Abnormal

# Email Security and Legal Compliance:

## Navigating Organisational Responsibilities in the Cyberthreat Landscape

MKT359_Oct_2023

# Executive Summary

Internet and electronic communications - such as emails and chat messages - are valuable tools for modern businesses, but they also present many threats to the security of information. Bad actors are finding new ways to gain access to organisations' communications technologies, networks, and information systems.

## Email-Enabled Cybercrimes:

Cyberattacks sent over email that use social engineering tactics to trick people into sharing private data or installing malicious software.

*Abnormal Security*

## Business Email Compromise (BEC):

A form of email attack that uses impersonation to steal money from unsuspecting victims and employs conversational techniques designed to build trust between the attacker and target.

*Fraud Act 2006, Section 2*

## Ransomware Attack:

A type of cyberattack that encrypts its victims' files where once attackers have infiltrated a system, they then demand a ransom in exchange for returning access to the data.

*Abnormal Security*

They can use this access to:

- Commit business fraud, such as business email compromise attacks, CEO impersonation, and vendor/invoice fraud.
- Gather sensitive account information such as access credentials and other confidential information, through phishing emails and hyperlinks contained within them.
- Deliver malware, such as ransomware and other viruses, trojans, and worms.
- Pursue interpersonal crimes and harms, such as cyberstalking, bullying, and trolling.
- Fraudulently solicit money from individuals or organisations.
- Enable other content crimes, such as the dissemination of prohibited materials.

Due to the importance that society attaches to business resilience, human dignity, and the prevention and detection of crime, there are an array of laws that regulate the use of email and email-like communications systems. These include cybersecurity laws that govern critical infrastructures and services; data protection laws that regulate the processing of personal data; laws that apply to private obligations, such as those that arise in a commercial context between businesses and are addressed in contracts; and laws that set out criminal offences.

This white paper examines some of the operational and legal contexts associated with emails and email-like communications to emphasise organisations' legal responsibilities to protect themselves from cyberthreats. In particular, where such laws exist, they may generally require organisations to have regard to the state of the art, including the state of technological development. In practical terms, when they do consider the state of the art, these organisations will want to consider the developments in email and email-like security technologies offered to the market by companies such as Abnormal Security.

## Malware Propagation:

A type of malicious software designed to disrupt a victim's computer, server, or network. It's a catch-all term for software like viruses, trojan horses, ransomware, spyware, worms, and more.

*Computer Misuse Act 1990, Section 3*

## Denial of Service Attack (DoS):

Occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

*Cisa.gov*

## Exfiltration of Personal Data:

The intentional, unauthorized, covert transfer of data from a computer or other device. Data exfiltration may be conducted manually, or automated using malware.

*IBM*

# Email and Email-Like Communications in a Business and Societal Context

Electronic communications are central to our business processes, societal functions and personal lives. Email is the most pervasive, well known, and oldest form of electronic communication in the modern technological environment. For example, the first network mail over the ARPANET, the forerunner to the Internet, was sent in 1971 and our reliance upon it is ever increasing[1]. Other popular forms of electronic communications, such as chat messaging and those within collaborative working platforms such as Teams, Slack, or Zoom, are essentially "email-like", in terms of their use of text and chat and due to their trajectory of growing adoption and use.

However, due to their centrality, email and email-like communications provide many attack vectors for bad actors who harbour malicious and criminal intentions.

The fact that email and email-like communications provide attack vectors for bad actors is well understood. What is less well-known is how this fits together in a legal sense; what this means for the well-being of our people; how this knits together for business trust and reputation; and why businesses and other organisations must keep abreast of technological developments that assist with the management and reduction of email and email-like threats.

Whatever the position we take when looking at the role that email and email-like communications play in our lives, one thing is certain: due to their centrality and for the purpose of operational risk management and the discharge of our legal and ethical duties, we must keep them front-and-centre of our thinking, recognising the need to have regard to the state of the art and the state of technological development. In this way we can ensure that we are able to take advantage of new email and email-like security technologies that can meaningfully aid operational risk management and discharge of legal obligations.

[1] According to Statista.com email remains an integral part of our daily online lives, despite the growth in alternative forms of electronic communications such as mobile messengers and chat apps. In 2017, the number of global email users was 3.718bn and is set to grow to 4.6bn in 2025. 306bn emails were sent and received every day in 2020, which is projected to rise to 376bn in 2025. https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/

# The Negative Side of our Reliance on Email and Email-Like Communications

It is widely recognised that email and email-like communications can be used for both cyber-enabled and cyber-dependent crimes. Cyber-enabled crimes encompass "traditional" crime areas that can be committed without the use of information and communications technologies (ICT), but that are scaled and industrialised through cyberspace. Examples include fraud, theft, and blackmail. Cyber-dependent crimes are ones that cannot be committed without the use of ICT—hacking, malware distribution, and denial of service attacks. Some cybercrimes are hybrid, covering both aspects. Additionally, many kinds of cybercrime can and do involve the use of email and email-like communications at some point of the attack. For example, email might be used as part of the preparatory phases of an attack, such as an attempt to obtain sensitive information; or email might be used in the substantive attack phase, executing fraud or to transmitting illegal payloads; or the email systems themselves might be the target of the attack, achieving account takeover or compromise.

## Personal Data in Email Systems

The data stored in email systems can be highly sensitive and can include personal information. Many employers allow their workers to use their business email for personal purposes or as a primary contact medium for dealing with customers. Other organisations may have to process personal customer data at the heart of their mission—police, healthcare businesses, schools, employment agencies, newpapers, telecommunications companies, and online social media platforms.

Personal data within emails can be targeted by cybercriminals for a variety of reasons—to provide leverage in a ransomware attack, to enable spying on dissidents by Nation State actors, or for Identity Theft and fraud purposes by organised crime groups. If an email account is taken over by cybercriminals, it can provide them with significant advantages.

Organisations that use email to process personal data might be regulated by data protection laws, thereby owing a duty of care to the persons whose data are contained in email systems.

