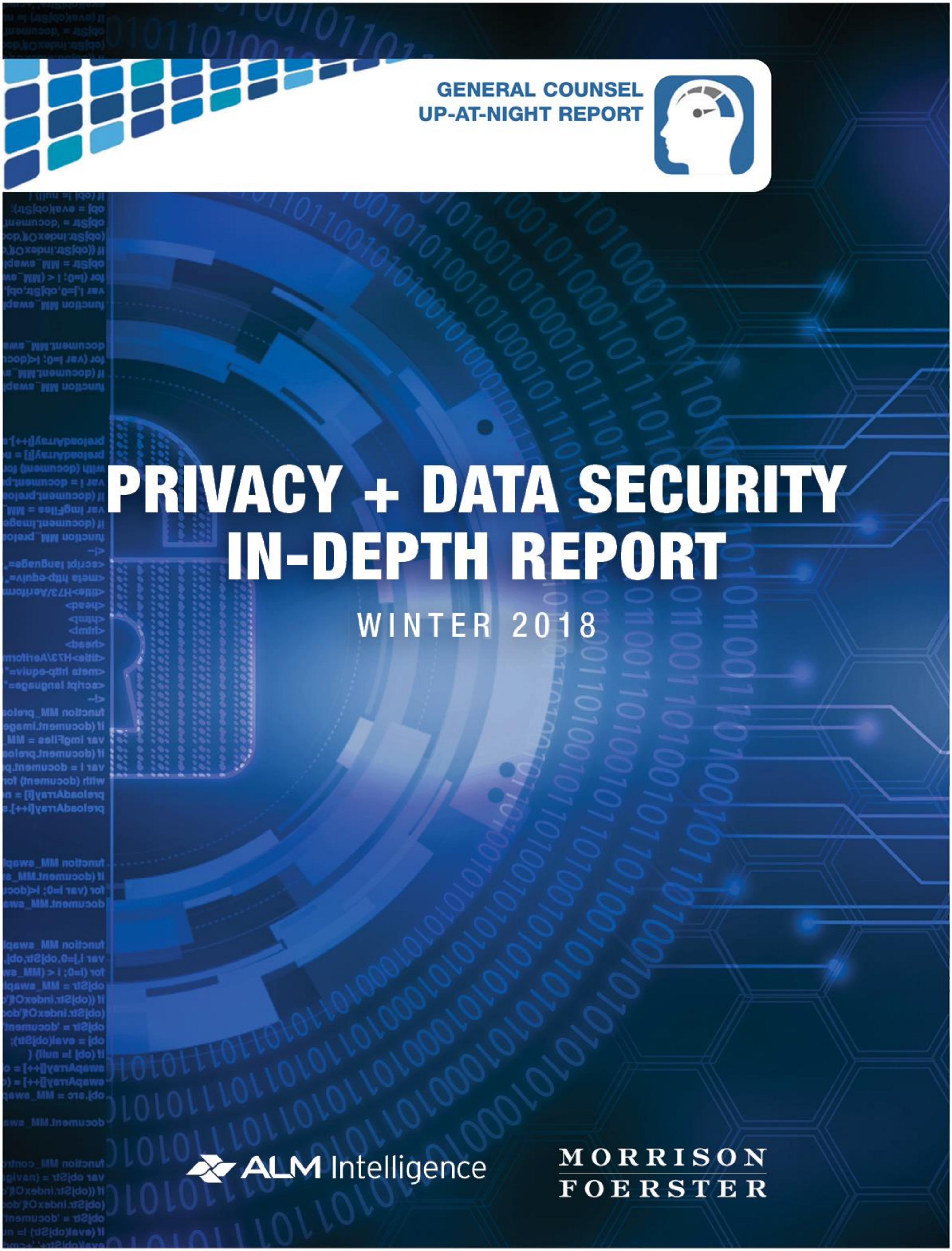

GENERAL COUNSEL
UP-AT-NIGHT REPORT

PRIVACY + DATA SECURITY IN-DEPTH REPORT

WINTER 2018

ALM Intelligence

MORRISON
FOERSTER

INSIDE

A MESSAGE FROM MORRISON & FOERSTER'S GLOBAL PRIVACY & DATA SECURITY CO-CHAIR

Last spring, Morrison & Foerster partnered with ALM Intelligence to develop the *General Counsel Up-at-Night Report*, providing a unique glimpse into the myriad challenges that legal departments – across industries and in companies large and small – juggle every day. We are happy to be able to share an updated iteration of our inaugural report that identifies emerging issues gaining momentum with in-house legal departments today.

According to the survey, issues related to privacy and data security continue to be among the top concerns of in-house legal departments, particularly with the rapid approach of the May 2018 deadline to comply with the European Union General Data Protection Regulation (GDPR). With possible penalties of up to €20 million or 4% of global annual revenue for non-compliance, companies cannot afford to turn a blind eye, particularly because the regulation is so broad, applying to companies that collect, use, or otherwise process personal information of individuals in Europe, regardless of whether the company has a physical presence in Europe.

