GENERAL COUNSEL
UP-AT-NIGHT REPORT

PRIVACY + DATA SECURITY IN-DEPTH REPORT

SUMMER 2017

ALM Intelligence

MORRISON FOERSTER

INSIDE

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

Morrison & Foerster is excited to partner with ALM Intelligence on the *General Counsel Up-at-Night Report*, 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 the findings with you.

According to the survey, privacy and data security are among the top concerns of in-house legal departments today. This comes as no surprise. High-profile security incidents have dominated news headlines. At the same time, enhanced global regulatory regimes have created a complex matrix of requirements with which global companies must comply.

A deeper dive revealed more nuanced findings, many of which were enlightening, including:

- One-third of survey respondents do not have a cyber incident response plan in place. Of those that have a plan, 30% have either never tested it with a tabletop exercise or test it less than once a year.
- 38% of respondents do not regularly report cybersecurity issues to their board of directors.
- Nearly a quarter of respondents reported facing a ransomware attack in the last year.

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 survey identified privacy and data security as a new area of concern among law department leaders, with 65% of respondents describing privacy and data security as a very important challenge (Figure 1).

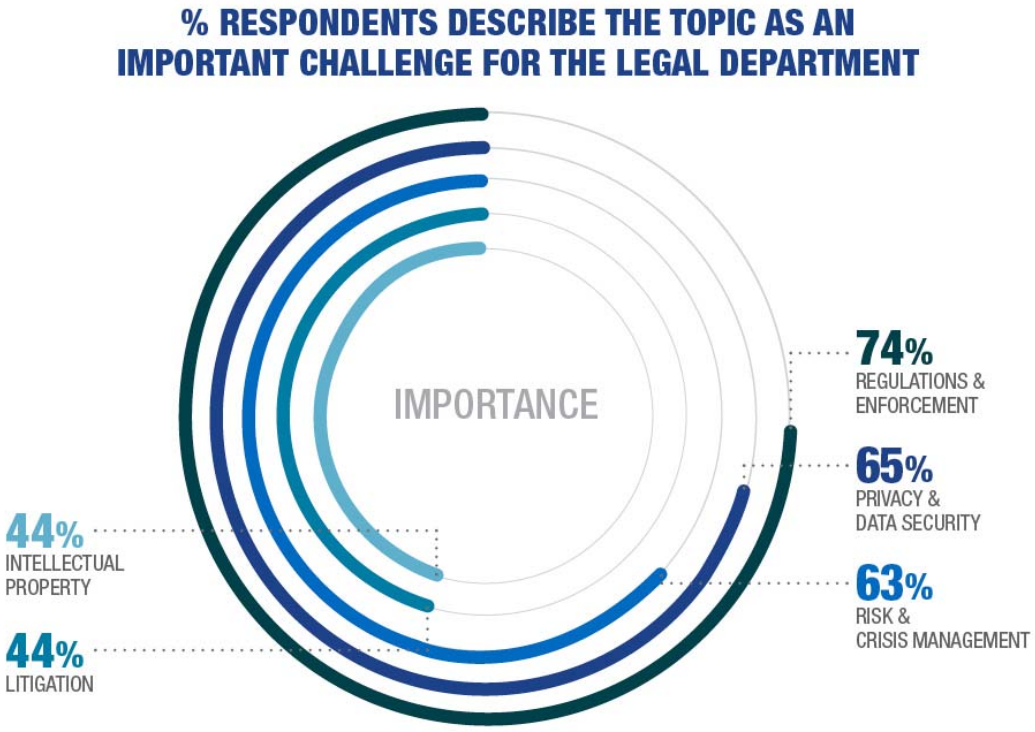

Figure 1
Most Significant Challenges Facing Law Departments

Respondents overwhelmingly identified hacking/phishing/malware/ransomware as the greatest area of concern (87%), followed by issues resulting from employee error (62%) and the risk of breaches via non-law-firm vendors (50%) (Figure 2).