# Business Email Compromise Example

A good example of a cyber-enabled crime that can also be cyber-dependent—and that is of deep concern to law enforcement agencies all over the world, due to its prevalence—is business email compromise (BEC). The UK National Cyber Security Centre[2] describes BEC as "*a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information*". The Federal Bureau of Investigation[3] in the United States says that BEC "*is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business - both personal and professional.*"

The main motivation behind a BEC attack is financial gain. BEC has a number of variants. Examples include:

- The attacker sends spoof emails that trick a person into transferring funds to an account under their control. To do this, the attacker might masquerade as a senior person in a business, in the expectation that by sending an email in that person's name, other people will be tricked into obeying the attacker's illicit instructions. This is sometimes known as "CEO Fraud".
- The attacker might send spoof invoices to perform the same trick. To do this, they might create wholly fabricated invoices that appear to be genuine, as happened in the Evaldas Rimasauskas case[4], or they might alter payment details in a genuine invoice. This is sometimes known as "Invoice Fraud". The email element within the crime might be that an email system is compromised for the purpose of sending the spoof invoice, so that it appears to come from a legitimate account and hence is genuine, or an email system might be compromised to give the attacker access to legitimate invoices which can then be altered, such as by changing the bank account details for the payment.

An attacker might also use email within the preparatory phase of a BEC attack. For example, during the preparatory phase, the attacker might use phishing emails for social engineering purposes, to obtain sensitive information that aids the attack such as details about the financial, invoicing and payments systems used by the victims of the attack. Alternatively, the goal might be to obtain access credentials for IT systems. The attacker might also use malware during the attack to obtain sensitive information, or to compromise a system, in which case the BEC attack will be a hybrid cyber-dependant and cyber-enabled attack.

## The Centrality of Phishing Emails Within Cybercrime

"Phishing emails, malicious document files, social engineering techniques, and unpatched soft- and hardware are the most common ways criminals introduce themselves into their victims' systems. Phishing is a key access vector for most types of online fraud schemes and malware-based attacks, aiming to intrude into systems, steal data, or extort money. Phishing emails containing malware, Remote Desktop Protocol (RDP) brute forcing, and VPN vulnerability exploitation are the most common intrusion tactics used by cybercriminals."

*Internet Organised Crime Threat Assessment, 2023*

[2] https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf
[3] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise
[4] https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business

# Other Criminal Purposes Enabled by Email and Email-Like Communications

## Europol's Assessment of Business Email Compromise and CEO Fraud

"As investment fraud takes the spotlight, business email compromise (BEC) and CEO fraud have remained key threats in the past 12 months, with some countries reporting a further increase in the number of cases. Continuing to lead to significant losses, both types of crime have grown in sophistication and become more targeted. Heavily relying on social engineering, attacks have increasingly focused on upper-level management, as well as on impersonating other staff members or changing invoice data in commercial transactions."

*Internet Organised Crime Threat Assessment, 2021*

Moving past the idea of a BEC attack and to draw things together, email and email-like communications play five major roles in cybercrime: (1) a social engineering tool, most obviously within a phishing attack, (2) a medium to deliver an illicit payload, most obviously the delivery of malware that is contained in the communication, or that is accessible through embedded hyperlinks, (3) a means of committing content and interpersonal crimes (e.g., to transmit unlawful images, or to support a campaign of harassment), (4) a method of denial of a service attack, or (5) an agent of spam, used to market illicit goods and black-markets. In some situations, the malicious use of email falls into multiple criminal categories.

As already noted, a key criminal purpose of social engineering emails, many types of spam emails and other attacks involving emails and email-like communications is fraud. For example, a person might be enticed to engage with a communication, which involves them handing over information that can be used for fraudulent purposes, or they might actually make a payment to a fraudster for goods and services thinking that they are using a legitimate marketplace. On the other hand, in a ransomware attack, the bad actor uses blackmail to make a demand with menaces, which is a crime under the Theft Act. Additionally, the commission of various computer misuse offences, covering unauthorised access to computer material, unauthorised access with intent to commit other offences and unauthorised acts with intent to impair the operation of a computer, are all offences under the Computer Misuse Act 1990.

## Evaldas Rimasauskas BEC Case - $120M Fraud

All sizes and types of organisations can fall victim to BEC attacks, including technology giants. In 2019, a Lithuanian cybercriminal, Evaldas Rimasauskas, was sentenced to 60 months imprisonment in the USA, following a lengthy, systematic invoice fraud scam that targeted two of the world's largest techcos. Rimasauskas raised spoof invoices that masqueraded as a real supplier to the victims, causing them to wire over $120M to bank accounts that he controlled.

# Account Takeover, or Account Compromise

If an attacker can take over an email account, they can use it as a platform for the commission of further cybercrimes. Moreover, email can form part of the attack vectors that lead to email account takeover or compromise.

The BEC example, above, illustrates what could happen: the email account that has been taken over could be used to send emails requesting payments that appear to the recipient to be legitimate, so they are tricked and fall victim to the fraud. A compromised email account could also be used to spray spam emails or malware.

It's also important to remember that account takeovers, another invasive attack, allow cybercriminals to facilitate espionage and data theft, because they have access to communications content and metadata. Equipped with these insights, the attacker will be able to commit additional cybercrimes.

In the workplace, many employers allow their workers to use their business email systems for personal purposes. Emails might also be the main contact medium for customers of businesses. In these situations, email account takeover or compromise can put these personal data at risk, leading to multiple data protection law infringements.

## Email Threats As Seen Through the Eyes of Law Enforcement

The Europol Internet Organised Crime Threat Assessment (IOCTA) 2021 provides a snapshot picture of the evolving nature of email-related cybercrime:

- **Emotet Botnet.** In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet. Emotet opened doors for Trojans, ransomware , and information stealers. Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document. If victims opened the attachment or the link, the malware got installed. The computer became vulnerable and was offered for hire to other criminals to install other types of malware.
- **Bank Phishing Emails.** Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information. These emails may look identical to the types of correspondence that actual banks send. They ask you to download an attached document or click on a link and replicate the logos, layout and tone or real emails, using language that transmits a sense of urgent.

# Evolving and Innovative Nature of Cybercrime

It must be kept in mind that cybercrime is a rapidly evolving area. It is also a highly innovative and entrepreneurial environment. For example, loose affiliations of criminals can operate as organised crime gangs, whose membership evolves with each attack, utilising criminal business models that replicate those in the lawful world. Thus, cyberspace includes a cybercrime gig economy and cybercrime online marketplaces with Crime-as-a-Service offerings. With Crime-as-a-Service, would-be cybercriminals can gain access to tools and services to enable them to launch their own cyberattacks, and in the cybercrime gig economy, criminals with cyberskills can make themselves available to hire.

The evolving and innovative nature of cybercrime enables cybercriminals to quickly take advantage of new opportunities, whether these be substantial social, economic, and technical upheavals, such as occurred during the pandemic, or more localised changes within specific organisations, or to capitalise on the discovery of vulnerabilities in technologies. Cybercriminals also need to evolve and innovate to avoid detection, apprehension, and prosecution. This includes evolving their attack tactics, techniques, and procedures to enable them to overcome or bypass detection and filtration technologies, including those that are applied to email systems.