Cybersecurity issues also continue to be a main area of concern as in-house legal departments face increasing pressure to report cybersecurity incidents and cyber incident response plans to their board of directors.

A deeper dive revealed more subtle variations in several of the key issues identified in the inaugural report, including:

- More respondents are reporting the presence of a chief privacy officer within their company.
- There is a significant variation in how organizations approach privacy training: 44% of respondents indicated that they provide workforce privacy training annually, while one-third of respondents (36%) indicated they do not provide any privacy training to their workforce and 20% reported providing training on an ad-hoc basis.
- A vast majority of respondents (65%) indicated that they have a cyber incident response plan in place. In spite of this, nearly one-quarter of respondents (23%) admitted that they have never participated in a cyber incident tabletop exercise, and only 5% of respondent organizations said that they test their cyber incident response plans on a quarterly basis.
- The latest findings reflect an increase in using consent as the preferred mechanism to move personal information globally.

With issues related to the GDPR looming and as cybersecurity incidents continue to impact businesses on a global scale, the best way in-house legal departments can protect their business is by being proactive and being prepared. We hope you find value in these and the other findings contained in this report and that they translate to actionable steps for your organization.

If you have any questions or if we can assist with any of these issues, please do not hesitate to contact me.

Best regards,

Miriam Wugmeister
Co-Chair, Global Privacy & Data Security
Morrison & Foerster
mwugmeister@mofo.com

INTRODUCTION

In spring 2017, ALM Intelligence and Morrison & Foerster conducted an online survey of 200 U.S.-based general counsel and in-house lawyers to gain a better understanding of the demand for legal services, law departmental operational and sourcing strategies, and the approaches taken by law departments in confronting five issues consistently raised in our ongoing conversations with general counsel:

- Privacy and Data Security
- Risk and Crisis Management
- Regulation and Enforcement
- Litigation
- Intellectual Property

The inaugural survey identified privacy and data security as new areas of concern among law department leaders. In our latest survey, privacy and data security remain top areas of concern for legal departments with 63% of respondents describing privacy and data security as very important challenges (Figure 1).

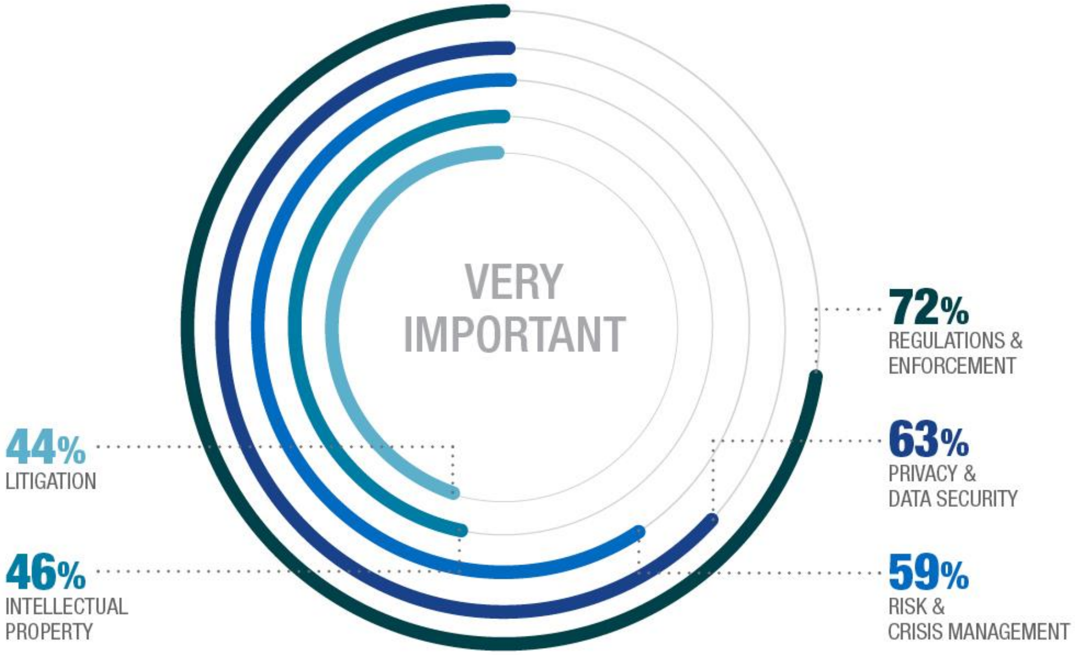

Figure 1
Most Significant Challenges Facing Law Departments

Respondents in the latest report overwhelmingly identified phishing/malware as the greatest area of concern (74%), followed closely by hacking (70%) and compliance obligations (68%) (Figure 2).

