

Reproduced with permission from Privacy & Security Law Report, 11 PVL 1792, 12/17/2012. Copyright © 2012 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## Cybersecurity: The Corporate Counsel's Agenda



BY HARRIET PEARSON

### Introduction

#### Imagine this scenario:

**T**he corporate IT director reports that malware has been discovered on your company's computer systems, and it is likely that business plans and intellectual property of the company, as well as sensitive personal information, have been exposed. U.S. state data security breach notification laws have been triggered and, once the required notices go out, media inquiries and letters from the Federal Trade Commission and state attorneys general arrive, seeking information about the incident and the company's cybersecurity practices. A letter comes from a prominent legislator asking questions about the incident. Corporate partners inquire about contractual data security and privacy obligations and the potential impact of the incident on their systems, data, and business. It is time for a regular Securities and Exchange Commission filing,

Harriet Pearson is a partner with Hogan Lovells US LLP in Washington where her practice focuses on privacy and cybersecurity. Pearson previously served as IBM's first global chief privacy officer and security counsel, responsible for information policies and practices affecting over 400,000 employees and thousands of business clients. She acknowledges the helpful reviews of this paper by Hogan Lovells colleagues Christopher Wolf, Deen Kaplan, Paul Otto and Jeffrey Lolley.

which requires evaluating whether to report the incident as a material risk. Shareholder representatives and plaintiffs' lawyers are organizing themselves to pursue actions related to the incident and its effect on the company, its operations and revenues, and individuals' privacy. And the Board wants to know what steps the Office of General Counsel has taken to assess and mitigate the legal risks.

This not-so-improbable scenario, and others like it, makes it imperative for corporate counsel to focus (or refocus) on the issues surrounding cybersecurity.

"Cybersecurity," simply put, is whether and how electronic data and systems are protected from attack, loss, or other compromise.<sup>1</sup> Signaling the degree to which cybersecurity-related concerns now occupy senior government officials, on Sept. 19, Senate Commerce, Science, and Transportation Committee Chairman John D. Rockefeller IV (D-W.Va.) personally contacted the chief executives of America's 500 largest companies to ask about their company's cybersecurity practices and their views on the role of the federal government to help protect commercial critical infrastructure.<sup>2</sup>

For business, Sen. Rockefeller's letter was only the latest cybersecurity-related development in the legislative, judicial, and regulatory spheres. U.S. government efforts to address the inherent vulnerability of computerized systems began in earnest in the 1990s, intensified in recent years, and will continue to progress in 2013 and beyond.<sup>3</sup> And while the United States seems

<sup>1</sup> A broader and more-nuanced definition can be found in the Obama Administration's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009) (8 PVL 795, 6/1/09), available at [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

<sup>2</sup> Industry sectors typically considered "critical infrastructure" include transport, telecommunications, energy, and financial systems, but the scope of what ultimately is included varies and is frequently subject to considerable discussion. For more on Sen. Rockefeller's inquiry, see Harriet Pearson & Lance Bultena, Senate Commerce Committee's Probe of Fortune 500 Corporate Cybersecurity Is Unprecedented, Hogan Lovells Focus on Regulation (Sept. 26, 2012), <http://www.hlregulation.com/2012/09/26/>.

<sup>3</sup> For example, prior to year's-end President Obama is widely expected to issue an Executive Order directing agency-industry work to develop recommended cybersecurity practices for key industries (11 PVL 1680, 11/19/12). See, e.g.,

to have taken the lead among governments to address these issues, particularly as it relates to the private sector's role, other nations also now are engaged.<sup>4</sup>

The frequency and severity of cybersecurity incidents involving business have increased in recent years,<sup>5</sup> triggering the governmental activity. Ongoing efforts by both the private and public sectors to prevent and address incidents raise two key questions:

- What constitutes a reasonable corporate defense and response?
- Which public or other authorities are in a position to guide and sanction corporate cybersecurity activities?