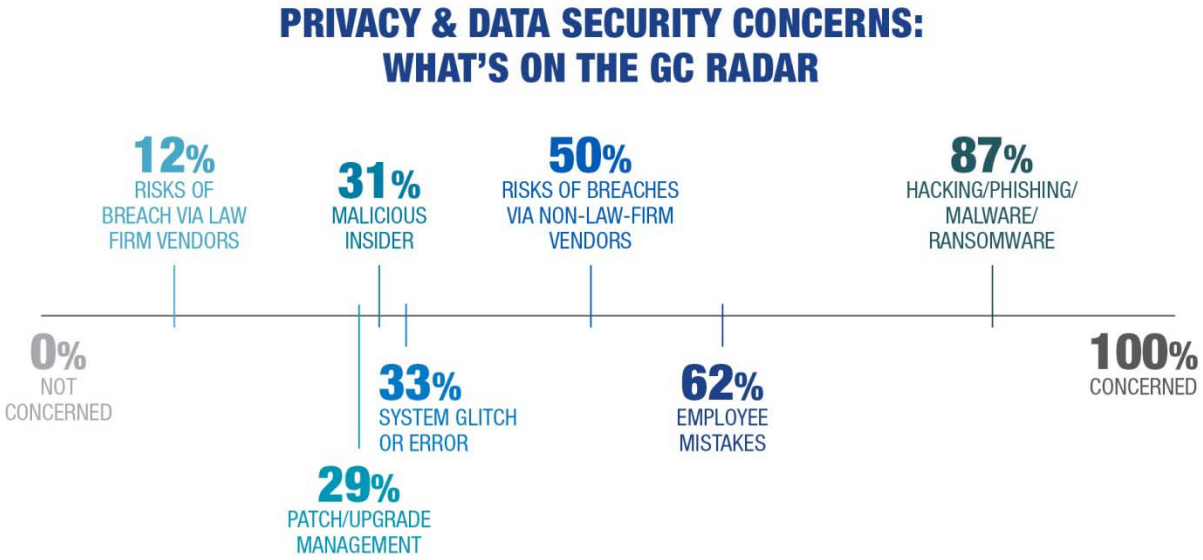

Figure 2
Privacy and Data Security Concerns Among General Counsel

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 10 years ago, few in-house practitioners would have identified cybersecurity as their foremost concern. Fast forward to 2017, and cybersecurity is a top-of-mind concern for a majority of general counsel.

The Threat of Ransomware Attacks

ONE IN FOUR COMPANIES WERE RANSOMWARE VICTIMS IN THE LAST YEAR

Hacking, phishing, malware, and ransomware attacks represent the greatest privacy and data security concerns among general counsel — a concern that may be based on personal experience. In our survey, nearly one in four respondents (24%) indicated that they faced a ransomware attack within the last year. Among companies that were victims of an attack, none reported that they paid the 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," two thirds of respondents (67%) indicated that they have a cyber incident response plan in place. That is great progress. 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 crisis.

As illustrated in Figure 3 below, of the 67% of companies that have an incident response plan in place, 19% test that plan with a tabletop exercise on a quarterly basis, while 51% conduct a similar exercise annually. The key to being a resilient company is testing that plan in the context of a breach.

Build muscle memory for your response and practice, practice, practice.

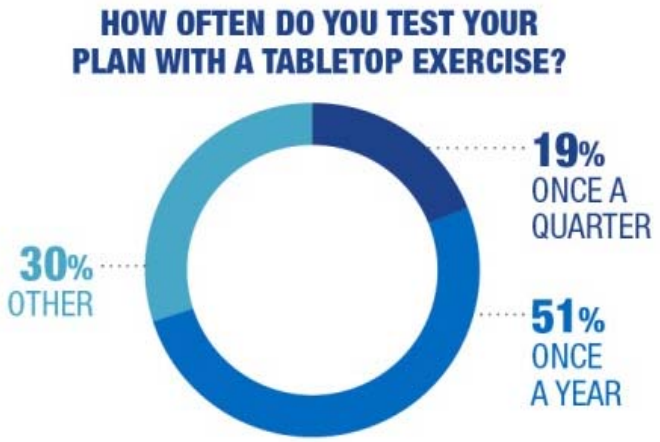

Figure 3
Frequency of Testing

Cybersecurity and the Board of Directors

Our survey reveals tremendous variation in the way law departments share information regarding cyber issues with their boards of directors.

Twenty-two percent of respondents see it as so important that they report to the board quarterly, while an additional 23% do so annually.

On the other end of the spectrum, nearly 40% of survey respondents indicated that they never report to the board of directors on cyber issues.

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. (Figure 12).