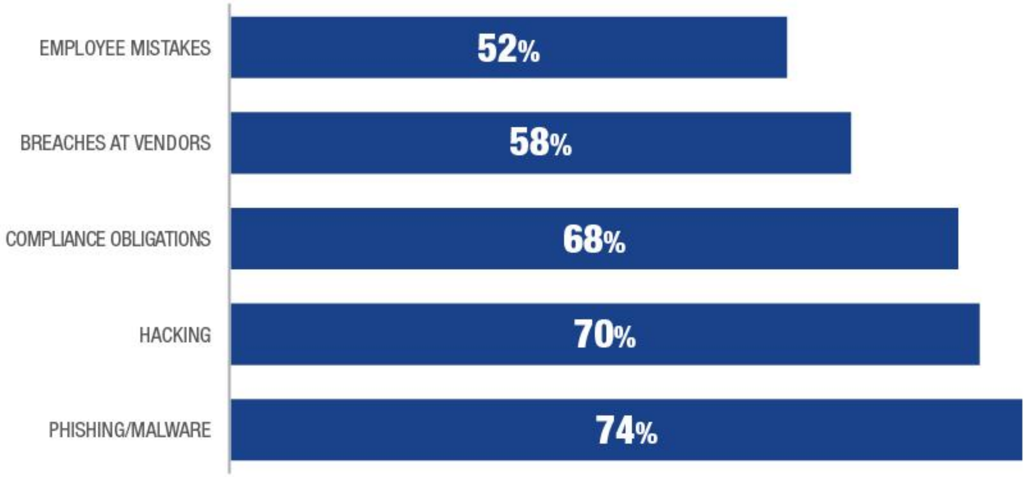

Figure 2
Top Five Privacy and Data Security Concerns Among General Counsel

In the sections that follow, we take a closer look at what specifically concerns law departments when it comes to cybersecurity and privacy, as well as how companies address related corporate governance, compliance, and operational challenges.

CYBER: A TOP-OF-MIND CONCERN

The steady stream of data security incidents making news headlines is a constant reminder of the potential risks that virtually every company currently faces. Just five or ten years ago, few in-house practitioners would have identified cybersecurity as their foremost concern. Fast forward to 2018, and cybersecurity is a top-of-mind concern for a majority of general counsel.

The Threat of Ransomware Attacks

Hacking, phishing, malware, and ransomware attacks represent the greatest privacy and data security concerns among general counsel – concerns that may be based on personal experience. In our survey, 17% of respondents indicated that they faced a ransomware attack within the last year. Among companies that were victims of an attack, none reported that they paid ransom.

Incident Response Planning

ONE IN THREE COMPANIES DO NOT HAVE A CYBER INCIDENT RESPONSE PLAN IN PLACE

Experts agree that the best incident response strategies are formulated well in advance of an actual data breach. In the "age of the breach," nearly two-thirds of respondents (65%) indicated that they have a cybersecurity incident response plan in place. While this is great progress, there is still room for improvement. According to the latest survey data, one-third of respondents reported their organizations currently do not have a cyber incident plan in place. It is important to highlight that the mere existence of a plan is not enough. Cyber incident plans also need to be properly formulated, contain all necessary information, and must be regularly tested. In light of the number of respondents who indicated that their companies were victims of a ransomware attack, maintaining a detailed plan to drive the discussion and build consensus before an attack is the key to making a cyber incident a challenge rather than a crisis.

As illustrated in Figure 3 below, of the 65% of companies that have an incident response plan in place, only 5% test that plan with a tabletop exercise on a quarterly basis. This represents a notable decrease from the inaugural survey, in which 19% of respondents reported that they conduct quarterly tabletop exercises. It is important to note that nearly one-quarter of respondents (23%) admitted they never participate in tabletop exercises. The key to being a resilient company is testing a plan in the context of a breach.

In the face of the increasing risk of cyber incidents, there are a number of key steps that a company can take to protect itself from unwarranted attacks, including the following:

1. Make sure software patches are routinely applied.
2. If possible, only use supported operating systems and other software.
3. Utilize antimalware and antivirus software tools and services.
4. Back up your critical data.
5. Train your employees to spot phishing emails.
6. Create a cross-functional incident response plan.
7. Practice responding to a ransomware attack in a tabletop exercise to be able to hit the ground running when this type of event occurs.
8. Establish or enhance relationships with law enforcement and other critical partners.

Lastly, build muscle memory for your response and practice, practice, practice.

How Often Do You Test Your Plan with a Tabletop Exercise?

