The Emergence of Cybersecurity Law

Prepared for the Indiana University Maurer School of Law
by Hanover Research | February 2015
# TABLE OF CONTENTS

Executive Summary and Key Findings ........................................................................................................ 2  
  INTRODUCTION ...................................................................................................................................... 2  
  KEY FINDINGS ....................................................................................................................................... 2  

Cybersecurity and the Law ........................................................................................................................ 4  
  THE CHALLENGE OF CYBERSECURITY ................................................................................................. 4  
  CORPORATE CYBERSECURITY PREPAREDNESS ................................................................................ 6  
  THE FUTURE OF CYBERLAW ..................................................................................................................... 8  

Legal Developments in Cyberlaw ............................................................................................................. 11  
  CYBERLAW LEGISLATION AND GUIDANCE ......................................................................................... 11  
    Lack of Federal Legislation .................................................................................................................. 12  
    Federal Trade Commission Act, Section 5 .......................................................................................... 13  
    SEC Disclosure Guidance ............................................................................................................... 15  
    NIST Framework ............................................................................................................................... 16  

How Lawyers Help Meet Cyberthreats ................................................................................................. 18  
  THE ROLE OF LAWYERS IN CYBERSECURITY .................................................................................. 18  
    Why Should Lawyers be Involved? ..................................................................................................... 18  
    What Are Lawyers Doing? .................................................................................................................. 19  
    What Should Lawyers Be Doing? ......................................................................................................... 22  

KNOWLEDGE AND SKILLSETS FOR CYBERLAWYERS ........................................................................ 24  
    What Lawyers Need to Know ............................................................................................................. 24  
    How Lawyers Learn About Cybersecurity .......................................................................................... 26  

Methodology ........................................................................................................................................... 29
EXECUTIVE SUMMARY AND KEY FINDINGS

INTRODUCTION

This paper examines cyberlaw as a growing field of legal practice and the roles that lawyers play in helping companies respond to cybersecurity threats. Drawing on interviews with lawyers, consultants, and academics knowledgeable in the intersection of law and cybersecurity, as well as a survey of lawyers working in general counsel’s offices, this study examines the broader context of cybersecurity, the current legal framework for data security and related issues, and the ways in which lawyers learn about and involve themselves in cybersecurity issues. These discussions are presented across the paper’s three sections:

- **Cybersecurity and the Law** explores the context in which cyberlaw is developing, examining the importance of cybersecurity to companies and corporations and how inside and outside counsel are responding.

- **Legal Developments in Cyberlaw** provides an overview of the current state of the legislation, regulations, and other sources of law and policy influencing cybersecurity.

- **How Lawyers Help Meet Cyberthreats** examines lawyers’ roles cybersecurity in more detail, including both the tasks they should perform and the tasks they do perform. This section also examines how lawyers are improving their knowledge of cybersecurity.

KEY FINDINGS

- **Cybersecurity is a growing priority for legal practitioners.** Of the corporate law departments surveyed for this study, over half rate cybersecurity as a “high concern.” To meet the growing demand for counsel on these issues, multiple large law firms have formed cybersecurity practice groups; some areas may even be experiencing a shortage of qualified practitioners. Although the market for cyberlaw services remains in a nascent stage, experts expect that in the long term, the field will continue to grow.

- **Corporations, including their legal counsel, can improve their preparedness for cyberthreats.** Multiple studies have found that substantial numbers of corporate leaders lack full confidence in their organizations’ preparedness. Similarly, among the corporate law departments surveyed for this study, the average self-rating falls well short of full preparedness. To address these threats, law departments need more resources, as well as better information about the issues surrounding cybersecurity and the law.

- **Cybersecurity has become as much a legal issue as a technical one.** Given the fragmented legal framework for data security and privacy issues, organizations must be aware of a “quilt” of laws and regulations they may be subject to; this is largely the purview of legal counsel. Working in coordination with IT professionals,
managers, and other parts of the corporation, lawyers must play a role in designing the procedures, training, and risk assessments required to implement managerial, operational, and technical controls needed to protect data.

- **Lawyers are becoming more proactive in addressing cybersecurity concerns.** Until very recently, companies primarily involved lawyers in the response to cybersecurity incidents, rather than in the planning against such crises. However, driven in part by pressure from agencies such as the Securities and Exchange Commission, legal counsel is becoming more proactive; among the corporate law departments surveyed for this study, nearly 70 percent report proactive involvement in cybersecurity.

- **Lawyers need more education in both the legal and technical aspects of cybersecurity.** Over two-thirds of the corporate law departments surveyed for this study rated improved cybersecurity training as “very” or “extremely” important. Experts suggest that such training should encompass both the legal and technical aspects of cybersecurity; when asked what areas of training would be “most beneficial” to them, corporate counsel largely agreed. However, experts also caution that lawyers cannot be expected to maintain detailed knowledge of associated technology. Instead, technical training should enable lawyers to “ask the right questions” of IT professionals and technical experts.
CYBERSECURITY AND THE LAW

THE CHALLENGE OF CYBERSECURITY

Over the past year, a number of high profile data security breaches at large retailers,¹ and broad-reaching security threats like the Heartbleed Bug,² have heightened public awareness about the threat of cyberattacks to personal information. Moreover, according to a 2013 study on the cost of cybercrime by the Ponemon Institute, the United States led nine other nations in highest average organizational cost-per-breach and largest average number of breached records.³ According to the same survey, the annualized cost of cybercrime increased by 30 percent from 2012 to 2013, now estimated at $11.6 million per year per company studied.⁴

As a result, cybersecurity has emerged as a primary concern for many corporate leaders. A 2014 survey of nearly 500 company directors and general counsel found that “data security” was the number one issue for directors that “keeps them up at night,” and the second most important issue for general counsel, after regulatory compliance.⁵ Similarly, among the corporate law departments surveyed for this study, a majority rated cybersecurity as a “high concern,” both company-wide and within the law department.

