Dykema

A Brief Primer on Cybersecurity Issues Prepared by Dykema

Cybersecurity in the Private Sector: The Evolving Role of General Counsel

www.dykema.com

California | Illinois | Michigan | Minnesota | North Carolina | Texas | Washington, D.C.

Cybersecurity in the Private Sector: The Evolving Role of General Counsel

A Brief Primer on Cybersecurity Issues Prepared by Dykema

I. Introduction

According to a 2012 story by Corporate Counsel and FTI Consulting, 55 percent of general counsel and 48 percent of directors list data security as their primary concern. This high level of concern reflects the increased vulnerability of businesses and organizations to cybersecurity incidents, which put confidential information and intellectual property at risk, and the high stakes natures of such events.

Cybersecurity and data theft can have substantial impact—on both the public and private sectors. Estimates show that private sector cyber-attacks and cyber-espionage, including intellectual property cyber-theft, cost the country $100 billion in revenue and 508,000 jobs annually. For the government, this means a national security vulnerability, particularly to the nation's critical infrastructure—i.e., energy, telecomm, finance, health, and Fortune 500 companies.

With such high stakes, general counsel find themselves at the apex of mitigating the legal and business risks posed by cybersecurity issues. The question for corporate leaders and managers is not whether cybersecurity attacks will occur but how such events will be managed and the risk of their occurrence minimized. Success in cybersecurity risk management, therefore, means preventing the preventable and achieving optimal results when prevention fails.

In approaching this critical issue, some of the issues to consider are:

- *What is the nature of your business or operation that gives rise to cybersecurity risk?*
- *What are your legal, policy, regulatory, reputational, employee, product launch, global impact, supply chain disruptions, privacy, and litigation risks?*
- *Is cybersecurity the sole responsibility of the IT team?*
- *What compliance issues are implicated relating to cybersecurity?*
- *What is the appropriate response to a cybersecurity incident?*
- *What is the role of state and federal governments relating to cybersecurity?*
- *What additional issues arise where you conduct business outside of the U.S.?*
- *Are you prepared for a major cyber-attack?*

General counsel and their legal teams need to be proactive about getting involved in cyber-preparedness and response initiatives, to reduce the risk of insufficient responses and unnecessary fall-out, including costly lawsuits.

II. What is Cybersecurity?

Cybersecurity is the protection of electronic data and systems from attack, loss, or other compromise. A breach in cybersecurity can result in disclosure of confidential information, misappropriation of trade secrets, disruptions in supply chains, litigation, significant economic losses, diminished brand names and business standing, and regulatory/compliance violations.

III. Why Cybersecurity is Not just an IT Problem

As organizations have evolved technologically by storing increasing amounts of critical information on networks and enabling employees to transfer it electronically, cybersecurity has evolved into a responsibility not only for technology teams, but also for legal teams. Intellectual property and consumer data, and the networks on which this information is stored, can be an organization's most valuable asset.

Criminals and competitors know this. Therefore, to gain competitive advantages, steal trade secrets, or sabotage an organization's reputation, criminals have moved away from traditional methods of industrial espionage to cyber-industrial espionage. Cyber-theft of intellectual property and consumer information is fast becoming one of the greatest legal risks to organizations. As a result, new laws are being passed, creating a new area of compliance aimed at protecting organizations' information, and thereby, overall business success.

IV. President Obama's Executive Order and its Implications on the Private Sector

In February 2013, President Obama signed the Improving Critical Infrastructure Cybersecurity Executive Order, which orders the development of a standardized cybersecurity preparedness and response plan (known as the "Framework").[1] In signing the Executive Order, the White House has sent the message that it wants organizations, particularly those in critical infrastructure industries, to adopt and implement the Framework as a cybersecurity best practice. The White House's commitment to prioritizing cybersecurity is evident in the Executive Order's first paragraph:

> **The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.** The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and **to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.**

Id. (emphasis added).

The National Institute of Standards and Technology, which is charged with developing the "Framework," has been holding planning sessions with the private sector to develop a comprehensive plan that can be tailored to address an individual organization's particular needs and obligations. A draft Framework is due to be rolled out in October 2013, and the final Framework should be available in February 2014. The Framework will be available for use by organizations of all sizes and types as a model for cyber-preparedness and responsiveness.[2] The Framework can be used to create a new plan, or to perform a gap analysis on an existing plan.

---

[1] Exec. Order No. 13,636, 78 C.F.R. 33 (Feb. 19, 2013).

[2] *See* Preliminary Cybersecurity Framework Illustrative Examples, National Institute of Standards and Technology, Aug. 28, 2013, http://www.nist.gov/itl/upload/discussion-draft_illustrative-examples-082813.pdf; *see also* Message to Senior Executives on the Cybersecurity Framework, Aug. 28, 2013, http://www.nist.gov/itl/upload/discussion-draft_executive-overview-082813.pdf.

Cyber-breaches can touch every part of an organization and can cripple its operations if successful. General counsel need to be involved in the development and maintenance of a cyber-plan because the plan may well both establish, and fulfill, fiduciary duties of an organization, including that of its Board of Directors or senior management. The cyber plan will also establish the organization's disclosure and legal compliance requirements that are triggered upon a cyber-breach.

An organization's adoption of the Framework is voluntary. Therefore, to make its adoption more appealing to business, the White House and Congress have been working to establish legislative incentives to promote adoption. On August 6, 2013, the White House announced possible acceptable incentives, including discounted cyber-insurance rates, cyber-attack recovery assistance, liability protection, and research funding.[3] Congress has been drafting proposed legislation in support of similar incentives, as well as legislation that would codify the Executive Order.[4]

The Executive Order also increased the resources behind the Department of Homeland Security's voluntary information sharing program, which promotes information sharing from the private sector to the government in the event of a cyber-attack to help DHS' crackdown efforts. DHS offers those private entities that share such information Enhanced Cybersecurity Services.