So it comes as no surprise that these issues have taken on new importance for senior corporate leaders. For example, a recent survey of 1,957 general counsel and 11,340 corporate directors indicated that cybersecurity and data protection for the first time rank as top-of-mind concerns, edging out perennial priorities like operational risk and Foreign Corrupt Practices Act compliance.<sup>6</sup> But now that the issues are on boards' radar screens, how should limited corporate resources best be directed so that key business assets are protected and legal and other risks are minimized? Unsurprisingly given the emerging nature of the challenge, the answer to how businesses—and their counsel—should address cybersecurity-related risk is evolving.

## The Cybersecurity Landscape

Consider some telling statistics. Internet access has grown from 361 million users in 2000 to 2.4 billion users in 2012.<sup>7</sup> The volume of digital data created in just the next two days will be more than that created from the dawn of history to the year 2003.<sup>8</sup> Instrumentation of more and more “things” that communicate and connect to each other opens up opportunities to make

Jennifer Martinez, White House to Meet Industry Groups on Cyber Order, The Hill (Oct. 17, 2012, 12:58PM), <http://thehill.com/blogs/hillicon-valley/technology/262573-white-house-to-meet-with-industrygroups-on-cyber-order>.

<sup>4</sup> Comprehensive national cybersecurity strategies that include a role or responsibility for the private sector have been or are under development in key markets such as the United Kingdom, Canada, and Australia. Countries such as India, China and Russia have taken significant and sometimes controversial steps to protect domestic critical infrastructures. And multi-jurisdictional entities such as the OECD and the European Union also are deliberating on measures that they can take in this area. See, e.g., Neelie Kroes, Vice-President of the European Commission, Securing Our Cyber-World, Address at the Top Level Conference on Cyber Security of Industrial Control Systems and Smart Grids/Amsterdam (Oct. 16, 2012), available at [http://europa.eu/rapid/press-release\\_SPEECH-12-732\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-12-732_en.htm). (11 PVL 1512, 10/15/12).

<sup>5</sup> See *infra* note 11.

<sup>6</sup> Corporate Board Member & FTI Consulting, Inc., 2012 Law and the Boardroom Study: Legal Risks on the Radar (Aug. 2012), available at <http://www.fticonsulting.com/global2/critical-thinking/reports/legal-risks-on-the-radar.aspx>.

<sup>7</sup> See Internet World Stats, Usage and Popular Statistics, <http://www.internetworldstats.com/stats.htm> (last visited Dec. 13, 2012).

<sup>8</sup> Estimate according to Google is consistent with other similar such estimates. See MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003*, TechCrunch (Aug. 4, 2010), <http://techcrunch.com/2010/08/04/schmidt-data/>.

whole systems—such as transport or the energy grid—more automated and responsive.

Cloud computing enables data to be processed off-premises more easily and inexpensively, making it an attractive computing option for many types of organizations. The consumerization of technology means that many of your employees want to use their smartphones and other devices for work and may already be doing so, even if your company has not yet developed a bring-your-own-device program. And many internet users are engaged in social networking of some type, for both work and play.

The fact that these technologies have rapidly become embedded in key parts of the economy and are now viewed as indispensable by most is a key reason why cybersecurity is now a national and economic security issue, as noted by the White House:

Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life.

9

The pervasiveness of these information and communications technologies means that the private sector—which in the United States owns and operates 85 percent or more of the critical infrastructure<sup>10</sup>—is now vulnerable to a wide range of cyber-related risks.

Several factors contribute to this vulnerability:

- Many technologies now in use were not engineered with a major focus on security when first released, yet they have now been pressed into service for mission-critical operations.
- Many technologies, when first installed, operated in an environment in which the major sources of known risk were careless insiders, hobbyist hackers, and petty cybercriminals.
- And before 2005 or so, relatively few regulatory requirements imposed specific obligations to protect sensitive information or to report data security breaches.

It is now widely understood, however, that organized cybercriminals and geopolitically motivated actors are targeting multiple industries to steal data and to attempt to plant the seeds of disruptive future attacks.<sup>11</sup>

<sup>9</sup> See White House, Cybersecurity, <http://www.whitehouse.gov/cybersecurity> (last visited Dec. 13, 2012).