Figure 1.1: Level of Concern about Cybersecurity Among Corporate Counsel

How much of a concern is cybersecurity within your . . .

Source: Survey of corporate law departments. See methodology section for further details.

² “Heartbleed.” CNET. http://www.cnet.com/tags/heartbleed/
⁴ Ibid., p. 24.
⁵ Ibid., p. 22.
The broad range of negative impacts that a successful cyberthreat poses to companies drive such concerns—financial loss is just one of the problems that can result from a breach. In 2012, for instance, PricewaterhouseCoopers found that about 38 percent of businesses experience financial losses as a result of cybersecurity incidents, but that similar numbers also suffer intellectual property theft and brand or reputation damage.\(^6\)

Indeed, given the often highly publicized nature of cybersecurity breaches, reputation damage may be one of the greatest threats this risk poses. Among the corporate law departments surveyed for this study, the cybersecurity consequence respondents ranked as their top concern is “Potential for damage to reputation with customers”; purely legal consequences, such as regulatory action or lawsuits, were ranked lower, with loss of shareholder confidence ranking lowest. Almost half of respondents gave a rank of 1 or 2 to “Potential for damage to reputation with customers” or “Loss of company’s intellectual property,” while only about a quarter gave such ratings to “Potential for loss of confidence among shareholders/investors.”

Figure 1.2: Corporate Counsel’s Top Concerns for Cybersecurity

Source: Survey of corporate law departments.

CORPORATE CYBERSECURITY PREPAREDNESS

Cybersecurity clearly has the attention of corporate leaders, including the law department. However, indications suggest that these leaders are not as prepared as they could be to meet these threats. PricewaterhouseCoopers found that fewer than half of the chief information officers and chief security officers it surveyed “have an effective information security strategy in place and are proactive in executing the plan.” The remainder either lack a strategy, fail to execute it adequately, or are essentially reactive in meeting cyberthreats.7

General counsel similarly have room for improvement. In a 2014 survey of corporate directors and general counsel, majorities of each group reported not having confidence in their company’s cybersecurity breach response plan, and nearly a third of each group indicated that they “are not convinced their company is secure and impervious to hackers.”8 Similarly, when asked to rate their preparedness to meet cyberthreats, the law departments surveyed for this study gave an average rating of 6.57 on a 10-point scale. Approximately 40 percent of respondents gave a rating of 8 or above, a proportion that increases to 70 percent for a grade of 6 or higher. Although this indicates moderate confidence in the general counsel’s preparedness, it also shows that law departments could be doing more to reach full preparedness for preventing and containing cybersecurity breaches.

![Figure 1.3: Corporate Counsel Preparedness to Meet Cyberthreats](source: Survey of corporate law departments.)

In this task, corporate law departments have at least two needs: better information and more resources. The latter problem emerged in a number of comments made by respondents to the survey conducted for this study. As one attorney put it, although cybersecurity is a “very important matter for us,” the law department lacks “the finances or manpower to dedicate to this issue.” Another respondent noted that boards and senior management tend to view cybersecurity as a cost center; with a focus on financial performance, they prefer to devote resources to “sales, marketing, and [other] activities that grow revenue.” It comes as little surprise, then, that the majority of law departments surveyed have no staff dedicated to cybersecurity at any capacity; only 23.5 percent reported employing staff full-time on the issue.

---

7 Ibid.
Beyond more resources, however, corporate leaders, including the law department, need to learn more about cybersecurity. In a 2014 survey, IT strategy and risk was ranked by 52 percent of corporate directors and 44 percent of general counsel as the “issue for which they need better information and processes to be as effective in their jobs as possible.”\textsuperscript{9}

Indeed, when law departments were surveyed for this study, only one-third of respondents reported being “very familiar” with the topic of cybersecurity. Most are, at best, “moderately” or even only “slightly” familiar with the issue. As one respondent put it, cybersecurity may be less of a concern for some law departments “probably because we do not know enough about it.”

\textsuperscript{9} Ibid., pp. 23-24.
THE FUTURE OF CYBERLAW

Looking ahead, the challenge of cybersecurity will remain a prominent issue for corporate leaders. However, the role of lawyers and law departments in addressing this challenge may develop more slowly. Although experts interviewed for this study cite a growing need for cyberlaw services, they also highlight difficulties translating that need into actual demand for legal services. On the other hand, indicators suggest that a shortage of qualified lawyers in the field may also be hampering the development of cyberlaw.