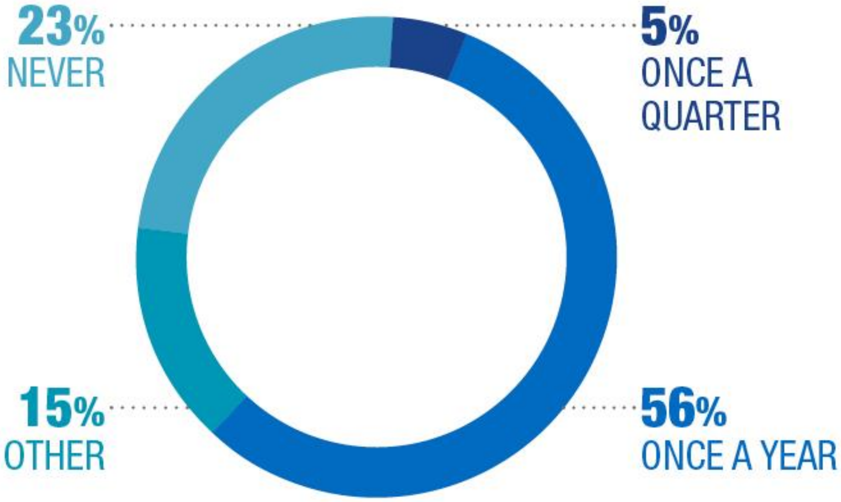

Figure 3
Frequency of Testing

Cybersecurity continues to be a top-of-mind issue for many boards of directors in the wake of recent large-scale data security incidents. As a result, we are seeing increased scrutiny on boards regarding their oversight role in the context of cyber preparedness and breach response and anticipate that more boards will request to be kept up to date on cyber and breach preparedness. Our survey reveals tremendous variation in the way law departments share information regarding cyber issues with their boards of directors (Figure 4).

According to the survey, 19% of respondents see it as so important that they report to the board quarterly, while an additional 32% do so annually. On the other end of the spectrum, 34% of survey respondents indicated that they never report to the board of directors on cyber issues.

How Often Do You Report on Cybersecurity Issues to Your Board of Directors?

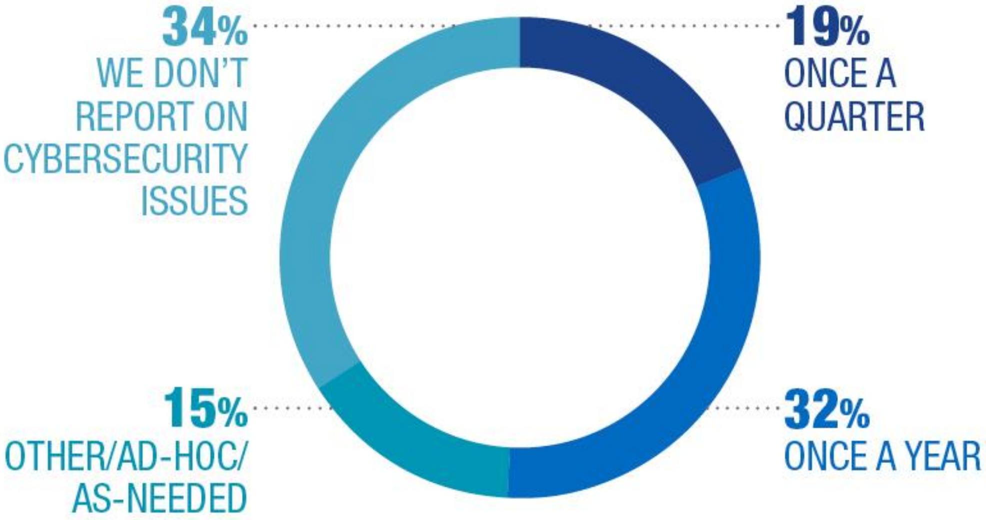

Figure 4
Frequency of Board Reporting

Although there is no simple solution to prepare for the threat of a cyber-attack, there are three broad topics that many boards of directors are starting to examine as they review and assess these issues:

- How important cybersecurity is to the company;
- What steps the company has taken to evaluate and mitigate cybersecurity risks; and
- What public disclosures the company has made.

PRIVACY: AN AREA OF GROWING CONCERN ON A GLOBAL SCALE

In this digital age where information has no borders, virtually every company has to worry about privacy. If a company has employees or customers, maintains a website, sells directly to consumers, or operates business to business, it must address privacy issues. The GC Up-at-Night research aims to understand how organizations are navigating in a fragmented global regulatory environment. This struggle is perhaps no more difficult than in the areas of privacy and data security, where unsettled law, shifting norms, and rapidly changing technology multiply the challenges.

The international transfer of personal information presents unique regulatory and compliance challenges for global organizations. When asked about their preferred mechanisms for transferring personal data globally, a majority of respondents (44%) identified contracts as the primary mechanism they rely on to move personal information. As seen in Figure 5 below, next to contracts is consent (24%), followed by binding corporate rules (16%) and privacy shield (12%).