<sup>10</sup> Estimates of private-sector ownership of the so-called critical infrastructure vary, but in the United States the figure usually cited is 85 percent or more. See, e.g., Dep't of Homeland Security, Critical Infrastructure Sector Partnerships, <http://www.dhs.gov/critical-infrastructure-sector-partnerships> (last visited Dec. 13, 2012). In countries in which the electricity grid, communication networks and broader energy sector are nationalized, the government may own and operate the majority of the most critical systems.

<sup>11</sup> Industry and university reports on the cyber-risk landscape abound. See, e.g., Symantec, Internet Security Threat Report: 2011 Trends (April 2012) (11 PVL 813, 5/14/12), <http://www.symantec.com/threatreport/>; McAfee Labs, 2012

Further complicating the landscape for business, data security and privacy laws in the United States already explicitly apply to companies, including those in key sectors such as financial services, health care, and energy. Perhaps the most significant such laws—because they bring relatively minor incidents to the attention of enforcement agencies, media, and potential plaintiffs—are the now pervasive state and federal laws requiring disclosure of the suspected compromise of sensitive personal information, such as Social Security numbers or health-related data. In addition to private plaintiffs’ attempting to claim damages from security breaches involving data about them, enforcement agencies such as the Federal Trade Commission increasingly pursue companies who have experienced a security breach, claiming that cybersecurity programs insufficient to prevent a cyber-attack violate the FTC Act and other authorities.<sup>12</sup>

A wide array of new cybersecurity, data security, and related privacy legislation also was pursued in the most recent Congress; while nothing passed both chambers, the White House and committed Congressional leaders have already stated their intentions to continue efforts to drive further action by the private sector, given the severity of cyberthreats to U.S. national security. Measures likely to be introduced and considered include those that would: facilitate greater industry-government information sharing (e.g., by offering liability protection); set national standards for data breach notification; and promote (or perhaps, if a crisis occurs, mandate) certain measures to be taken by the private sector to protect critical industry sectors such as transportation, communications, and financial services.

Perhaps the most telling recent development, in terms of signaling the maturation of this issue as a board-level topic, was the SEC’s issuance of disclosure guidance in October 2011.<sup>13</sup> The SEC explained that

Threats Predictions, <http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf>; Georgia Tech, Emerging Cyber Threats Report 2013 (2012), <http://www.gtiscsecuritysummit.com/pdf/2013ThreatsReport.pdf>; IBM X-Force 2012 Mid-Year Trend and Risk Report (Sept. 2012), <http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF>; Verizon, 2012 Data Breach Investigations Report, [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf).

<sup>12</sup> Since 2005, the FTC has brought more than thirty-five data security cases charging companies or individuals with violations of the FTC Act, imposing remedies that frequently include long-term FTC oversight and corporate commitment to a revamped data security and privacy program. For a current listing of such cases, see FTC Bureau of Consumer Protection, Business Center, <http://business.ftc.gov/legal-resources/29/35> (last visited Dec. 13, 2012). In the first judicial challenge to the FTC’s authority to pursue such actions, Wyndham Hotels and its amici have argued that the Commission has exceeded its statutory authority under the “unfairness” prong of the FTC Act (11 PVLR 1335, 9/3/12)—but even invalidation of that element of its authority would leave the FTC with considerable ability to pursue “deceptive practices” and potentially for it or Congress to reframe its unfairness authority. See Brief of U.S. Chamber of Commerce, Retail Litigation Center and American Hotel & Lodging Association as Amici Curiae Supporting Defendants, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX PGR (D. Ariz. Oct. 5, 2012), available at <http://op.bna.com/pl.nsf/r?Open=dapn-92xvvy>.