To ensure that risk management frameworks are optimised and as effective as possible, organisations always need to keep in mind the dynamic nature of cybercrime. Steps and measures that have been adopted in the past to manage email and email-like threats and risks might lose some of their protective powers over time. This underscores a key facet of risk management, which is that it is a continual and ongoing process, rather than a moment-in-time event.

To ensure that risk management frameworks are optimised and as effective as possible, organisations always need to keep the dynamic nature of cybercrime in mind.

Furthermore, risk management frameworks need to reflect the fact that threat actors have different motivations, incentives, and goals, which alongside different attack tactics, techniques, and procedures, are key variables within risk assessments and treatments. There is not a universally agreed categorisation system of threat actors, so terminology differs between organisations and across territories. However, categories that will be widely recognised include Nation-State Actors, State-Sponsored Actors, Advanced Persistent Threats (APTs – these are often considered to be State-Sponsored), Hacktivists, Organised Crime Groups (these can also be State-Sponsored, or State-aligned) and a range of individual hackers with different skills and motivations that range from highly skilled "Old Guard" Hackers through to "Script Kiddies" who are new entrants, often of younger age with relatively low-level skills who harbour ambitions to climb the Hacker ranks[5]. Due to the innovative and entrepreneurial nature of cybercrime, cybercriminals can move between categories. For example, skilled hackers might work with State-Sponsored Actors or Organised Crime Groups from time-to-time. Motivations for their criminal behaviours can range from ideology for Nation-State and State-Sponsored Actors, to financial gain for Organised Crime Groups, to even just the thrill of a challenge. A common goal for cybercriminals is to avoid detection, apprehension, and prosecution and especially in cases of espionage often the goal is to remain hidden, unlike in ransomware attacks where the goal is to be as visible and disruptive as possible. What this means in practice is those different types of cybercriminals will be looking at email opportunities in different ways, for different purposes and with different skill levels.  This further underscores the fact that risk management for email has to be a continual and ongoing process, so that defences are able to resist evolving threats. Ideally, risk management for cybercrime purposes will take account of the behaviour aspects of the different categories of attacker.

[5] There are also people who engage in deviant behaviour online and through the use of email and other communications channels that are criminal by definition (e.g., making and sharing abuse images, or cyberstalking), but do not fall within the focus of this White Paper.

# The Opportunistic Nature of Cybercrime

Cybercriminals are constantly looking for new opportunities for crime and new victims to exploit. A recent example of a global criminal opportunity was the pandemic. This required a massive and rapid shift to online working, using video conferencing and collaborative working platforms as well as other technologies like VPNs, which were implemented at unprecedented speed and scale. Alongside this, the cashless economy took an exponential leap forward, due to the mass migration to online shopping. Sadly, among the many human tragedies that the pandemic caused, countless numbers of people either lost their jobs or suffered reduced incomes when put on furlough. This confluence of circumstances was a boon for cybercriminals who were able to exploit vulnerabilities in new communication and collaboration platforms, including vulnerabilities in their deployment and the establishment; various opportunities for fraud related to online shopping, such as parcel re-delivery fraud; and people's understandable thirst for updates on the virus and social restrictions. All of which exposed the public to dis-information about vaccines and treatments. Additionally, the need to find new jobs, supplement income, or protect savings, exposed them to recruitment fraud and savings and investment fraud. Children's time spent online also skyrocketed, exposing them to the worst that the Internet and cybercriminals have to offer.

Central to many of the Covid-driven cybercrimes was email and email-like communications, which acted as lures for social engineering and phishing, as delivery systems for malware and dis-information, and as targets for account takeovers.

## Opportunist Crime Example: Exploitation of Ukraine's Humanitarian Needs

The criminal underworld seems to stop at nothing to achieve its goals, including taking advantage of humanitarian crises. According to Europol, this also included taking advantage of people who wanted to raise funds for Ukraine:

"The invasion of Ukraine also showed once again cybercriminals' adaptability and opportunism. Online fraudsters responded swiftly to the circumstances and exploited the crisis by developing a variety of narratives related to it. They targeted victims across the EU under the guise of supporting Ukraine or Ukrainians. Fake webpages were created to solicit money, using URLs that included misleading key words. Emails pretending to raise funds for the humanitarian effort were sent from fraudulent addresses. In some cases, fraudsters impersonated celebrities that led or supported real campaigns or spoofed the humanitarian organisations' domains, inviting victims to donate in cryptocurrencies"

*Europol Internet Organised Crime Threat Assessment, 2023*

# "Bad AI"[6]

It is impossible to escape the fact that developments in Artificial Intelligence are leaping forward at an incredible pace, due to concerted efforts by technology companies to gain first-mover advantages and market share. All of the major technology companies are heavily invested, with new businesses starting-up every single day. Alongside this, governments all over the world are seeking to establish their countries as global and regional leaders in the field. OpenAI's ChatGPT has become the "poster child" of these developments, gripping public imagination since the launch of GPT-4 in March 2023. ChatGPT, which stands for "Chat Generative Pre-Trained Transformer", is a "Large Language Model" chatbot, which allows users to generate all kinds of content—artistic works, academic research, journalistic materials, legal documents, and even computer code. It is understood to be the fastest growing consumer software application ever. Not surprisingly, it has spurred the speedy development of competing applications, as ChatGPT's competitors do not want to fall too far behind.

In addition to providing boundless opportunities for legitimate use, AI has corresponding potential for illegitimate pursuits. Sadly, although inevitably, AI can and is being used for bad. Indeed, for bad actors, AI is the stuff of dreams. The context in which this needs to be viewed is the way that technologies have always enabled cybercrime to scale and industrialise. Unfortunately, each leap forward in technology has paid massive dividends to criminals. The Internet has enabled crime to be conducted remotely from anywhere in the world, whereas traditional crime generally required the attacker and victim to be in close physical proximity to one another. It has also distanced the criminal from law enforcement, whereas before they could be in the same jurisdiction. Technologies like The Onion Router (Tor), VPNs, Virtual Machines, and End-2-End Encryption have enabled criminals to mask their identities. All of these factors lessen the risk of detection and apprehension. Cryptocurrency has enabled large amounts of money to be laundered with considerable reduction of risk to cybercriminals, where previously they might have been reliant on Money Mules handling small volumes of cash. Dark Web marketplaces have enabled illicit content, goods, and services to be traded with ease, whereas previously things might have been handled in dark alleyways, car parks, and remote meeting points. Increased online connectivity, adoption of smartphones, and the expansion of the Internet of Things has exposed more people to criminal activity. With every step forward in the progression of technological development, the criminal's job has become easier, the risks lowered, and the rewards increased. AI, as the latest big leap forward, will add rocket fuel to the growth and development of cybercrime.