On the one hand, cyberlaw practice seems to be growing with every passing year. Some large law firms are already forming cybersecurity practice groups, which experts point to as a sign of “strong demand” for this expertise. Leading firms such as Hogan Lovells, Hunton & Williams, Sidley Austin, and K&L Gates already maintain cybersecurity-related practice groups, and even mid-sized firms are now venturing into the field. In California, law firms

11 DeMarco, J. Partner, DeVore and DeMarco. Phone Interview, July 18, 2014.
face a shortage of practitioners qualified in cybersecurity, as they compete with the Silicon Valley companies who often hire these lawyers as inside counsel. Multiple experts interviewed for this study agreed that the supply of lawyers knowledgeable in these areas is inadequate to meet current needs.

At the same time, cyberlaw practice may not have expanded as rapidly as some might have expected. David Bodenheimer, a partner at Crowell & Moring, chairman of the ABA Public Contract Law Section’s Cybersecurity Committee, and author of an early paper on cybersecurity and its legal ramifications, notes that the field of cyberlaw has grown more slowly than he initially predicted. Although firms are establishing practice groups in the field, many lawyers may still find it difficult to sustain a practice based on cybersecurity alone. Bodenheimer points to a kind of paradox: there are insufficient lawyers to perform the work companies should be doing in this area, but until companies fully realize the risks and regulatory requirements they face, there may be an inconsistent flow of work for lawyers who are active in the area.

Bodenheimer remains optimistic for the growth of cyberlaw. In the long term, he calls cyberlaw a “[bet] on the future,” as these issues are sure to become only more important. Other experts interviewed for this study agreed. Harriet Pearson, a partner at Hogan Lovells in Washington, D.C. and known to some as the “First Lady of Privacy,” noted that the “pervasiveness” of cybersecurity issues suggests a huge growth potential for the field. The mounting concern over cybersecurity issues triggers many legal considerations for managing risk, as well as proactive legal counselling opportunities. Pearson compares the trajectory of cyberlaw with that of other legal niches such as asbestos and toxic tort sites, in that once a major incident occurs, it will sustain the cyberlaw industry for a long time.

Clearly, the continuing evolution of the legal framework for cybersecurity should only increase the role of lawyers in addressing these concerns. In the following sections, this


Ibid.


white paper first explores the current legal developments in the field, followed by a more detailed discussion of how lawyers can help organizations to meet cyberthreats.
LEGAL DEVELOPMENTS IN CYBERLAW

CYBERLAW LEGISLATION AND GUIDANCE

A basic definition of cybersecurity is “whether and how electronic data and systems are protected from attack, loss, or other compromise.”\(^{22}\) It falls largely on general counsel and other senior lawyers to advise on a large scope of cybersecurity legal issues, including privacy concerns, data breaches, information sharing, and developing a plan of action for potential cybersecurity crisis situations. Currently, data protection and privacy are governed by a “patchwork” of state and federal regulations, as well as industry-specific legislation and guidelines that can leave both large and small companies wondering where to begin.\(^{23}\) More than 50 federal statutes address aspects of cybersecurity in some capacity, whether directly or indirectly, with no overarching piece of legislation in place.\(^{24}\)

In this environment, corporate law departments naturally pay the most attention to regulations and private lawsuits, rather than federal or state legislation. Among those surveyed for this study, a majority cite regulations or lawsuits as the greatest motive for taking action, with almost equal numbers driven by internal concerns (e.g., shareholders). Substantially fewer are concerned about legislation or binding judicial precedent.

![Figure 2.1: Types of Cybersecurity Law on Corporate Counsel’s Radar](source)

Although it is beyond the scope of this white paper to provide an exhaustive account of all sources of current cybersecurity law, the ensuing discussion outlines the major current

---


influences in the field. These include congressional actions, Section 5 of the Federal Trade Commission (FTC) Act, the SEC’s disclosure guidance, and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

**LACK OF FEDERAL LEGISLATION**

Congress has not passed major cybersecurity legislation since 2002. While many states have established their own laws to address cybersecurity, there is still no unifying federal legislation that addresses these issues. Broadly speaking, recent legislative proposals relating to cybersecurity in Congress concentrate on 10 main issues:

- National strategy and the role of government;
- Reform of the Federal Information Security Management Act of 2002 (FISMA);
- Protection of critical infrastructure (especially the electricity grid and the chemical industry);
- Information sharing and cross-sector coordination;
- Breaches resulting in theft or exposure of personal data such as financial information;
- Cybercrime offenses and penalties;
- Privacy in the context of electronic commerce;
- International efforts;
- Research and development (R&D); and,
- The cybersecurity workforce.

The privacy and information security practice group at law firm King & Spalding outlines several pieces of legislation that have been introduced to Congress recently that touch on cybersecurity issues. In addition to “several narrower bills” on cybersecurity introduced in the House of Representatives, the major recent attempts at federal cybersecurity legislation include:

- **Personal Data Privacy and Security Act of 2014.** Introduced by Senate Judiciary Chairman Patrick Leahy (D-VT) and four other Senate Democrats, this bill would create a national standard for data breach notification and require businesses to keep consumer information safe from hackers. Furthermore, it would toughen criminal penalties for those who conceal a damaging breach, require companies that keep data to establish safety policies, and update computer hacking penalties.