While respondents generally prefer to rely on contract clauses to govern the process, the differences between the spring and fall results show consent is gaining acceptance as a preferred mechanism to move personal information globally.

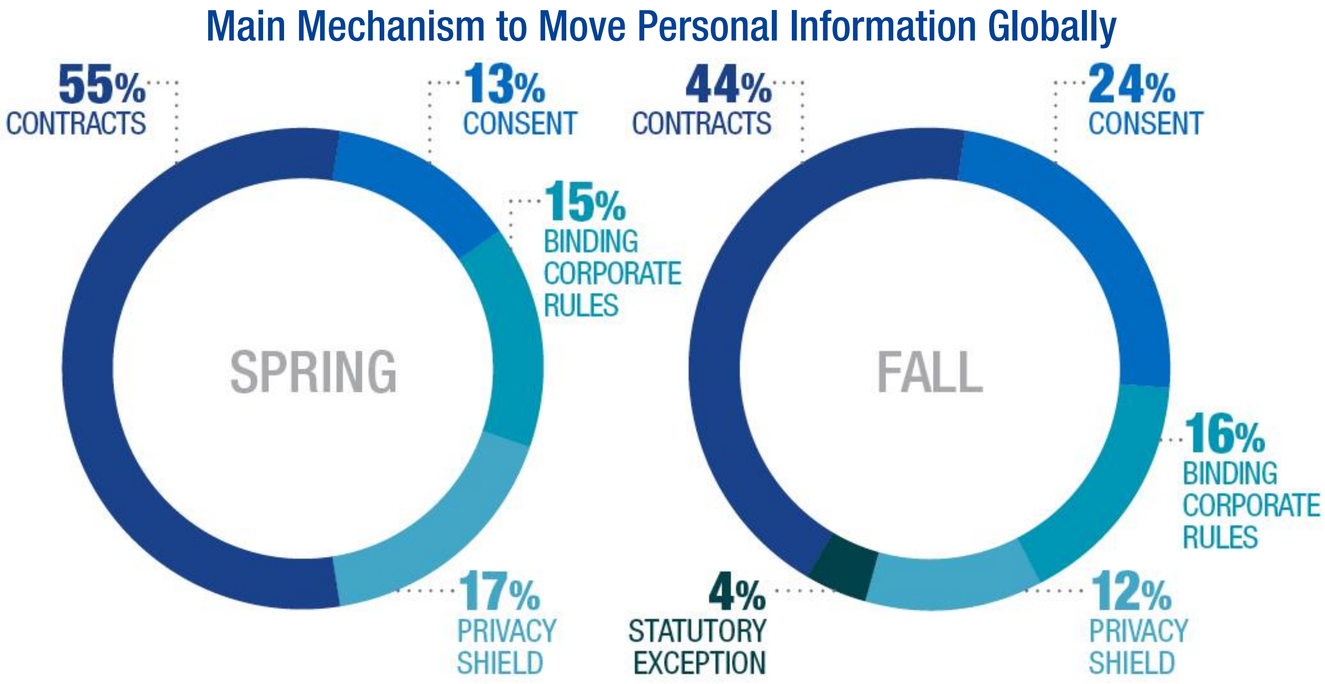

Figure 5
Main Mechanisms for Global Transfer of Personal Data

GDPR Readiness

As the GDPR compliance deadline quickly approaches, legal departments are scrambling to keep pace, and with good reason. The GDPR introduces far-reaching obligations for companies that collect, use, or otherwise process personal information of individuals in Europe. In contrast to the EU's current privacy regime – comprised of a patchwork of national data protection laws – the GDPR seeks to provide a single pan-European framework. The new regulation, which will apply directly in all Member States on May 25, 2018, applies to companies established in the EU and to companies outside of the EU that offer goods or services directly to individuals in the EU or that monitor the behavior of individuals in the EU.

GDPR Budgets

Of the respondent organizations with business operations in Europe, an overwhelming majority reported that they are budgeting less than US$500k to comply with the GDPR (Figure 6). While managing scarce resources to confront challenges was a concern expressed in the survey, low budgets may also reflect the fact that respondents do not realize the full scope of the issues they need to consider. Morrison & Foerster's GDPR Readiness Center features a list of essential questions you should be asking as your organization prepares for the GDPR.

How Much Are You Budgeting to Comply with GDPR?