In addition to providing boundless opportunities for legitimate use, AI has corresponding potential for illegitimate pursuits.

[6] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/the-biggest-ai-moment-ever-for-cybercrime-just-happened
https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/
https://www.esecurityplanet.com/threats/wormgpt-chatgpt-ai-hacking/

Bad actors' use of AI has already been observed in cybercrime and many law enforcement agencies, cybersecurity authorities, and technology experts have issued warnings and alerts to this effect. For example, Europol and others have recently drawn attention to the risk that AI might be used to develop or refine malware and SQL injection attacks; to assess vulnerabilities of targets' networks; and to assist with password guessing and brute-force attacks. Europol is also concerned about AI being used in social engineering attacks, for example to design ever-more convincing phishing emails, which can bypass technological and human filters. Other leading security commentators have drawn attention to WormGPT, which is being advertised on the Dark Web as the cybercriminal's alternative to ChatGPT[8].

Therefore, all of the email-enabled and email-targeting cybercrimes discussed above are likely to amplify in sophistication, severity, and scale by cybercriminals' use of AI.

Organisations need to be able to defend themselves against AI-enabled cyberattacks. Fortunately, it is not all one way and it will therefore come as a relief that AI is also being deployed to guard against cyberattacks by technology vendors like Abnormal Security that utilise AI to protect their customers against malicious emails and email-like communications.

Email-enabled and email-targeting cybercrimes are likely to amplify in sophistication, severity, and scale, with the malicious use of AI.

[7] https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence
[8] https://krebsonsecurity.com/2023/08/meet-the-brains-behind-the-malware-friendly-ai-chat-service-wormgpt/

# Legal Dimensions of Email Use

## Key Security-Focused Legislation Relevant to Email

Security-focused legislation that affects the use of email and email-like communications includes:

### 1. Computer Misuse Act 1990

The CMA criminalises unlawful access to computer material, unauthorised access with intent to commit or facilitate commission of further offences; unauthorised acts that impair the operation of computers, programs or data; unauthorised acts causing or creating risk of serious damage; and making, supplying or obtaining articles for use in the above offences. If email is used as part of a hacking attack, such as by propagating malware, or email is the target of such an attack, offences under the CMA will be committed.

When we consider email-related threats and risks through a legal lens, we observe a range of duties for business resilience and security, which includes the protection of assets and people. Key components of the relevant legal framework are as follows:

- Various listed businesses are subject to the UK Corporate Governance Code[9], while some private businesses are subject to the Wates Principles. Central to both of these frameworks is the need to ensure appropriate risk management, which involves the adoption of systems of internal control. The purpose of risk management and systems of internal control is to identify and manage the risks that the business is facing, to ensure ongoing business success and the accuracy of financial and related reporting. Plainly, the principles within these frameworks extend to managing email-related threats and risks.
- Sectoral obligations within regulations. Many sectors of the economy are subject to their own specific and targeted schemes of legislation and regulation, which are intended to add resilience and to protect interested parties, such as consumers. Thus, for example, rules within the financial services sector, the telecommunications sector and within utilities and regulated markets extend to the management of email-related threats and risks.
- Legislation has been adopted for the purposes of managing cybersecurity risks in critical infrastructure and services, which extends to some online platforms. The UK NIS Regulations 2018 and the EU Second NIS Directive apply in these situations. Where cybersecurity risks can arise with email, these regulations will apply.
- The General Data Protection Regulation (GDPR) applies in the UK and across the EU. Other countries and regions around the world have adopted similar legislation. The purpose of the GDPR is to achieve a high level of protection for personal data that is undergoing processing. These objectives are addressed by the Data Protection Principles, one of which deals with integrity and confidentiality issues, which is supplemented by additional rules on the security of personal data undergoing processing and rules that require the reporting and communication of Personal Data Breaches in certain circumstances. Again, these rules will encompass email-related threats and risks to personal data and data processing systems.

[9] https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf

## 2. General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018

These laws protect personal data, including personal data contained in emails. Controllers of personal data are under a duty to ensure security of these data, which includes protecting them from email-based attacks, such as ones that use email to propagate malware or that phish data or access credentials to computer systems. If an attacker uses email as part of an attack, to obtain personal data, they will commit an offence.

## 3. NIS Regulations 2018

The purpose of NIS is to ensure the security of critical infrastructure and digital services, so that they are protected against cyberattacks. The operators of these services are legally required to ensure this protection, which extends to cyberattacks that utilise email.

- Private law obligations for resilience, security, and the protection of assets and people can be created in contractual situations, which may stand alongside other rules in legislation and regulations, or as standalone duties. Nowadays, it can be expected that businesses will adopt contractual terms and conditions to require the taking of operational steps and measures by their contracting partners and suppliers to guard against risks to the objectives set out in the preceding bullets. Terms and conditions might expressly refer to email-related risks, or the coverage of email might be implied by operation of law, where that is needed for business efficacy purposes.
- Similarly, private law arrangements can be contained in overarching schemes that apply to particular sectors of the economy or particular business activities, with impacts for email-related threats and risks. A prominent example is the Payment Card Industry Data Security Standard (PCI DSS) scheme, which seeks to protect the cardholder data environment through the application of rules for business resilience and security.
- The regulated professions usually operate under codes of conduct or similar schemes that can capture requirements for resilience and security. For example, the maintenance of client confidentiality is a key objective for professions such as medicine, accountancy, and law. Email-related threats and risks obviously engage with these concepts and requirements.

Therefore, as a guiding principle, wherever an organisation is subject to legal requirements for business resilience, security, and the protection of assets and people, it can be anticipated that various legal duties will exist, which will apply to email-related threats and risks. Where such obligations exist, this will necessarily mean that organisations will need to perform risk assessments, to understand both the nature of the risk that can be presented by email and email-like communications and the nature of the technical and organisational measures – i.e., controls and countermeasures – that can be adopted to manage those risks at an acceptable level.

Conversely, due to the twinning effect of operational and legal security, wherever an organisation is operationally focused on email-related threats and risks, it will be likely that a corresponding legal duty to manage those risks will exist, which might be found within the areas of law identified above or elsewhere.