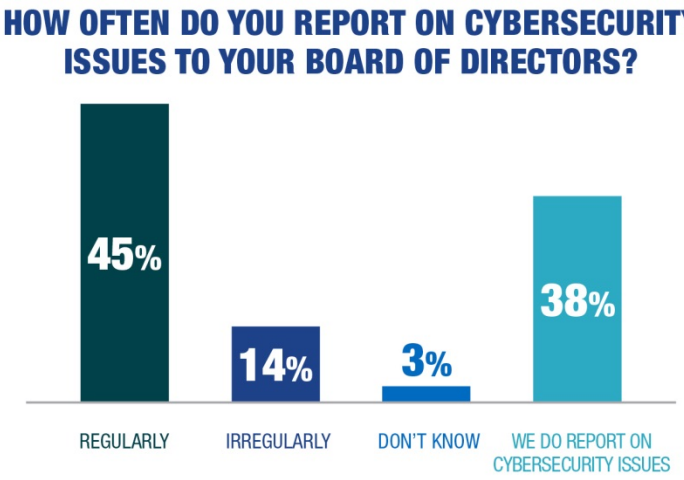

Figure 4
Frequency of Board Reporting

PRIVACY: AN AREA OF GROWING CONCERN

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. For companies with international operations, compliance with complex and often conflicting privacy regulations imposes onerous obligations on the legal department and other functions alike.

Global Data Transfers

The international transfer of personal information presents unique regulatory and compliance challenges for global organizations. When asked about the preferred mechanism for transferring personal data globally, respondents overwhelmingly indicated that they rely on contractual clauses. As seen in Figure 5 below, 55% identified contracts as the primary mechanism to move personal information, followed by Privacy Shield (17%), binding corporate rules (15%), and consent (13%).

The strong preference for contract clauses may be attributed to the uncertainty surrounding Privacy Shield or the fact that that it only works for transfers between Europe and the United States. A minority of respondents (13%) identified consent as the primary mechanism for moving personal information globally, likely owing to the significant logistical limitations of utilizing consent.

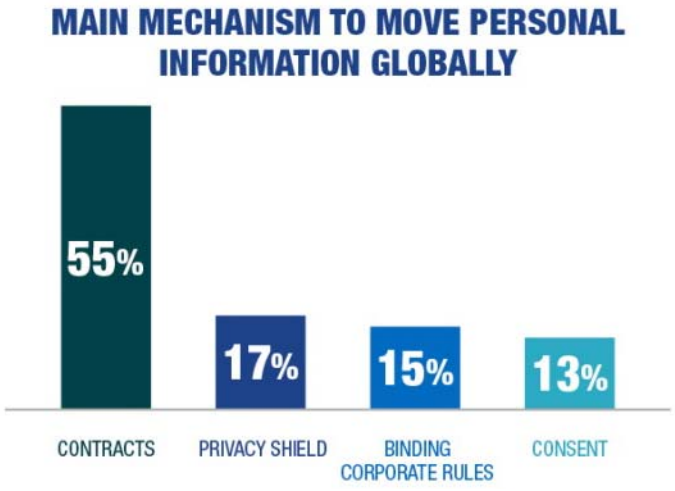

Figure 5
Main Mechanism for the Global Transfer of Personal Data

GDPR Readiness

The EU General Data Protection Regulation (GDPR) introduces far-reaching obligations for companies that collect, use, or otherwise process personal information. 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 in May 2018, applies to companies established in the EU, and to companies outside the EU that offer goods or services directly to individuals in the EU or that monitor the behavior of individuals in EU.

GDPR Budgets

A little more than half of the companies surveyed (54%) have European operations. Of those companies, 90% report that they have budgeted less than US$500,000 to comply with GDPR. The remaining 10% have budgeted between US$500,000 and US$1 million (Figure 9).

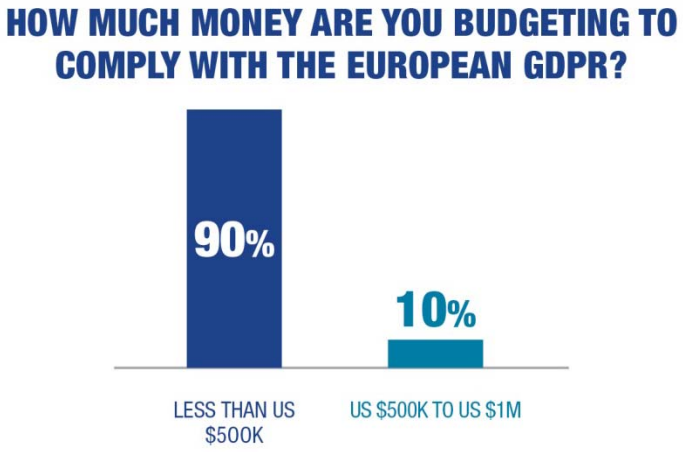

Figure 6
Size of GDPR Budgets

Data Protection Officers

Among the new compliance requirements under GDPR, some companies will be obligated to appoint a Data Protection Officer (DPO). As captured below in Figure 7, 10% of respondents already have a DPO in place in at least one country, while 16% indicate that they anticipate appointing a DPO to comply with GDPR.