<sup>13</sup> Division of Corporation Finance, SEC, CF Disclosure Guidance: Topic No. 2: Cybersecurity (Oct. 13, 2011) (11 PVLR

public companies should disclose the risk of cyber-incidents if such risks may materially affect a registrant’s products, services, relationships with customers or suppliers, or competitive conditions, or they would render investment in the company speculative or risky. While the 2011 guidance is not binding and interprets existing legal obligations, all thirty of the Dow 30 companies discussed cybersecurity or data breaches in their 2012 Form 10-K risk factor disclosures.<sup>14</sup>

With such legislative and regulatory focus, it is not surprising that 2012 marked the first time that general counsel and corporate board members ranked cybersecurity and data security as their number one issue of concern.<sup>15</sup>

An excerpt from the 2012 Law and the Boardroom Study notes that:

Today, there is arguably no more insidious threat to a public company than that of cyber risk; it’s invisible, ever-changing, and pervasive—making it very difficult for boards to manage . . . [The] level of concern has nearly doubled in the last four years: In 2008, only 25% of directors and 23% of GCs [general counsel] noted data security as an area of high concern.

<sup>16</sup>

A strong consensus thus has emerged in the United States that neither the private sector nor government is doing enough. It is now a given that more must be done to protect key operations and data against cyberthreats.<sup>17</sup> The concern is growing. And the U.S. concern has prompted other national governments to begin similar efforts and dialogues with industry efforts that have the potential to create inconsistent and even conflicting requirements for international companies.<sup>18</sup>

## A Ten-Point Agenda for Corporate Counsel

Companies can and should take a range of actions in advance of a cyber-incident. The business rationale for doing so is clear; an effective program that adjusts to address new risks is a must to protect against data loss,

1742, 12/3/12), <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

<sup>14</sup> Hogan Lovells research (Dec. 13, 2012).

<sup>15</sup> See 2012 Law and the Boardroom Study, *supra* note 6, at 2.

<sup>16</sup> *Id.*

<sup>17</sup> The lack of information on the full range of corporate responses to cybersecurity risk is perhaps not surprising given the sensitivity of these issues. Thus reports based on even very limited survey samples are widely cited as proof that corporate boards and management are inattentive to cybersecurity risk. See, e.g., Jody Westby, *Boards Are Still Clueless About Cybersecurity*, *Forbes* (May 16, 2012, 10:18AM), <http://www.forbes.com/sites/jodywestby/2012/05/16/boards-are-still-clueless-about-cybersecurity/> (citing Jody Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report* (May 16, 2012) (11 PVLR 411, 3/5/12), available at <http://op.bna.com/pl.nsf/r?Open=dapn-92xvvy>).

<sup>18</sup> A full treatment of this issue, and its potential to create trade barriers, is beyond the scope of this article. For an example of how the issue can manifest in a significant manner, consider the Indian government’s attempts to protect its communications infrastructure by imposing sourcing standards meant to increase supply chain security. See Joji Thomas Philip & Kalyan Parbat, *India Impact Seen on Results of Global Telecomm Gear Firms*, *Economic Times* (Aug. 20, 2010, 6:55AM), [http://articles.economicstimes.indiatimes.com/2010-08-02/news/27621923\\_1\\_telecom-gear-chinese-vendors-security-concerns](http://articles.economicstimes.indiatimes.com/2010-08-02/news/27621923_1_telecom-gear-chinese-vendors-security-concerns).

intellectual property theft, and operational disruption. And the presence of an effective cybersecurity program is likely required or expected by regulators or other key constituents (such as investors)—or shortly will be.

No doubt, much of the needed work inside companies will be done by Information Technology (IT) Security and related technical and business personnel. But particularly because the environment is dynamic—and the standard of care not well understood—the role of counsel is vital and strategic.

This much is clear: As with other areas of legal risk, having and documenting a compliance program can reduce the potential liability from even a single incident.<sup>19</sup> Given that a body of cybersecurity baseline best practices and standards exists, counsel can play a key role to help the organization identify and implement such practices, and document those steps.

The Ten-Point Agenda offered below is designed to help in-house attorneys develop their own effective approaches to cybersecurity. The Agenda draws on the practical experiences of multiple organizations and considers a wide array of legal, regulatory, and policy developments in the United States and other nations. While it will no doubt evolve, the Agenda offers a good starting yardstick against which corporate counsel can assess their own cybersecurity-related actions.