# People and Well-Being

An area of rapidly growing concern in the economy is people and well-being. This can be expressed in many ways, such as the ESG agenda, or as matters of business purpose and ethics. The ESG agenda, which stands for Environmental, Social and Corporate Governance, provides a set of modern criteria to aid the development of investment strategies, with the Social criteria encompassing how people are treated in the workplace. These areas have many related legal dimensions, for example the law of industrial relations, employment law and equality law.

If we consider email-related threats and risks from the people and wellbeing perspective, many issues stand out as matters of practical and substantial concern. For example:

- If a business is subject to a BEC attack, or another cybercrime that involves social engineering of people through activities such as phishing, what will be the impacts on the employee who has been targeted? These may range from the person suffering anxiety and distress due to being victimised, to them being caught up in stressful incident management and response procedures, to them being potentially put under suspicion and perhaps disciplinary processes.
- Similarly, if the attack is successful due to a failure of security risk management, the operational team responsible for preventative security may suffer similar effects to those felt by the employee in the previous example.
- If the attack is highly disruptive, the incident management and response team might be put under immense and prolonged pressure that endures for a substantial period. These impacts might be amplified in particular security situations, such as a ransomware attack that is ongoing past the point of detection and requires engagement with people and actors that take the responders out of their comfort zone, such as dealing with the threat actor, or with law enforcement, or with the legal community.

In this rapidly developing era of people and well-being concern, risk management frameworks might need to be adjusted to consider not just the operational impact on business of email-related threats and risk, but also the people and well-being impacts. This may be necessary not just to give effect to ESG, business purpose, and ethics duties and obligations, but because there might also be concrete corresponding legal obligations in play. The extent and boundaries of the employer's duty of care to protect their workers from email-related threats and risks is yet to be fully established, but it is conceivable that some cyberattacks will result in impacts that bring into question whether the employer has satisfied and discharged their duty of care owed to the employee.

This provides a further reason for organisations to ensure that they have adopted appropriate risk management and controls frameworks to protect against email-related threats.

In this rapidly developing era of people and well-being concern, risk management frameworks might need to be adjusted to consider not just the operational impact on business of email-related threats and risk, but also the people and well-being impacts.

# Data Protection and Cybersecurity Law Under the Microscope

The principal pieces of legislation are the GDPR and the Network and Information Security legislation (NIS).

These areas of the law provide us with a substantial basis for properly understanding the twinning of the law and operational security, which in turn enables us to understand the true nature of legal duties as they pertain to managing and controlling email-related threats and risks. The principal pieces of legislation are the GDPR and the Network and Information Security legislation (NIS). Both areas of law are of EU origin. The EU adopted the GDPR and the NIS Directive in 2016. The GDPR automatically applied in the UK and was supplemented by the Data Protection Act 2018, whereas the UK gave effect to the NIS Directive through the NIS Regulations 2018. Despite Brexit, both laws still apply in the UK. The EU adopted the Second NIS Directive in 2022, to expand the scope of its coverage, but NIS 2 does not apply in the UK, albeit it is open to the UK Government to amend the 2018 Regulations, to re-align the UK with the EU, if it so wishes.

## The GDPR

The GDPR is concerned with the processing of personal data by Controllers and Processors. Processing refers to actions performed on personal data both automatically, i.e., by computers, network and information systems and other automated systems (e.g., CCTV), and manually in certain circumstances. It covers the whole information lifecycle, from the initial collection of personal data right through to its final deletion and destruction, whether or not this is done by the Controller itself, or by a Processor on the Controller's behalf. The difference between a Controller and Processor lies in the fact that the Controller decides or determines the purpose and means of processing, whereas the Processor acts only on the Controller's instructions. For example, an organisation that provides data processing services to a Controller, such as Cloud Service provider or a data centre or an application provider, will be classified as a Processor. The person whose personal data is processed is known as the Data Subject. Therefore, the Data Subject is the beneficiary of the protections provided by the GDPR, whereas the regulated parties are the Controller and Processor and the regulated activity is data processing.

## The Security Duties of Operators of Essential Services (OES)

(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.

(2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

(3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

*NIS Regulations 2018, para 10*

Personal data is information that relates to an identified or identifiable living individual. This covers direct identifiers, such as a person's name and indirect identifiers such as their date of birth, address, biometrics and information generated by or related to their use of processing equipment and third party services, such as the use of online services, public services, business and retail services,services provided by clubs, membership organisations, charities, and religious institutions.

The processing of personal data is governed by a series of Data Protection Principles. These provide the architectural structure and backbone of data protection law and set requirements such as that processing should be fair, lawful, and transparent and processed in a manner that ensures appropriate security of the personal data.

The principle concerning the security of personal data undergoing processing is known as the integrity and confidentiality principle, which mirrors a critical concept within operational security, namely The CIA Triad. The idea within The CIA Triad is that information assets, including computers, networks and information, need to ensure confidentiality, integrity and availability. The fact that the security principle omits a reference to availability is immaterial, as the protections that the principle requires implicitly mean that personal data should be secured so that it is available to authorised persons when required.

The security principle is augmented by additional rules in Article 32 of the GDPR, titled Security of Processing, the details of which are set out in the call-out box. Observant readers will notice the following elements in Article 32:

- Controllers and Processors shall implement appropriate technical and organisational measures for the security of personal data.
- These measures shall be appropriate to the risk.
- The risk assessment should have regard to the state of the art, the costs of implementing the measures, the nature, scope and context of processing, and the risks to the rights and freedoms of natural persons (i.e., the people whose personal data are to be secured).
- An indicative but non-exhaustive range of potential measures are identified.

Translating these requirements into core questions, A.32 requires the Controller and Processor to address these issues:

- Insofar as email-related threats and risks are concerned, how are they identified, how should they be classified, and how can they affect personal data and the people whose data are processed?
- What falls within the state of the art for dealing with these risks?
- What are the full range of technical and organisational measures that should be adopted for risk management, seeing that only an indicative, non-exhaustive list of measures is provided?

When these questions are considered in light of the legal duty, the conundrum is obvious: while the law sets the duty, it does not provide the answer to how the duty is to be addressed. Therefore, the law requires the organisation to look elsewhere for the answers. There is only one place where the answers can be found, which is within operational security. Only operational security knows what the email-related threats and risks are within any given organisation, what the state of the art for security looks like and what controls are appropriate to address the threats and risks, hence why legal and operational security are twinned. This twinning always arises wherever there is a legal duty for security. The law itself can never presume to know what is operationally required to deal with operational security risks. That is why the law uses phrases such as "appropriate technical and organisational measures", rather than providing highly prescriptive lists of specific controls requirements.