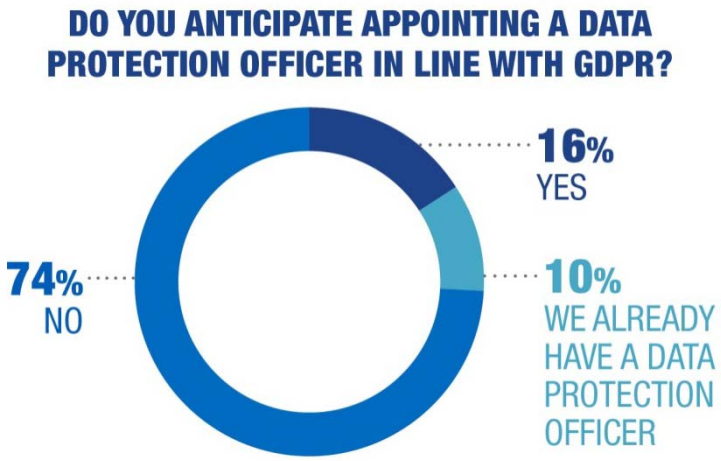

Figure 7
Companies With a Data Protection Officer

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 GDPR and Japan's Personal Information Act. For the 12% of companies that have added resources, the resources have included additional headcount and/or an increased outside counsel budget (Figure 8).

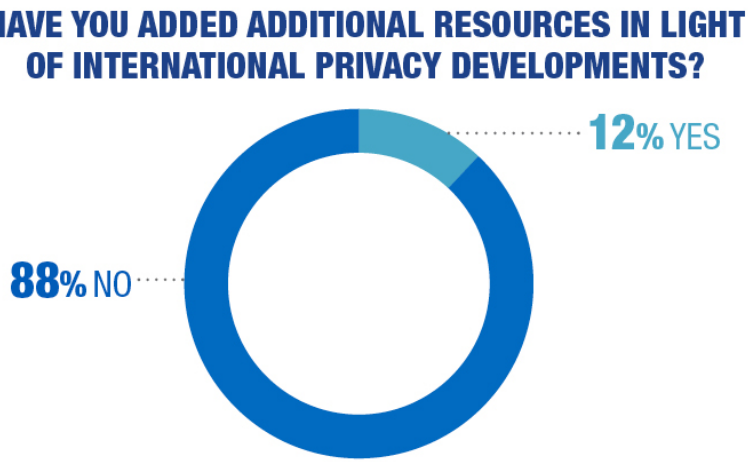

Figure 8
Companies That Have Added Resources to Meet International Privacy Requirements

Employee Training

Training on privacy issues continues to be a growing trend and standard regardless of industry sector or company size. Three-quarters of respondent companies (75%) provide privacy training for at least some of their respective workforces. Forty percent provide privacy training on an annual basis (Figure 9).

Figure 9
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 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 10 below, an overwhelming number of respondents (78%) indicate that primary responsibility for privacy issues sits with the legal or compliance department.