- **Data Security Act of 2014.** Introduced by Senate Homeland Security and Government Affairs Committee Chairman Senator Tom Carper (D-DE) and Senator

---

25 Ibid., pp. 2-3.
Roy Blunt (R-MO), this bill would require entities including financial institutions, retailers, and federal agencies to better safeguard sensitive information, investigate security breaches, and notify consumers when there is a substantial risk of identity theft or account fraud.

**The National Cybersecurity and Critical Infrastructure Protection Act of 2013.** This act addresses liability protections for private agencies that voluntarily cooperate on cybersecurity measures; cross-industry information sharing on cyber threats; and cyber-incident response teams to support critical infrastructure owners.

In a recent statement at the American Bar Association (ABA) Section of International Law 2014 Spring Meeting in New York, former Senator Evan Bayh suggested that “it will probably take a cyberattack succeeding in some way that significantly harms the country before we’ll be able to reconcile the debate in Washington about legislation.” Bayh urged bipartisan support to pass cybersecurity legislation before a serious cyberthreat prompts action.\(^29\)

Without an overarching federal legislative framework in place, it remains “very easy [for companies] to make mistakes” in cybersecurity management, given the “complex patchwork of state, federal, and international laws.”\(^30\)

Experts interviewed for this study tended to echo these concerns. Joseph DeMarco, a partner at the boutique privacy and information security law firm DeVore and DeMarco in New York, observes that the law is lagging behind developments in cybersecurity, and that the lag is growing over time rather than shrinking.\(^31\) Harriet Pearson, of Hogan Lovells believes that the law in its current state is not appropriate to address the consequences of data breaches and other cyberthreats. Pearson asserts that the law needs to evolve, with immunities or limitations of liability for companies dealing with the most “catastrophic” incidents. This requires the creation of a paradigm for cybersecurity that has not yet been established by legislation.\(^32\)

In the absence of federal legislation, experts have identified a number of regulatory or executive influences on cybersecurity law, including the FTC, the SEC, and the NIST Framework. The remainder of this section considers these influences in turn.

**FEDERAL TRADE COMMISSION ACT, SECTION 5**

The United States does not currently have a comprehensive law dealing with data security similar to the Data Protection Directive used by the European Union. Instead, the FTC supplements industry-specific legislation with its broad authority under Section 5 of the

---


\(^{31}\) DeMarco, Phone interview, Op. cit.

Federal Trade Commission Act (15 U.S. Code § 45). Section 5 states that the FTC has the authority to investigate “unfair or deceptive acts or practices in or affecting commerce.” The FTC has used Section 5 to pursue investigations of “unfair” or “deceptive” data security and privacy practices, usually relying on the “deception” aspect more so than claims of “unfairness.”

In order to avoid a Section 5 violation, the FTC suggests that companies adopt a “privacy by design” strategy, offer simplified choices for businesses and consumers about their data, and allow greater transparency of practices. The privacy by design principle encourages companies to consider potential privacy and data security issues at every stage of company, product, or service development. Furthermore, two applied principles support the baseline privacy by design guidance:

- Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.
- Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

Privacy by design is a key principle for general counsel to understand in order to advise companies on ensuring their practices and products or services are consistent with legal requirements, posted privacy policies, product descriptions, and user expectations. The principle is proactive for protecting private information, rather than traditional reactive frameworks, with the understanding that it is harder to “correct architectural deficiencies after rollout.” The FTC also recommends that businesses and policymakers adopt “simplified choice mechanisms that give consumers more meaningful control” over their privacy and make their data practices more transparent.

Jennifer Woods, an attorney with the intellectual property group at Clark Hill PLC, explains that many data security and privacy cases are not solely based on a Section 5 violation, but could be related to other statutes under FTC authority such as the Fair Credit Reporting Act.

---

35 Ibid.
36 Ibid.
and the Children’s Online Privacy Protection Act. The FTC has 60 different sets of laws, rules, and guides that give it authority to pursue privacy and data security violations. Laws are published in the United States Code, while most rules are published in Title 16 of the Code of Federal Regulations.

SEC DISCLOSURE GUIDANCE

In October 2011, the SEC’s Division of Corporation Finance released disclosure guidance for situations related to cybersecurity risks and incidents in response to “more frequent and severe cyber incidents.” No existing disclosure requirement specifically refers to cybersecurity, but other requirements may indirectly compel registrants to disclose the risks and incidents related to cybersecurity. For example, SEC registrants should disclose the risk of cyberthreats if these factors make investment in the company “speculative or risky.” The guidance document states that, depending on the circumstances of a particular registrant, the following risk disclosures may be appropriate:

- Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and,
- Description of relevant insurance coverage.

The Division of Corporation Finance provides further guidance on management’s discussion and analysis of financial condition and results of operations, description of business, legal proceedings, financial statement disclosures, and disclosure controls and procedures. However, the SEC points out that this guidance “is not a rule, regulation, or statement of the Securities Exchange Commission” and represents the views of the Division of Corporation Finance.