## The NIS Regulations – Protecting Network and Information Systems

The NIS Regulations in the UK apply to operators of essential services in the energy sector (electricity, oil and gas), transport (air, rail, water and road), health (hospitals, clinics and other health care settings), drinking water supply and distribution, digital infrastructure (Top Level Domain Name Registries, the Domain Name Service and internet exchange points), and to relevant digital service providers (namely online marketplaces, online search engines and cloud computing services). Sometimes called "The Cybersecurity Regulations", NIS regulates critical infrastructures and services.

The law itself can never presume to know what is operationally required to deal with operational security risks.

The basic duty for cybersecurity for operators of essential services is threefold to (1) manage the risks posed to the security of the network and information systems on which their essential services rely, to (2) prevent and minimise the impact of incidents affecting those systems and to (3) ensure a level of security for those systems that is risk-appropriate, having regard to the state of the art. The duties placed on relevant digital service providers are broadly the same, although they are also directed to take account of compliance with international standards.

Essentially, the duties in NIS are aligned with those in the GDPR, raising the same questions and conundrums.

# Impacts of Legal Non-Compliance

Where there is a failure of operational security that constitutes a failure of security law, the impacts can be considerable.

For example, the GDPR contains regulatory enforcement mechanisms that can be deployed by the data protection regulator, as well as rights to judicial remedies for the impacted Data Subjects and rights for them to otherwise intervene in the Controller's operations. The regulatory enforcement mechanisms include a power to impose fines of up to 4% of annual worldwide turnover[10] and powers to intervene in, modify, or stop data processing activities. The investigative processes that precede the taking of formal enforcement action can be highly disruptive to the organisation under investigation because the regulator can undertake audits, inspections and demand the delivery of information. Where a person suffers damage or distress because of non-compliance, they can pursue compensation claims before the courts, including as part of class actions[11]. At any time in their relationship with the Controller, a Data Subject can also exercise their other statutory rights, such as their right of access to data (sometimes called a "DSAR"): these rights are commonly used after a security breach.

**£17,000,000**
**Maximum fine for non-compliance with NIS Regulations.**

Regulatory action for contravention of the NIS Regulations covers the same ground, with the maximum fine being £17,000,000.

The EU versions of these laws contain equivalent provisions, although more sectors and organisations are regulated under the latest version of the NIS Directive in the EU in comparison to the position in the UK.

It would be correct to observe that exposure to regulatory action and litigation under the above legislation depends upon the regulator and people affected becoming aware of a security breach. Many breaches are instantly transparent to these persons, due to the observable, public impacts, but this is not always the case. The GDPR and NIS address this potential, as they both contain breach notification rules that mean that incidents at a particular level of severity need to be reported to the regulator. The GDPR also requires serious personal data breaches to be communicated to the impacted persons. Thus, the law contains in-built mechanisms to make security breaches transparent in situations where they might otherwise be concealed from view.

[10] The basis of calculation depends upon the article of the GDPR that has been contravened as well as factors such as whether the organisation that is being fined is part of a group of companies, in which case the annual worldwide turnover that is considered is that of the group as a whole, rather than the individual company's.
[11] This is a colloquialism for group litigation or representative actions.

Where a security breach engages another regulatory scheme, such as those applying to financial services, telecommunications and to the regulated professions, the regulatory body will be able to take the enforcement actions and apply the sanctions that are set by the law in question. These can span everything from the setting of new licence conditions, to the imposition of fines.

In a commercial situation, a security breach can have a variety of legal impacts. For example, there might be exposure to contractual damages claims or similar contractual remedies. If a scheme such as PCI DSS applies, a scheme member might be excluded from operating within it, with consequential business interruption, or be exposed to fines: PCI DSS provides a set of security requirements that certain acquiring banks and merchants need to adhere to, to be able handle credit card payments for major card brands such as Visa, MasterCard, and American Express.

Businesses might also be prevented from engaging in bids for commercial contracts, or be disadvantaged in such bids, due to having a poor history of insecurity, for example in competitive tender schemes run by government and public authorities that utilise scoring mechanisms that measure security and resilience issues. Security breaches can also damage an organisation's brand and reputation, which might render it toxic to others, resulting in it being disenfranchised from entering into legal relationships with others.

If we consider fraud issues, businesses might have insurance cover to recover their losses. There are also banking and related compensation schemes that can provide similar cover. Recovery of losses under these schemes is not unconditional. Generally, they require the defrauded party to have taken steps to protect themselves. Therefore, where a person or organisation falls victim to an email-related fraud, the quality of the controls that they put in place to protect themselves may become an issue within the compensation claim. This is often the case in insurance situations.

These examples are just a snapshot of the range of potential legal impacts that can arise from a security breach. Email-related security breaches can put the victim organisation in breach of its legal duties for security, thereby exposing it to legal risk, or they can have an effect on brand and reputation that causes consequential legal effects.

Email-related security breaches can put the victim organisation in breach of its legal duties for security, thereby exposing it to legal risk.

# The Consensus of Expert Opinion: How the Law Will Determine the Details for Operational Security

The analysis in this white paper has established that security operations and security law are twinned, so that the detail of the legal duty for security is found within security operations themselves. However, the range, number, and combination of steps and measures that can be taken for operational security are potentially boundless, so the real answer is found at a different level of abstraction, i.e., within the consensus of expert opinion for operational security. This observation requires us to understand how the law deals with matters of technical detail when they are unclear and in dispute.

A suitable comparison for the world of operational security is that of professions, as they are both areas where technical expertise matters.

## Why the ISO 27000 Family of Standards is the Location of the Consensus of Expert Opinion

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1/SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management system (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information."

*ISO/IEC 27000:2018, Clause 0.1*

Sometimes, the problem is so entrenched and intractable that it has to be resolved in court.

For example, consider the situations of medicine, accountancy, or law. From time to time, things will go wrong in the delivery of these services. When this happens, we might be concerned with a situation of professional negligence. Sometimes, the problem is so entrenched and intractable that it has to be resolved in court. If the case was about alleged clinical negligence, arising from surgery that went wrong, the judge will not be able to determine by themselves whether the surgery was or was not performed at a sub-standard level, i.e., negligent, because the judge is a lawyer, not a medical expert. Instead, the case will be decided with the assistance of expert evidence, provided on behalf of the surgeon and the patient. The expert witnesses will also be surgeons and qualified to provide their opinions on the quality of the surgeon's work and whether it was performed in-line with expected standards. In other words, the legal issue of the surgeon's alleged professional negligence will be resolved by the consensus of professional opinion on acceptable practice for operations of the kind in question. If the surgeon's approach falls within the range of acceptable operational approaches as understood and agreed by the consensus of professionals, they will not be guilty of negligence despite the fact that the surgery went wrong. Sometimes things will go wrong with very unfortunate consequences despite the surgeon adhering to agreed standards. The same is true of accountancy and law and for others areas involving professional and highly technical skill, such as engineering.