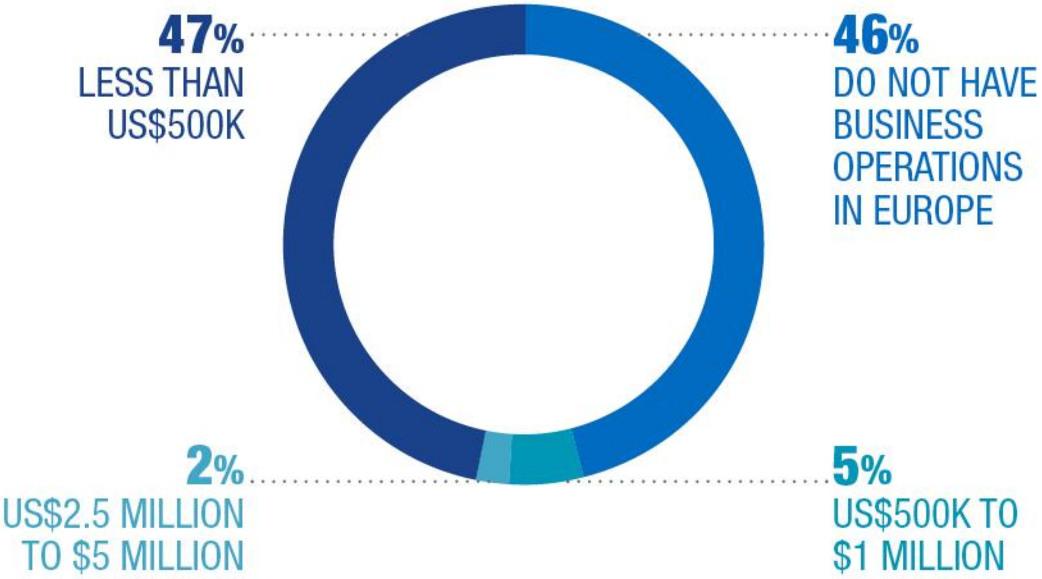

Figure 6
Size of GDPR Budgets

Data Protection Officers

Among the new compliance requirements ushered in by the GDPR, some companies will be obligated to appoint a data protection officer (DPO). When asked where in their organizations the position would be situated, one-quarter of respondents (25%) indicated that the position would be based in Europe, while 12% indicated that the position would be situated in global headquarters outside of Europe. The remaining 62% indicated the question is not applicable to their business.

If You Are Required to Appoint a Data Protection Officer Under the GDPR, Where Would That Person Be Located?

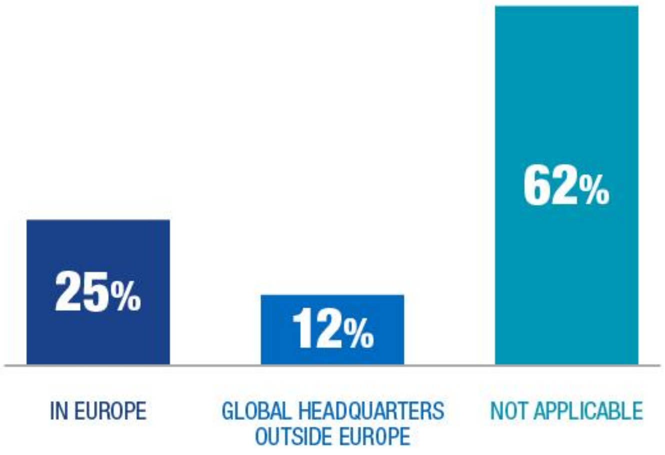

Figure 7
Where in an Organization Would a Data Protection Officer Be Situated

Other International Requirements

An overwhelming number of respondents (88%) report that they have not added any additional resources in light of international privacy developments, such as the GDPR and Japan's Personal Information Act (Figure 8). For the remaining 12% of companies that have added resources, some of the main resources they have included are additional headcount and/or an increased outside counsel budget (Figure 9).

Have You Added Additional Resources in Light of International Privacy Developments?

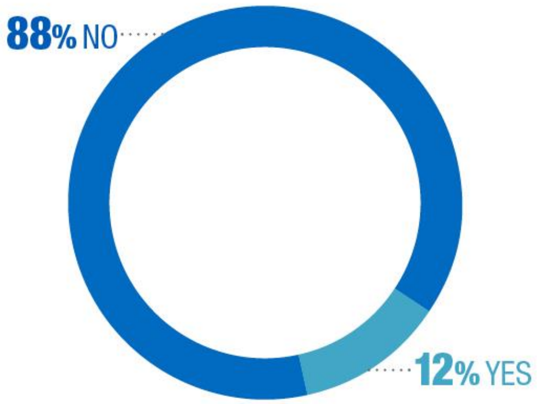

Figure 8
Companies That Have Added Resources to Meet International Privacy Requirements

Of Those That Said Yes, Additional Resources Respondents Have Added:

SPRING

- Attorney and security headcount
- Compliance manager
- Expertise, people
- Head of information security, one additional staff member and IT tools
- Parent company staff
- Outside legal counsel budget

FALL

- Big four accounting firm gap assessment
- Outside experts
- Staff and external resources

Figure 9
Resources That Companies Have Added to Meet International Privacy Requirements

Employee Training

While training on privacy issues continues to be a priority for a vast majority of companies, with 64% of respondent organizations providing privacy training to at least some of their respective workforces, nearly 40% of respondents indicated that they don't provide any privacy training to their workforce (Figure 10).