Although there have been calls for additional cybersecurity disclosure regulations from the Commission, experts worry about whether the SEC is the right agency to address cybersecurity issues and about how to “strike the right balance” between protecting

---

44 Bulleted points quoted from: Ibid.
45 Ibid.
investors and protecting companies from the adverse consequences of disclosure. At present, SEC commissioners do not appear to be planning additional regulations.46

**NIST FRAMEWORK**

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), a response to the Executive Order from President Barack Obama that tasked it with addressing how to protect critical infrastructure sectors the previous February.47 While the NIST Framework is not a regulation or official standard of care, Ron Plesco, principal at KPMG and a board member of the National Cyber Forensic Training Alliance,48 suggests that it will likely become a “de facto standard of care” through “case law and public opinion.”49 The potential importance of the Framework, however, may not be fully appreciated by practicing lawyers, including inside counsel. A May 2014 survey by Today’s General Counsel revealed that about one-third of respondents had not heard of the NIST Framework, and that another one-third had heard of it but had not reviewed it.50 Only around one-third of respondents had read and planned to use the Framework.51

Critical infrastructure, the core of the NIST Framework’s focus, is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”52 To protect critical infrastructure from cyberthreats, the NIST Framework is recommended for organizations of all sizes, regardless of threat exposure or the sophistication of cybersecurity systems, in recognizing, assessing, and managing risk.53 The NIST Framework provides a common roadmap for organizations to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state; and,

---

50 Ibid.
51 Ibid., p. 47.
53 Ibid.
54 Bulleted points quoted from: Ibid., p. 4.
Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is intended to be flexible and adaptive to serve an array of risk management processes for cybersecurity, including compatibility with other guidance documents like the International Organization for Standardization (ISO) 31000:2009 and ISO/IEC 27005:2011, the NIST Special Publication 800-39, and the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline. The NIST Framework is also applicable to a broad range of sectors – including transportation, financial services, energy and utilities, and the government – although its usage in other industries, like health care, is still uncertain. The Privacy & Information Security practice group at King & Spalding LLP predicts that NIST will continue to work alongside sector-specific agencies and associations to further develop the Framework for implementation in various industries.

Experts interviewed for this study generally do not believe that the NIST Framework will become a dispositive standard of care for corporations. In part, this is because the NIST Framework is currently a voluntary measure for companies. However, the NIST Framework is an important methodological roadmap for planning and implementing a company’s compliance plan. The NIST Framework is one place where a court may look when considering whether a company exercised a standard of care, and though the Framework may not be “dispositive,” it will likely be “influential” in such decisions. In a sense, the Framework may serve as a “gap-filler” for the piecemeal collection of laws that currently relate to cybersecurity concerns.

---

55 Ibid., pp. 5-6.
60 DeMarco, Phone Interview, Op. cit.
HOW LAWYERS HELP MEET CYBERTHREATS

THE ROLE OF LAWYERS IN CYBERSECURITY

WHY SHOULD LAWYERS BE INVOLVED?

As the welter of laws, regulations, and policies touching on cybersecurity suggest, the issue has become as much a legal problem as a technical one. In the past, many companies believed that cybersecurity could be managed primarily by IT staff and risk management. While some may still hold that belief, the question has largely shifted from whether lawyers should be involved in a company’s cybersecurity efforts to when lawyers should become involved. Lawyers are best suited to apply relevant laws to the facts and circumstances of the company, assess compliance, and inform decision-making for companies’ cybersecurity efforts as they relate to the law. Indeed, most of the corporate counsel surveyed for this study are involved to some extent in their company’s cybersecurity efforts, with a majority reporting that they are at least “moderately” involved.

Figure 3.1: Level of Involvement in Cybersecurity by Corporate Counsel

![Bar chart showing involvement level]

Source: Survey of corporate law departments.

However, it seems likely that lawyers should be even more involved in companies’ cybersecurity efforts. Companies may limit their involvement in part due to confusion over roles. Timothy Opsitnick, founder and general counsel for JurInnov, a cybersecurity consulting firm that works with companies and law firms on IT, compliance, and legal issues, points out that company IT and risk management staff often lack “hard stops” for

---

knowing when a cybersecurity matter should be elevated to legal counsel. He explains that “often IT and risk management staff believe that they can handle the legal aspects of cybersecurity, but the better question is: should they be handling it?”67

The NIST Handbook addresses this issue by breaking down computer-based security controls into three functions: technical controls, management controls, and operational controls.68 While an IT unit could manage the technical subset, other controls require procedures, training, and risk assessments for an organization based on the types of information and risks involved.69 Many aspects of cybersecurity are backed up by statutory or regulatory regimes. While IT can safeguard data within a company, IT staff may not be aware of the regulatory requirements associated with data. For these reasons, lawyers have become an integral part of cybersecurity planning, assessment, and management.

However, experts interviewed for this study also stress that legal counsel forms only one part of the broader cybersecurity team, which should include legal, IT, management, and financial experts.70 The challenge of managing cybersecurity within a company is so large and complex that it should not be managed by just one unit.71 Rather, the best cybersecurity management team should be a “collaborative partnership” between several supporting units.72

WHAT ARE LAWYERS DOING?

