a law that requires notice to data subjects in the event of certain breaches, a few states require no notice to regulators. In other states, such as New York or Massachusetts, regulators must be notified if a single resident receives notification of a cybersecurity breach, while in still others, such as California, notice is required only where a certain number of individuals are affected (often 500 or more, but this varies by state).

Sector-specific federal laws require reporting of cybersecurity breaches in certain circumstances. In the healthcare industry, entities covered by HIPAA must notify the Department of Health and Human Services following a breach of unsecured PHI, as those terms are defined within the statute. Financial institutions must often likewise report certain incidents to their primary regulator.

Time frames

30 | What is the timeline for reporting to the authorities?

In the healthcare industry, entities covered by HIPAA must notify the Office of Civil Rights (OCR) within 60 days of the end of the calendar year in which a breach is discovered for breaches involving PHI of fewer than 500 individuals and without unreasonable delay in matters involving more than that number.

Under the state laws, the triggers for when regulatory authorities must be notified vary. While all states have a law that requires notice to data subjects in the event of certain breaches, a few states require no notice to regulators. In other states, such as New York or Massachusetts, regulators must be notified if a single resident receives notification of a cybersecurity breach, while in still others, such as California, notice is required only where a certain number of individuals are affected (often 500 or more, but this varies by state). Timelines for these notices also vary, with Vermont requiring notice within 14 business days of discovery of a breach that triggers notice and other states requiring notice without unreasonable delay and simultaneous with or before notice is sent to consumers.

Entities covered by the New York Department of Financial Services (NYDFS) Cybersecurity Regulation or some similar state insurance data security laws must generally report incidents within 72 hours after determining that a cybersecurity event has occurred that triggers notice.

ROPES & GRAY

Edward R McNicholas
edward.mcnicholas@ropesgray.com

Fran Faircloth
fran.faircloth@ropesgray.com

Briana Fasone
briana.fasone@ropesgray.com

2099 Pennsylvania Avenue NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
www.ropesgray.com

Reporting

31 | Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws. While these state laws are not uniform, they can generally be said to define a 'breach' as the unauthorised acquisition of or access to unencrypted computerised data that compromises the security, confidentiality or integrity of personal information. Most states also include a requirement that the incident is reasonably likely to cause harm to individuals. Organisations that experience a security breach may be required to notify affected individuals or state regulators (or both) of the incident. Timing of notices varies by state and sector, with Colorado, Florida and Maine requiring notice within 30 days of discovery of the notifiable event, while the NYDFS requires notice in 72 hours and one banking agency (the Federal Deposit Insurance Corporation) recently proposed a 24-hour notice requirement.

Several sector-specific federal laws also require reporting of certain breaches in particular circumstances. For example, in the healthcare industry, entities covered by HIPAA must notify the OCR within 60 days of the end of the calendar year in which a breach is discovered for breaches involving PHI of fewer than 500 individuals and without unreasonable delay in matters involving more than that number. Entities regulated by the Securities and Exchange Commission are expected to make prompt public disclosures regarding any cybersecurity incidents, in addition to disclosing general cybersecurity risk, and it has become increasingly standard and expected for organisations to issue a 'current report' (known as an 8-K), which is not a regularly scheduled disclosure, for the disclosure of material cybersecurity events.

UPDATE AND TRENDS

Key developments of the past year

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

The private sector in the United States is subject to a complex and often overlapping or conflicting set of laws and regulations that affirmatively impose obligations and prescribe limitations on cybersecurity practices, leaving companies unsure of how best to comply. In response, the private sector has taken concerted steps to address cyber risks, most notably through industry standards and by enhancing contractual protections in vendor relationships.

simmons+simmons

Our team provides a business-focused and pragmatic approach.

Our international data, privacy and cybersecurity practice spans the globe advising within the Asset Management & Investment Funds, Financial Institutions, TMT and Healthcare & Life Sciences sectors.

Our lawyers advise on the full suite of data and cybersecurity issues – from implementing preventative measures and regulatory requirements through to data breach response and full-scale litigation.

simmons-simmons.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-941-0