Does Your Company Provide Privacy Training to Your Workforce?

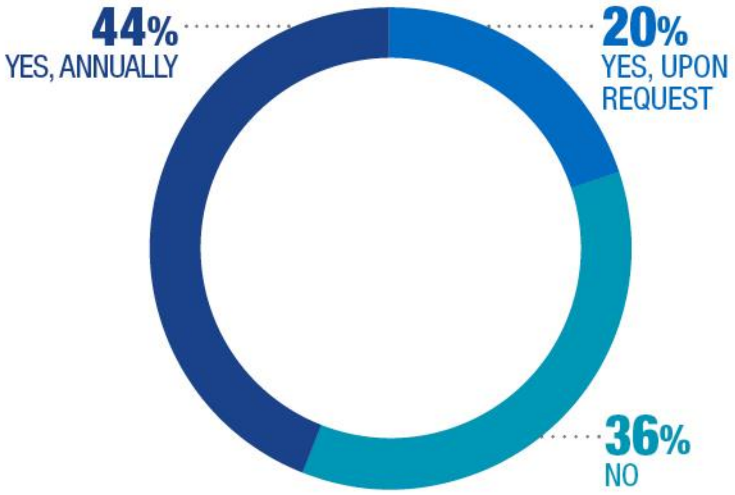

Figure 10
Companies That Provide Privacy Training

OPERATIONAL CONSIDERATIONS

Distinguishing Between Data Security and Privacy

Data privacy and data security are distinct yet interrelated concepts with respect to a company's informational assets. Data privacy refers to an organization's handling of individuals' personal data in a manner that is both legally compliant and consistent with the representations it makes to the individuals whose data it holds. Data security, on the other hand, refers to the steps the organization takes to live up to those representations and prevent misuse or improper access. Understanding this distinction is important to ensure that businesses take a holistic approach to these issues.

53% OF COMPANIES DISTINGUISH BETWEEN DATA SECURITY AND PRIVACY

In our survey, respondents were nearly evenly split when asked if their companies distinguish between data security and privacy, with 53% indicating that their company makes a distinction.

Specifics regarding the ways in which companies distinguish between data privacy and data security differ. In answering the question "How does your company distinguish between cyber and data security versus privacy?" survey respondents indicated that their companies make the distinction in one of five ways:

- Policies and Procedures
- Reporting Structures
- Data Classification
- Training
- Systems

One other response was instructive, indicating that the distinction between privacy and data security is unnecessary because the company "do[es] not have personal data, so [there are] no privacy issues." In today's business environment, it is hard to imagine a company that does not maintain *any* personal information. Companies may not appreciate that privacy obligations apply to all data that identifies an individual or relates to an identifiable individual.

The Emerging Role of Law Departments

Distinguishing between privacy and data security also clarifies the respective roles of the legal and information technology departments.

Law departments have quickly established themselves as corporate leaders in addressing privacy issues. As illustrated in Figure 11 below, an overwhelming number of respondents (79%) indicate that primary responsibility for privacy issues sits with the legal or compliance department.

Within Your Organization, Where Is the Responsibility for Privacy?

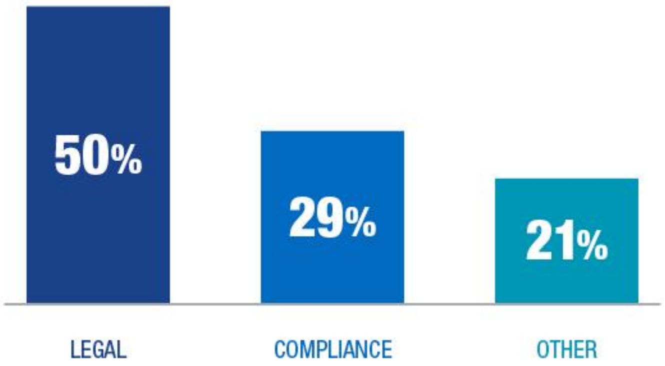

Figure 11
Corporate Department(s) Responsible for Privacy

Our latest survey results show a notable increase in the presence of a dedicated chief privacy officer (CPO) at their companies. Previously, only 14% of respondents pointed to the presence of a CPO at their company. However, the new data shows a 10% increase in this area, with 24% of respondents pointing to the presence of a CPO at their company. This suggests a growing awareness of the impact of privacy on the corporate bottom line.

The Role of IT Departments

THREE IN FOUR RESPONDENTS INDICATE HAVING A CHIEF INFORMATION SECURITY OFFICER AT THEIR CORPORATION

While relatively few organizations reported having a CPO, 75% of survey respondents indicated having a chief information security officer (CISO), with 27% maintaining organizational structures where the CISO reports through IT (Figure 12).