There are currently many different levels of involvement for lawyers in companies’ cybersecurity efforts, depending in part on the size of the company and its particular circumstances. Generally, experts observe that larger companies are more likely to have lawyers involved, either because they have their own in-house counsel or because they have access to external advisors that smaller companies lack.73 Some companies involve lawyers on a nominal basis to answer a few questions, while others have their own lawyers leading internal cybersecurity efforts, and some companies bring outside legal counsel to perform cyber-compliance reviews on policy and procedure within the company.74

Overall, it is becoming increasingly common for companies to involve legal counsel in cybersecurity matters. This trend is attributable, in part, to increased regulatory pressure on companies to prepare for cyber incidents and to disclose cyber risks and data breaches to consumers. Harriet Pearson commented that lawyers’ involvement in corporate

---

70 Ibid.
cybersecurity has especially increased with regard to data breaches and privacy concerns.\textsuperscript{75} Timothy Opsitnick points out that in cases of theft, such as identity theft, or where there is a clear violation of a regulation, lawyers are “not only common, but essential.”\textsuperscript{76}

Among the corporate law departments surveyed for this study, over 80 percent have participated in at least one type of cybersecurity-related action or precaution. The most common step taken by the companies surveyed is also the one that the most law departments have performed: preparing an information or data security policy. Notable amounts of respondents have also participated in employee training or cybersecurity audits. Also notable, however, is that most companies that have experienced a data breach involve their general counsel in the response; although a minority of companies surveyed have experienced such a breach, a majority of these (76 percent) involved the law department in the response.

This points to an important conclusion that emerged in the interviews conducted for this study: companies are more likely to involve lawyers as a \textit{reactive} measure, after an incident has occurred, rather than as a \textit{proactive} measure.\textsuperscript{77} SEC Commissioner Luis Aguilar made a similar point in a June 2014 speech at the “Cyber Risks and the Boardroom” Conference in New York:\textsuperscript{78}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure3_2.png}
\caption{Cybersecurity Steps Involving Corporate Counsel}
\end{figure}

\textsuperscript{75} Pearson, Phone interview, Op. cit.
\textsuperscript{76} Opsitnick, Phone interview, Op. cit.
\textsuperscript{77} Budish, Ryan. Fellow, Berkman Center for Internet and Society, Harvard University. Phone interview. July 18, 2014.
Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. Yet, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues... In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management.

Timothy Opsitnick explains this in part by noting that compliance and IT units are more likely to drive the proactive measures, while lawyers drive the reactive responses to an incident. Most companies bring in legal counsel after experiencing either a major or minor crisis situation. An example of a “minor crisis” would be a company receiving a grievance from a business partner about meeting particular cybersecurity requirements; lawyers might be brought on board to bring the company’s procedures up to standard with the partner’s requested requirements. A “major crisis” would be a large-scale data security breach.

Despite these practices, however, at least one expert interviewed for this study has observed a trend toward increasingly proactive involvement for legal counsel, partly as a result of the increased attention to cybersecurity by regulatory bodies like the SEC. This trend may be reflected in the responses of corporate law departments when asked whether their cybersecurity involvement tends to be proactive or reactive. For most, it is both, with a relatively small proportion (22 percent) reporting only a reactive involvement.

---

**WHAT SHOULD LAWYERS BE DOING?**

Legal counsel may take on many roles in advising companies on cybersecurity matters. Primarily, legal counsel must understand the “patchwork” of laws that govern cybersecurity matters at the state and federal levels, including sector-specific legislation, and be able to communicate this information with stakeholders. More specifically, Harriet Pearson suggests a 10-point cybersecurity agenda for corporate counsel (Figure 3.4).

---

**Figure 3.3: How Companies Involve Lawyers in Cybersecurity**

Does your company tend to involve lawyers as proactive or reactive measures to cybersecurity?

<table>
<thead>
<tr>
<th></th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>16%</td>
</tr>
<tr>
<td>Reactive</td>
<td>22%</td>
</tr>
<tr>
<td>Both</td>
<td>53%</td>
</tr>
<tr>
<td>Don't know/not applicable</td>
<td>9%</td>
</tr>
</tbody>
</table>

Source: Survey of corporate law departments.