## 1. Fulfill Fiduciary Duty of Board and Management

In the event of a cybersecurity-related incident, some commentators have observed that lawsuits might challenge whether corporate board and management have met their fiduciary and statutory duty to safeguard the company's stock price and assets.<sup>20</sup>

A documented and generally effective cybersecurity program can, as discussed previously, assist in the defense of such claims. While a detailed description of what such a program looks like is beyond the scope of this article, the key questions an organization's senior leadership should be able to ask itself, and answer satisfactorily, include:

- Does our organization fully understand its cybersecurity risk profile and related legal obligations?
- Is a sufficiently skilled cybersecurity leadership team in place to support our organization's risk profile and strategy? Is it a multi-disciplinary team involving the IT organization, physical security (since, for example, a cyber-attack or data breach can be facilitated by unauthorized physical access to key persons or assets), human resources, enterprise risk, compliance, communications (for crisis response)—and legal?

<sup>19</sup> The U.S. Sentencing Guidelines set out the key elements of corporate compliance programs, the existence of which can demonstrate institutional commitment to compliance and thus reduce the potential liability associated with a single incident. Lawyers and compliance officers frequently help design, guide and implement corporate compliance programs that are consistent with the recognized Guidelines. See U.S. Sentencing Guidelines Manual § 8B2.1 (2012) (outlining the requirements of an effective compliance and ethics program).

<sup>20</sup> See, e.g., Westby, *supra* note 17. Claims might arise under the general fiduciary duty to protect assets, under the Sarbanes-Oxley obligation to provide meaningful assurance about the security of information assets, and under numerous specific data security laws.

- Are our resources allocated such that our highest value assets are protected?
- Is the program documented sufficiently?
- Are cybersecurity measures and thinking embedded and integrated throughout the business (i.e., before key data or assets are moved, or new initiatives undertaken, are cybersecurity-related risks and obligations considered)?

### Recommended Actions:

- Assess cybersecurity legal, policy, regulatory, and reputational risk landscape. Ensure consultations involve experts with direct visibility to cyber-attack patterns and sources, as the methods and targets of these evolve quickly.
- Confirm that organization's enterprise risk management program has considered all relevant cybersecurity risks, including legal and policy risks identified.
- Confirm that enterprise security program meets standard of care expected of the organization given its industry and maturity: Are the most important assets protected? Are the fundamentals in place?
- Ensure periodic update of cybersecurity risk assessment, given dynamic environment.

## 2. Address Disclosure Obligations and Appropriate Communications

In the United States, the SEC's recent guidance on cybersecurity-related disclosure has helped focus public attention on whether and how public companies are communicating cybersecurity-related issues to investors and other interested constituents.<sup>21</sup>

Particularly but not exclusively because of this consideration, cybersecurity-related internal and external communications by employees and other individuals associated with a public company should be done with discipline, for example with the benefit of training on how to communicate factually and without speculation. The ease with which inappropriate communication can spread in today's social media-rich environment, as well as the temptation created for potential whistleblowers by the Dodd-Frank Wall Street Reform and Consumer Protection Act, suggests that early attention to and guidance on appropriate communications will serve the company well.

### Recommended Actions:

- In light of SEC Guidance on this topic, review 10-K and other relevant public filings of the organization and its peer companies (in terms of industry, size and sophistication).
- Evolve the organization's public filings and other communications as necessary.
- Train Investor Relations, Communications, IT Security team (especially first responders and incident teams), and other personnel likely to have cybersecurity-related information to communicate only factually and to seek help when needed.

<sup>21</sup> Recent business press speculated about data compromises at prominent companies such as Coca-Cola that were not reported to shareholders. See Ben Elgin et al., *Coca-Cola Gets Hacked and Doesn't Tell Anyone*, Bloomberg News (Nov. 4, 2012, 6:01PM), <http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html>.