Operational security needs to be looked at in exactly the same way. Like medicine, accountancy, law, and engineering, determining the requirements of operational security in any given set of circumstances requires the application of professional and technical skills. Therefore, the question of what needs to be done to satisfy legal duties as they pertain to email-related threats and risks will be found within the consensus of expert opinion for operational security.

# Where to Find the Consensus of Professional Opinion for Operational Security

So, where is the consensus of professional opinion for operational security found? Plainly, businesses and organisations up and down the land employ their own security experts, with a variety of titles and labels attached. However, they do not represent the consensus of expert opinion as such. Instead, as security experts, they should operate in accordance with the consensus of expert opinion. The principal location for the consensus of expert opinion are standards that are published by recognised standards-making bodies. In the area of information and cybersecurity, the most universally acclaimed body of international standards is the ISO/IEC 27000 family of standards that are developed and published jointly by the International Organisation for Standardisation ("ISO") and the International Electrotechnical Commission ("IEC"), which are both headquartered in Switzerland. To understand the significance of these bodies, it is worth considering their membership. ISO's members consist of most of the world's national standards bodies. A map of the world on ISO's website shows its immense geographical coverage[12]. The IEC's geographical reach is also impressive, made up of full member states[13] and affiliate countries[14]. It is impossible to be involved in operational security and not to come across the 27000 family and be influenced by it.

Central to the security processes that these standards prefer is the idea of an Information Security Management System. Key components with an ISMS are requirements for risk management and continual improvement.

The approach to risk management is amplified by ISO/IEC 27005:2022, which requires a context-driven approach to risk assessment and risk treatment. In summary, the organisation needs to:

- Understand its internal and external context (which includes its technology and data landscape, the threats and risks that it faces and its legal obligations).
- Set its risk identification, acceptance and assessment criteria.
- Perform its risk assessment aligned to those criteria.
- Develop its risk treatment plan based on a comparison of its assessed risks and the risk acceptance criteria.

[12] https://www.iso.org/members.html
[13] https://www.iec.ch/national-committees#nclist
[14] https://www.iec.ch/dyn/www/f?p=103:9:0

When risks are deemed unacceptable, it will have three treatment options; (1) stop performing the risk activity (i.e., terminate the risk), (2) modify the risk (i.e., treat the risk), or (3) seek to share it with a third party (i.e., transfer the risk). Risk modification is achieved through the application of controls. The controls library in ISO/IEC 27002:2022 places these controls in four categories, i.e., organisation controls, people controls, technological controls and physical controls.

Understanding context - or "context establishment", as it is called within the standard - is pivotal to understanding how everything fits together. If the context changes to a material extent, the risk assessment and risk treatment process will need to be revised, to ensure that the treatment plan remains relevant and up to date. This means that risk management needs to respond not only to changes in the threat landscape, but also to changes in the state of the art for protective security and controlling risks, which can include technological developments by security companies like Abnormal Security. As such, operational risk management is an ongoing process of iterative reviews and changes, to ensure that the security controls framework (i.e., the "appropriate technical and organisational measures", to use the GDPR's language) is always relevant and optimised. This is why the idea of continual improvement is central to an ISMS.

## Shifting Risks - The Consensus Requires Controls to Be Kept Under Review

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

As information security risks and the effectiveness of controls change depending on shifting circumstances, organizations need to:

a) monitor and evaluate the effectiveness of implemented controls and procedures;

b) identify emerging risks to be treated; and

c) select, implement and improve appropriate controls as needed.

To interrelate and coordinate such information security activities, each organization needs to establish its policy and objectives for information security and achieve those objectives effectively by using a management system

*ISO/IEC 27000:2018, Clause 4.1*

For example, Clause 10.5 of ISO/IEC 27005:2022, says that "*the organisation's monitoring process should encompass all aspects of the risk assessment and risk treatment processes for the purposes of ... ensuring that the risk treatments are effective, efficient and economical in both design and operation ...*". This means that controls to address email-related threats and risks need to be kept under review. The principle of economy in design and operation is particularly interesting: it encompasses the idea that new technologies can be more economical in the sense that they can automate steps that are otherwise dealt with manually. For example, traditional email technological controls may leave a suspect email present within an email inbox, leaving the decision to the inbox owner as to what to do with it, which means that latent risks are embedded in the system. If a new technology can remove the human steps and components, to automatically terminate the latent risk, the new technology would be more economical in design and operation in comparison to the traditional technology.

Clause 10.5.2 expands upon this by saying:

"*Factors that affect the likelihood of the occurrence of threats and their corresponding consequences can change, as can factors that affect the suitability or cost of the various treatment options. Major changes affecting the organisation should be reason for a more specific review. The risk monitoring activities should be regularly repeated and the selected options for risk treatment should be reviewed periodically.*"

Likewise, Clause 10.8 goes on to say:

"*Ongoing monitoring and review that the context, the outcome of the risk assessment and risk treatment, as well as management plans, remain relevant and appropriate to the circumstances is necessary to ensure that the information security risk management process is correct.*"

When we place, for example, legislation such as the GDPR side-by-side with the standards for best practice as represented by the ISO/IEC 27000 family, it becomes all the more obvious why GDPR A.32 refers to context, risks of varying likelihood, the state of the art and appropriate technical and organisational measures. The legislation is mirroring and adopting the approach within the consensus of expert option for operational security. All sensible lawmakers, judges, and lawyers will defer to the consensus of expert opinion on complex and technical operational matters when seeking to describe related legal requirements.

All sensible lawmakers, judges, and lawyers will defer to the consensus of expert opinion on complex and technical operational matters when seeking to describe related legal requirements.

# Conclusions on Operational and Legal Impacts for Email-Related Threats and Risks

Email-enabled threats and risks are becoming AI-enabled and this progression has a one-way trajectory.