---

82 Ibid.
Table: Pearson’s 10-Point Agenda for Corporate Counsel

<table>
<thead>
<tr>
<th>Agenda Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fulfill Fiduciary Duty of Board and Management</td>
<td>If a cybersecurity incident occurs, a company will need to be able to prove they have met their duty for safeguarding company stock price and assets. A protocol to fulfill this duty should be a part of an effective cybersecurity plan.</td>
</tr>
<tr>
<td>2. Address Disclosure Obligations and Appropriate Communications</td>
<td>Training employees on effective internal and external communication during a cybersecurity incident can prevent escalating the issue further. Early attention and training on communicating factually without speculation and establishing channels for seeking assistance can serve a company well.</td>
</tr>
<tr>
<td>3. Guide Participation in Public-Private Partnerships and Law Enforcement Interactions</td>
<td>Industry and government forums for sharing threat information, response strategies, and cybersecurity best practices can be a useful part of a company’s cybersecurity program. However, there should be a strategy for company participation and training for individuals involved to reduce risk and avoid conflicts with clients or government authorities.</td>
</tr>
<tr>
<td>4. Achieve Regulatory Compliance</td>
<td>Companies should assess the regulations relevant to its circumstances, including federal and state-level data security and breach notification laws. However, avoid overinvesting in “check-the-box” compliance efforts that may hinder more effective cybersecurity measures.</td>
</tr>
<tr>
<td>5. Provide Counsel to Cybersecurity Program</td>
<td>Companies should appoint or identify legal counsel to become familiar with the security program and legal issues potentially raised by its implementation. These individuals should be prepared to bring any policy issues or potential legal risks to senior management or the board.</td>
</tr>
<tr>
<td>6. Prepare to Handle Incidents and Crisis</td>
<td>Counsel can help prevent escalation of an incident to a crisis by helping guide sessions to prepare the company with a plan of action for incident response. Identify key internal and external resources for managing incident response, consider involving senior management in a tabletop exercise, and consider in advance what legal issues are implicated during an incident.</td>
</tr>
<tr>
<td>7. Manage Cybersecurity-Related Transactional Risk</td>
<td>Mergers and acquisitions, vendor/supplier contracts, and consumer/client contracts can all implicate cybersecurity-related risk. Create a due diligence checklist and approach to cybersecurity issues, review contractual provisions, and review the vendor oversight program to integrate cybersecurity risk considerations into approach.</td>
</tr>
<tr>
<td>8. Effectively Use Insurance</td>
<td>Insurance can be a valuable way to protect a company, but the exclusions and conditions of the insurance should be examined carefully. Cybersecurity insurance products have improved since their first introduction to the market a decade ago.</td>
</tr>
<tr>
<td>9. Monitor and Strategically Engage in Public Policy</td>
<td>Stay informed of developing policy standards, engage in advocacy via industry associations, and engage in conversations on key issues so that policymakers and industry leaders are aware of company positions and concerns.</td>
</tr>
<tr>
<td>10. Discharge Professional Duty of Care</td>
<td>Corporate and outside counsel should take precautions to protect client and related information, particularly when using or relying upon e-mail, social media, cloud, and other digital capabilities.</td>
</tr>
</tbody>
</table>

Source: “Cybersecurity: The Corporate Counsel’s Agenda.”

To gauge the extent to which corporate counsel have taken on this agenda, Hanover asked law departments whether they have performed any of these tasks. Again, results suggest that general counsel have significant room for improvement in addressing cybersecurity. The highest rate of implementation for any agenda item is only 53 percent, and nearly one-fifth of respondents have not taken on any of these tasks. Expectedly, crisis preparedness and regulatory compliance rank highly, while less immediate tasks – such as using insurance or engaging in public policy – are less commonly addressed.

---

Figure 3.5: Engagement with Pearson’s Ten-Point Agenda

<table>
<thead>
<tr>
<th>Agenda</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare to handle incidents and crises</td>
<td>53%</td>
</tr>
<tr>
<td>Address disclosure obligations and appropriate communications</td>
<td>48%</td>
</tr>
<tr>
<td>Achieve regulatory compliance</td>
<td>46%</td>
</tr>
<tr>
<td>Manage cybersecurity-related transactional risk</td>
<td>43%</td>
</tr>
<tr>
<td>Discharge professional duty of care</td>
<td>37%</td>
</tr>
<tr>
<td>Fulfill fiduciary duty of board and management</td>
<td>32%</td>
</tr>
<tr>
<td>Effectively use insurance</td>
<td>28%</td>
</tr>
<tr>
<td>Monitor and strategically engage in public policy</td>
<td>22%</td>
</tr>
<tr>
<td>Provide counsel to cybersecurity program</td>
<td>13%</td>
</tr>
<tr>
<td>Guide participation in public-private partnerships and law enforcement interactions</td>
<td>10%</td>
</tr>
<tr>
<td>None of the above</td>
<td>17%</td>
</tr>
</tbody>
</table>

Source: Survey of corporate law departments.

KNOWLEDGE AND SKILLSETS FOR CYBERLAWYERS

WHAT LAWYERS NEED TO KNOW

Experts interviewed for this study identified three main areas of knowledge that lawyers working in cybersecurity could improve on: **legal knowledge**, **technical knowledge**, and **communication skills**. Surveyed corporate counsel largely agree. Corporate counsel most commonly select legal knowledge and technical knowledge as the two areas in which it would be "most beneficial" for lawyers to receive cybersecurity training.
Regulatory knowledge is central to lawyers involved in a company’s cybersecurity efforts. Foundational regulations are driving most companies’ efforts, so an understanding of the “quilt” of regulations and standards that apply to a company is a major component of legal counsel’s responsibility.  

Harriet Pearson suggests that legal issues associated with information sharing and incident response; privilege assertion; legal issues with law enforcement interaction; active defense measures; and public disclosure about cybersecurity events and risks are just a few areas in which knowledge and awareness could be improved.

However, cybersecurity goes beyond regulatory law, encompassing private contracts as well. Harriet Pearson notes, for instance, that the trend toward companies contracting out business processes to different organizations sets up the potential for a broad base for legal activity regarding cybersecurity incidents. The cyberlaw industry will be faced with sorting out the responsible parties when data breaches or other cyberthreats occur in companies outsourcing business processes to other organizations.

For similar reasons, David Bodenheimer recommends that legal education integrate information security into the curriculum for contract law. Many cybersecurity issues result from business-to-business contracts rather than statutes or regulations, and lawyers need to be aware of basic information security concerns when working with contractual

---

86 Ibid.
agreements between clients. Bodenheimer also suggests that facets of cybersecurity law could be integrated elsewhere in the law school curriculum, such as in ethics courses, as mishandling information security can put a lawyer at risk of malpractice or may damage client relations.