### 3. Guide Participation in Public-Private Partnerships and Law Enforcement Interactions

Participation in appropriate industry and government-industry fora is recognized as a useful part of an organization's cybersecurity program. Such initiatives allow for the sharing of threat information and response strategies, as well as best practices. Frequently law enforcement will be involved in such initiatives, or will get involved in a bilateral discussion with a company during the course of an investigation.

Company personnel who are likely to participate in such initiatives should be trained, per Agenda Item 2 above, on how to protect company confidential information and interests while engaging in these fora. Furthermore, the organization should have a strategy for its participation in such fora that optimizes its investment and avoids conflicts with, for example, governmental clients or authorities in its global markets.

#### *Recommended Actions:*

- Review and confirm whether the company's industry and government information-sharing partnership strategy is sound, and managed to benefit the organization (and will not put it at undue risk). Questions to ask include: Who is engaged? With whom? What information is being shared? What is done with incoming information?
- Update information-sharing protocols to include legal oversight and training of relevant personnel.
- Appoint or identify legal counsel to assist with issues arising out of industry or law enforcement interactions.
- Ensure appropriate personnel have law enforcement contacts and relationships before an urgent situation requires them.

### 4. Achieve Regulatory Compliance

Depending on an organization's industry and geographic presence, a number of data security and privacy laws and regulations may apply to it, such as the Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act, the Gramm-Leach-Bliley Act, and state-level data security and data breach notification laws. While an effective regulatory compliance program is helpful to avoid broader types of liability, at the same time organizations should avoid over-investing in check-the-box compliance efforts to the detriment of risk-based cybersecurity measures that may be more effective.

#### *Recommended Actions:*

- Assess security-related regulatory compliance obligations.
- Assess sufficiency and efficiency of existing regulatory compliance efforts; streamline as needed.
- For compliance with breach notification laws, ensure training and preparation of incident response team and confirm that process followed is fully coordinated with (if not part of) cyber-incident responses.

### 5. Provide Counsel to Cybersecurity Program

As organizations evolve their cybersecurity programs, they frequently implement additional measures that may, in some or many jurisdictions, require legal

analysis or prudential measures that would benefit from counsel's involvement. For example, a desire to conduct more robust network and systems monitoring may raise employee privacy and industrial relations issues. Another example: Security-related policies and practices contemplated for bring-your-own-device programs should be reviewed by counsel for various legal issues, including but not limited to privacy.

#### *Recommended Actions:*

- Appoint or identify legal counsel to become familiar with the security program and legal issues potentially raised by its implementation.
- Be prepared to bring novel issues of policy and legal risk to senior management team and/or board.

### 6. Prepare to Handle Incidents and Crises

No security program is perfect; incidents will take place. The key to handling them well is preparation that can prevent an incident from becoming a crisis. Counsel is an essential part of a security response team and should participate and help guide periodic tabletop sessions that help prepare the organization. Legal-specific issues that bear advance planning include considering when and how the attorney-client privilege will be asserted in the event of an incident and how incident documentation will occur and be retained.

#### *Recommended Actions:*

- Appoint or identify legal counsel to participate in and counsel the incident response team and process. They should be or become familiar with cybersecurity concepts, fact patterns, and terms.
- Identify and qualify further key internal and external resources (e.g., forensics, outside counsel, communications).
- Ensure the team and process are exercised regularly to prepare for incidents. Consider involving senior management in a tabletop exercise.
- Consider in advance key legal issues particularly implicated during an incident, such as when to use attorney-client privilege; when and how to escalate communications to senior management; and what criteria should be used to disclose an incident.

### 7. Manage Cybersecurity-Related Transactional Risk

At least three major types of transactions implicate cybersecurity-related risk:

- Mergers and acquisitions in which assets to be acquired or disposed may have cybersecurity-related risks that should be understood and addressed (e.g., a cybersecurity program in need of updating; the existence of prior incidents that probably compromised key intellectual property or other assets; or pending litigation or other actions associated with a cybersecurity incident).
- Vendor/supplier contracts should include provisions that establish the responsibility of parties for safeguarding the relevant systems and data. If warranted, supply chain security provisions may be explored, if product integrity is a significant issue in the industry.
- Customer/client contracts can anticipate likely issues and attempt to allocate responsibility for incidents (in business-to-business context) or to establish a preferred venue for claims disputes (e.g., arbitration instead of class actions).