Email and email-like communications are central to societal and business activities and so it is imperative that organisations manage their email-related threats and risks for operational and legal purposes. Where a legal duty for security arises, such as for the resilience and security of the organisation, or to protect information assets, or to protect people and their wellbeing, or to protect other organisations, the steps that need to be taken will be found within the consensus of expert opinion for management and control of these threats and risks.

The consensus of expert opinion makes it clear that a risk-based approach to the management of email and email-like communications must have regard to both the internal and external context of the organisation and the state of the art. This means that risk management must be an ongoing, dynamic, and active process that keeps track of the changing threat landscape and the state of technological development, both in terms of the development of threats and the development of technological controls and countermeasures to guard against these threats and to reduce their impacts.

Key characteristics of the threat landscape include the fact that bad actors such as cybercriminals are innovative, entrepreneurial, opportunistic, and agile and that they have consistently taken advantage of legitimate technological developments for illegitimate purposes. This has enabled attackers to scale their threats to industrial levels. Inevitably, the latest step in that journey of misuse of technology for deviant purposes is the misuse of AI, which law enforcement agencies, security researchers, technology companies, and academics all over the world are now warning about. This means that email-enabled threats and risks are becoming AI-enabled and this progression has a one-way trajectory.

It follows that as part of a dynamic risk management process for email and email-like communications, organisations should consider the state of the art in AI-enabled email security systems. As such, this requirement is embedded into the law.

# "Good AI"

Traditional email security technologies are proving inadequate in protecting contemporary enterprises from increasingly advanced attackers. These features are no longer sufficient in safeguarding organizations. The traditional approach taken by email security technologies involves a range of features that limit its effectiveness.

For example, traditional methods like secure email gateways (SEGs) are based on the implementation of static rules for filtering purposes, such as safe and block lists of IP addresses and email addresses that permits or block email traffic based on known addresses and identities. This approach lacks agility and dynamism, and threat actors can contrive attacks to overcome these filters. For example, if a bad actor compromises a safe listed IP address or email address, the filters will allow their traffic, leaving the victim exposed.

Another filtering approach applies to malware embedded in email content, or hyperlinked by content. These filters may rely on anti-virus signatures that are outdated. Moreover, they are based on filtering out known threats and risks, rather than unknown ones. Again, due to the innovative and entrepreneurial characteristics of certain threat actors, the attacker can also overcome these filters. This allows for the phenomenon of Zero-Day attacks, which exploit previously unknown vulnerabilities. An optimised approach to security will not be limited to dealing with known threats and risks, because cyber-attackers purposefully and systematically take advantage of the target being blind to their full range of vulnerabilities. An optimal approach should also address unknown threats and risks.

Similarly, traditional technologies might limit their coverage to discrete sections or areas of the technology estate, meaning that the protection they provide is not fully comprehensive. However, our communications systems are becoming increasingly integrated and connected across a range of applications, both on-premise and in the Cloud. A more holistic and optimised approach would provide protection across the integrated estate and across any platforms and applications that can be misused like email and email-like communications that may need to be protected to the same level as email itself. Many cyber-attackers take a wholly rational approach to their attacks, to take advantage of the non-protected areas. Ideally, protection against malicious communications should be integrated across platforms and applications, both on premise and in the Cloud.

Threats can also arise internally, by rogue insiders. Some traditional email security technologies are concerned only with inbound communications, leaving internal traffic and outbound traffic unprotected.

Some technologies might identify potential risks, but they do not provide a complete solution, as they can leave the ultimate decision about eradication and deletion to the end user. This means that malicious communications may be stored, with the risk that a future an action might be taken on them. Another part of the problem in this situation is that the protection that is offered rests on the end user acting rationally and making the best decision, which means that the protection builds on a fallacy, because human beings do not always behave rationally. Instead, we suffer from bounded or limited rationality, due to a range of factors such as our tendency to act upon cognitive biases or heuristics.

Email security technologies that are AI-enabled and operate in a more integrated way across platforms and apps, such as those offered by Abnormal Security, take a different approach to the problem domain. Rather than relying on basic, narrow filters, or on end users making the right decision on every occasion, they utilise behavioural AI to build a much stronger and comprehensive understanding of behaviours of users of email and email-like communications, to provide a deeper insight into threats. This application of behavioural AI means that the technology can analyse and understand behaviours not just of potential external threat actors, but also internal threat actors. Additionally, the behavioural AI can analyse both good behaviours and bad behaviours. By extension, this means that the focus of security is not just known threats and risks, but also previously unknown or undiscovered ones. All of these insights can then be leveraged collectively, to provide enhanced protection and security, to include the automatic eradication and elimination of communications that present threats and risks, rather than leaving it to the end user to make the final determination and decision and without leaving the threat festering in the system.

# Recommendations

1. Organisations should ensure that their risk management frameworks for identifying, assessing, and treating email-related threats and risk are adaptive, comprehensive, and fit for purpose.
2. An organisations' risk management processes should consider the state of the art as it relates to the controls frameworks that they deploy for treating email-related threats and risks.
3. Organisations should consider the state of technological development, both in terms of how technologies are and can be leveraged in cyber-attacks and how they are and can be used to provide protection.
4. Organisations should consider how AI can be used both for good and for bad.
5. Organisations should ensure that they have adopted an appropriate risk management framework for email-related threats and risks, which should have regard to the consensus of professional opinion on operational security.
6. Organisations should adopt the use of AI-enabled technologies for managing email-related threats and risks as part of compliance with relevant laws.

# About Stewart Room

Stewart Room is the Global Cyber Security and Data Protection Leader at DWF Law LLP and the Global Technology Sector Leader. With over 30 years' experience in professional services, as a Barrister, Solicitor and Management Consultant, he is recognised by the legal directories as one of the UK's leading data protection and cyber security lawyers and has acted in many landmark cases. He has authored and contributed to nine influential textbooks on information law, including writing the UK's first law books on security law and on email law. He is a member of the European Data Protection Board's expert support pool for legal and technology matters; the President of the National Association of Data Protection Lawyers; a co-founder of The Cyber Security Challenge UK; and a past winner of the Financial Times Legal Innovator of the Year award.

# About DWF

DWF is a leading global provider of integrated legal and business services. Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients. We deliver integrated services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our eight key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

## Disclaimer

This document is prepared for information purposes only and it is not intended to constitute legal advice on specific legal issues. Neither Abnormal Security nor DWF accept any responsibility for reliance on the information in this document. If you need legal advice, please consult a suitably qualified lawyer.

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

More information is available at abnormalsecurity.com

## Interested in Protecting Your Email from the Full Spectrum of Attacks?

Request a Demo → See Your ROI →