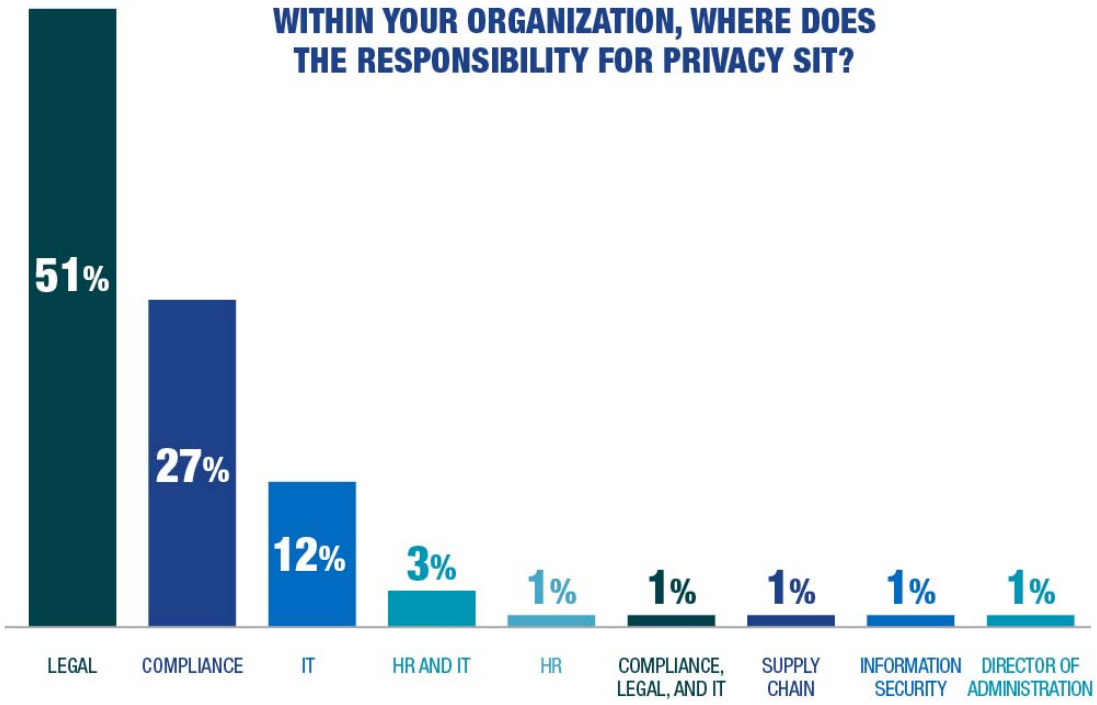

Figure 10
Corporate Department(s) Responsible for Privacy

14% OF COMPANIES HAVE A CHIEF PRIVACY OFFICER

Some companies have appointed a dedicated Chief Privacy Officer (CPO). Our survey indicates, however, that number is relatively low. Only 14% of respondents in our survey pointed to the presence of a CPO at their company.

The Role of IT Departments

75% **OF COMPANIES HAVE A CHIEF INFORMATION SECURITY OFFICER**

While relatively few organizations reported having a CPO, 75% of survey respondents indicated having a Chief Information Security Officer (CISO) with the majority (42%) maintaining organizational structures where the CISO reports through IT (Figure 11).

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.

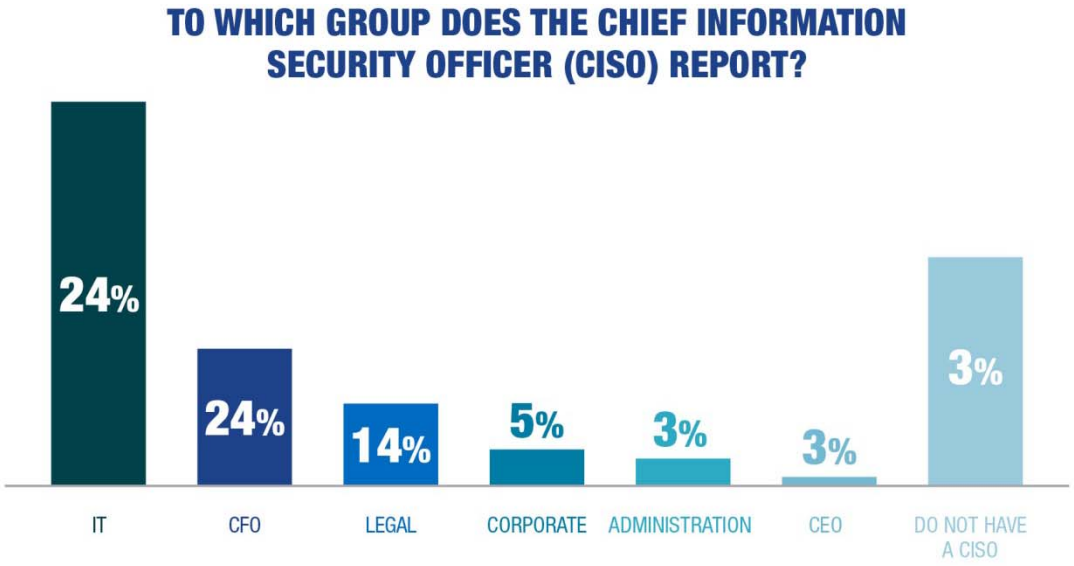

Figure 11
CISO Reporting Line

CONCLUSION

Privacy and data security have rapidly ascended to top-of-mind concerns for in-house legal departments — and with good reason. We've witnessed a significant uptick in stringent international regulations, increased enforcement, and data security incidents in just the last few years. The latter include, notably, ransomware attacks, which one-quarter of respondents reported facing in the last year alone. 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 a sizable minority 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 and will increasingly be viewed as an essential tool to reduce exposure of the company.

The survey also shed light on the importance of not only *drafting* an incident response plan, but also routinely *testing* it with realistic 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.

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.