*Recommended Actions:*

- Create or update due diligence checklist and approach for cybersecurity issues.
- Review key contractual provisions used in vendor/supplier and customer/client transactions.
- Initiate and support review of vendor oversight program, to embed new cybersecurity risk considerations into approach.

**8. Effectively Use Insurance**

Many more and better cyber-risk insurance products are available today compared to when the first such products appeared on the market a little over a decade ago. While these products should be purchased carefully, given exclusions and conditions imposed, they can be valuable ways to protect an organization.

*Recommended Actions:*

- Commission review of availability and efficacy of cyber-risk insurance for organization's purposes. Include advance legal review of insurance contract, especially exclusions.

**9. Monitor and Strategically Engage in Public Policy**

Cybersecurity legislative and regulatory efforts are certain to continue in the United States and elsewhere. Key issues include: whether and how to set cybersecurity standards for commercial critical infrastructure (CCI); which industries are considered to constitute CCI; and how to incent more robust information-sharing (e.g., create liability protections and strengthen protection of information shared with government).

A reasonable corporate response to this landscape can include:

- monitoring (to ensure advance awareness of emerging standards);
- advocacy via associations (to promote industry-wide considerations); and
- more active advocacy via smaller coalitions (to ensure that positions on key issues are socialized with key policymakers and industry leaders).

*Recommended Actions:*

- Commission work to inform and develop the company's cybersecurity policy position and priorities, if not already articulated.
- Ask the following: Is the organization sufficiently aware of regulatory, standards, and legislative initiatives globally, to anticipate impacts on the business?
- What mix of monitoring, association work, and more active advocacy should the organization employ to protect its interests? What are the most damaging and most helpful steps Congress or relevant regulators might take, and how likely is the organization's current strategy to prevent or obtain the desired result on these more important issues?

**10. Discharge Professional Duty of Care**

By virtue of their work, corporate counsel are entrusted with particularly sensitive information, and are expected to protect it.

Earlier this year, the American Bar Association amended Rule 1.6 of the Model Rules of Professional Conduct to add a new section on lawyers' obligation to maintain reasonable security of client information.<sup>22</sup> The new language supplements the existing duty of confidentiality, and reflects the ABA's recognition of the increased risk of the inadvertent or targeted compromise of systems and data held by lawyers. Even if the Model Rules had not been amended, however, it stands to reason that corporate as well as outside counsel should take precautions to protect client and related information, particularly when using or relying upon email, social media, cloud, and other digital capabilities.

*Recommended Actions:*

- Organize a continuing legal education session for the in-house legal team on the topic of cybersecurity and in particular the role and responsibilities of lawyers and other key individuals to practice safe computing.
- Review the organization's social media policy with in-house legal team, and discuss, if applicable, particular considerations for lawyers.
- Confirm outside counsel's sensitivity to these matters.

**Conclusion**

The cybersecurity challenge is complex and dynamic, especially because there is a powerful upside to the continued embrace of digitization and connectivity. Intensifying cyber-threats and an active legislative, regulatory, and standards-setting environment mean that the organizational, IT, and data security measures that were reasonable and prudent in the recent past are unlikely to suffice today and certainly will not meet expectations in the future.

Alongside other efforts by senior leaders in government and industry, corporate counsel should satisfy themselves that their company's enterprise risk management strategy is informed by a 360-degree view of the risk that includes the legal and policy landscape. They should review and help refine corporate and legal action plans so that such plans emphasize governance, prevention, and preparedness, and are multi-disciplinary and sustainable. They should be a model of contemporary security-conscious behavior. Finally, to understand and potentially influence evolving standards care in this area, they should monitor and consider strategic involvement in the policy and standards arena.

<sup>22</sup> Model Rules of Prof'l Conduct R. 1.6, available at <http://www.abanow.org/2012/06/2012am105a/>.