Basic technical training in cybersecurity is also an important area for lawyers to build knowledge, although many experts stress that detailed technology expertise is not necessary. A recent ABA Commission on Ethics also noted that lawyers have a responsibility to stay informed of technology developments and risks. Along those lines, Harriet Pearson notes that lawyers should be able to “sort the wheat from the chaff” in terms of the types of cybersecurity threats that a company may face.

Ryan Budish, a fellow at the Berkman Center for Internet and Society at Harvard University, adds that lawyers need a certain degree of technical knowledge to understand if they are actually meeting the legal standards set out. Basic knowledge of cybersecurity can help lawyers to communicate with IT staff and “ask the right questions” about potential concerns. However, Timothy Opsitnick cautions that technology is evolving so quickly that it would be unfeasible for lawyers to stay informed on the technical details of the cybersecurity field; although he believes that the demand justifies building an educational practice around a cyberlaw specialty, he suggests that such a program should not focus too much on the technical side of cybersecurity.

Finally, several experts emphasize the value of communication skills for explaining cybersecurity issues to non-experts. Lawyers are responsible for translating cybersecurity laws and policies for their clients, helping them understand how the laws relate to their particular circumstances, and explaining the trade-offs of various approaches.

HOW LAWYERS LEARN ABOUT CYBERSECURITY

Experts note that there is an immense amount of information on cybersecurity and legal practice available to lawyers through the ABA, government websites, private newsletters, and many conferences. The Congressional Cybersecurity Caucus provides weekly updates of developments in the public sector, and the Georgetown Cybersecurity Law Institute is

---

an important resource for keeping up with developments in cybersecurity law. The ABA publications and the annual Georgetown Cybersecurity Law Institute may be the best sources for holistic coverage of cybersecurity developments, while conferences and specialist publications provide information on particular issues like privacy issues or cyber-insurance.

In practice, no one source of information on cybersecurity predominates among lawyers. When asked which source they use, corporate counsel responding to the survey conducted for this study were almost equally likely to select various options, including newsletters, conferences, and government websites. Encouragingly, roughly two-thirds of respondents consult at least one of these sources to learn about cybersecurity.

Figure 3.7: How Lawyers Learn About Cybersecurity

![Graph showing the sources of information used by lawyers to learn about cybersecurity.](source)

Source: Survey of corporate law departments.

However, despite the abundance of information, some of the experts consulted for this study feel that lawyers are still not sufficiently informed about cybersecurity issues. Ryan Budish points out that while there are some well-trained experts, most lawyers probably do not have the adequate knowledge to address issues in cyberlaw. Practicing lawyers seem to agree; when asked about the importance of improving formal education and training in

---

97 Pearson, Phone interview, Op cit.
the field, corporate counsel responded affirmatively, with over two-thirds rating such improvement “very” or “extremely” important.

Figure 3.8: Importance of Formal Education and Training in Cybersecurity

In-house legal counsel may be better informed on cybersecurity issues within a company. In-house counsel are more in tune with the cybersecurity issues companies are facing and have inside knowledge of their company’s particular cybersecurity challenges and vulnerabilities. Outside counsel can be “divorced from the reality of what’s going on” with corporate cybersecurity, unless they are one of the few lawyers who have frequent involvement with the same companies. Still, in-house corporate counsel will often bring in outside counsel to augment their skills and knowledge on the most difficult issues.

---

**METHODOLOGY**

To develop the findings of this paper, interviews were conducted during the second half of 2014 with lawyers, consultants, and academics knowledgeable in the intersection of law and cybersecurity. These interviewees are cited directly throughout this paper.

In addition to these in-depth interviews, an online survey of corporate law departments was administered in November 2014. Of the 149 individuals who took the survey, most respondents (89 percent) work as attorneys in their employer’s law department or general counsel’s office, with the remainder working as paralegals or in other positions. As shown below, around half of respondents work in companies with more than 700 employees, with the rest distributed more or less evenly across a range of sizes.

**Size of Companies Surveyed**

Approximately how many employees does your company/corporation employ?

<table>
<thead>
<tr>
<th>Employee Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 or less</td>
<td>17%</td>
</tr>
<tr>
<td>51-100</td>
<td>7%</td>
</tr>
<tr>
<td>101-250</td>
<td>7%</td>
</tr>
<tr>
<td>251-500</td>
<td>11%</td>
</tr>
<tr>
<td>501-700</td>
<td>5%</td>
</tr>
<tr>
<td>More than 700</td>
<td>52%</td>
</tr>
</tbody>
</table>
PROJECT EVALUATION FORM

Hanover Research is committed to providing a work product that meets or exceeds partner expectations. In keeping with that goal, we would like to hear your opinions regarding our reports. Feedback is critically important and serves as the strongest mechanism by which we tailor our research to your organization. When you have had a chance to evaluate this report, please take a moment to fill out the following questionnaire.


CAVEAT

The publisher and authors have used their best efforts in preparing this brief. The publisher and authors make no representations or warranties with respect to the accuracy or completeness of the contents of this brief and specifically disclaim any implied warranties of fitness for a particular purpose. There are no warranties that extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by representatives of Hanover Research or its marketing materials. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein may not be suitable for every partner. Neither the publisher nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Moreover, Hanover Research is not engaged in rendering legal, accounting, or other professional services. Partners requiring such services are advised to consult an appropriate professional.