This suggests that businesses tend to view data security as under the purview of IT, while the responses presented above in Figure 10 indicate that responsibility for privacy tends to be under the control of the legal or compliance departments.

To Which Group Does the Chief Information Security Officer (CISO) Report?

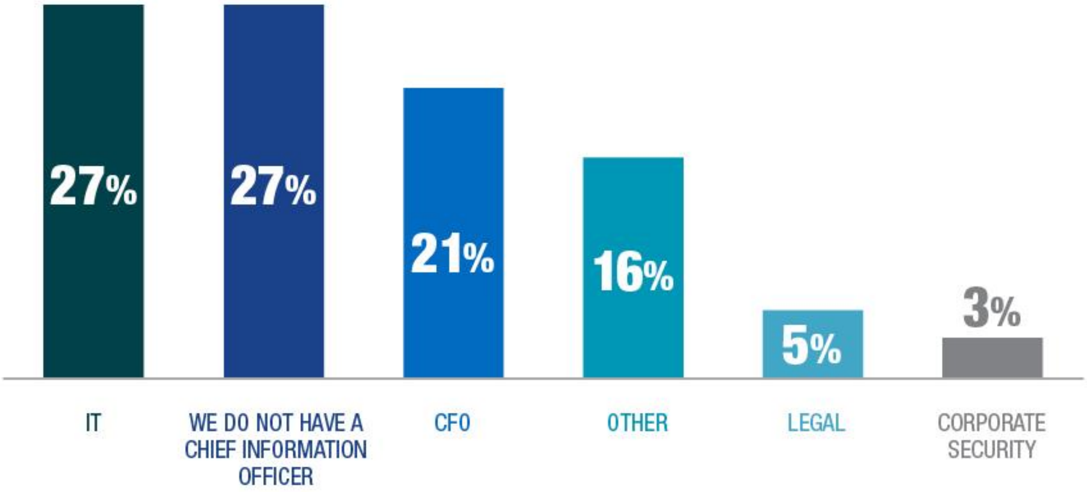

Figure 12
CISO Reporting Line

CONCLUSION

Privacy and data security have rapidly ascended to top-of-mind concerns for in-house legal departments – and with good reason. With the GDPR deadline looming around the corner and as stringent international regulations, increased enforcement, and data security incidents show no signs of slowing down, organizations need to be prepared, now more than ever. As evidenced by the data presented in this report, primary responsibility for all of these issues overwhelmingly falls to an organization's legal and compliance professionals.

As our survey indicates, organizations have responded admirably to these new challenges – training employees on privacy issues and maintaining cyber incident response plans, which are now the industry standard, but there is more to be done. In one watershed finding, we discovered that sizable minorities of respondents do not report on cyber issues to their boards of directors and others do not report on these issues frequently. With increased scrutiny on boards to exercise oversight on cyber issues, reporting to the board on privacy and cyber matters will increasingly be viewed as an essential tool to reduce exposure of the company.

The survey also sheds light on the importance of not only *drafting* an incident response plan, but also routinely *testing* it with realistic tabletop exercises. Our data shows nearly one-quarter (23%) of respondent companies have never participated in a tabletop exercise and only 5% conduct quarterly tabletop exercises. The most resilient companies have a practiced plan in place so that respective roles are clearly defined and communicated when every minute counts.

We hope you found these survey insights valuable. For additional resources for privacy and data security and GDPR compliance, visit Morrison & Foerster's Cybersecurity Resource Center (www.mofo.com/cybersecurity) and GDPR Readiness Center (www.mofo.com/gdpr). If you require any additional guidance to help manage these business challenges, please feel free to contact us.

ABOUT THE AUTHORS

About ALM

ALM, an information and intelligence company, provides customers with critical news, data, analysis, marketing solutions, and events to successfully manage the business of business. Customers use ALM solutions to discover new ideas and approaches for solving business challenges, connect to the right professionals and peers to create relationships that move business forward, and compete to win through access to data, analytics, and insight. ALM serves a community of over six million business professionals seeking to discover, connect, and compete in highly complex industries.

About ALM Intelligence

ALM Intelligence supports legal, consulting, and benefits decision-makers seeking guidance on critical business challenges. Our proprietary market reports, rating guides, prospecting tools, surveys, and rankings inform and empower leaders, enabling them to proceed with confidence.

About Morrison & Foerster

We are Morrison & Foerster – a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology, and life sciences companies. The *Financial Times* has regularly named the firm to its lists of most innovative law firms in North America and Asia since publishing its Innovative Lawyers Reports in those regions. In the past few years, *Chambers USA* has honored MoFo's Privacy and Data Security, Bankruptcy, and IP teams with Firm of the Year awards, the Corporate/M&A team with a client service award, and the firm as a whole with the Global USA Firm of the Year award. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

ALM Intelligence

MORRISON
FOERSTER