The Federal roll out of the Framework—a best practices model—along with proposed incentives to adopt the Framework and the ECS information sharing mechanism, are just the beginning of a growing cybersecurity compliance program. This reflects not only the increasing importance that organizations need to place on their cybersecurity preparedness and responsiveness, it also demonstrates that the private sector and its legal teams need to stay informed and become more involved in this rapidly evolving complex area of the law.

V. Cybersecurity Disclosure Obligations: State, Federal, Sec. 10-K

Most states have laws that require organizations to disclose cyber-breaches, particularly when consumer information is compromised.[5] In addition, more than 50 federal statutes address cybersecurity in varying forms.[6] The Securities and Exchange Commission, in turn, requests public companies to make certain disclosures about cyber-threats and risks to its investors.[7] SEC guidelines suggest disclosure on the 10-K in the following areas:

> **1. Risk Factors:** Risk factor disclosures under Item 503(c) should include a discussion of cybersecurity and cyber incidents if such issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether to make such disclosure, companies should consider all available information, which the SEC staff notes includes the frequency and severity of prior cyber incidents, the probability of and qualitative and quantitative magnitude of risk from future attacks. The Disclosure Guidance states that companies also should take into account the adequacy of any preventative measures taken to reduce cybersecurity risks, taking into account the industry in which they operate.
>
> Cybersecurity risk factor disclosures should be tailored to a company's individual facts and circumstances and should avoid "boilerplate" disclosures. Among the disclosures that may be appropriate are discussions of: the nature of the company's business or operations that give rise to cybersecurity risk; a description of outsourced functions that have material cybersecurity risks, including how the company addresses those risks; the actual and likely costs and consequences for the company of a cyber-incident; the occurrence and impact of any actual or threatened cyber incidents at the company; and relevant insurance held by the company.

---

[3] *See* Incentives to Support Adoption of the Cybersecurity Framework, White House Blog, Aug. 6, 2013, http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[4] *See* Senate Commerce panel unveils cybersecurity bill, The Hill, July 11, 2013, http://thehill.com/blogs/hillicon-valley/technology/310487-senate-commerce-panel-announces-cybersecurity-bill.

[5] State Security Breach Notification Laws, National Conference of State Legislatures, Aug. 20, 2012, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx; *see also* Data Security Breach Notification Laws, Congressional Research Service, Apr. 10, 2012, http://www.fas.org/sgp/crs/misc/R42475.pdf.

[6] Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, Congressional Research Service, June 20, 2013 (including Table 2 list of laws with cybersecurity provisions), http://www.fas.org/sgp/crs/natsec/R42114.pdf.

[7] Securities and Exchange Commission, CF Disclosure Guidance, Topic No. 2: Cybersecurity, Oct. 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Companies also may need to disclose known or threatened cybersecurity incidents to put the cybersecurity risk factor disclosures in context. Thus, where a company has experienced a specific type of cyber incident, the company should consider discussing it as well as its known and potential costs and other consequences.

2. Management's Discussion and Analysis of Financial Condition and Results Operations: Under Item 303, the MD&A should include a discussion of cybersecurity risks and incidents if cyber incidents have had or are likely to have a material effect on a company's liquidity, results of operations or financial condition or would cause reported financial information not to be necessarily indicative of future operating result or financial condition.

3. Description of Business: Public companies should discuss cyber incidents in their Description of Business to the extent that such incidents materially affect a company's products and services, relationships with customers or suppliers, or competitive conditions. Such disclosure should consider the impact of the cyber incidents on each reportable segment.

4. Legal Proceedings: Companies may need to include in their Legal Proceedings disclosure a discussion of material pending legal proceeding involving a cyber-incident where the company or any of its subsidiaries is a party to the litigation.

5. Financial Statement Disclosures: Cybersecurity risks and cyber incidents may have significant effects on a company's financial statements. For example, prior to a cyber-incident, a company may incur substantial costs in the development of preventative measures.

6. Disclosure Controls and Procedures: Companies should consider the risks that cyber incidents may pose to the effectiveness of their disclosure controls and procedures. If it is reasonably possible that a cyber-event might disrupt a company's ability to provide the SEC with information required to be disclosed in SEC filings, then a company may conclude that its disclosure controls and procedures are ineffective.

7. Form 8-K: The Disclosure Guidance reminds companies that they may need to disclose the costs and other consequences of material cyber incidents in a Form 8-K if necessary to maintain the accuracy and completeness of information in the context of securities offerings.

Since these guidelines were issued, there has been a call to the SEC for mandatory cyber-risk disclosures. For now, SEC guidelines indicate disclosing cyber-related information is voluntary, but actions from Congress signal that mandatory federal disclosure requirements are likely coming.

VI. A Look Ahead to Potential Legislative Compliance Obligations

What we have addressed in this paper thus far is only the beginning. Congress is continuing to look for additional Federal means to bolster cybersecurity. In April 2013, the House of Representatives reintroduced and passed four cybersecurity bills:

Cybersecurity Enhancement Act of 2013, which "requires the development of a strategic plan to guide cybersecurity research and development (R&D) across the federal government." (H.R. 756)

Cyber Intelligence Sharing and Protection Act, which is "[t]o provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes." (H.R. 624)

Advancing America's Networking and Information Technology Research and Development Act of 2013, which "would expand the activities of the Networking and Information Technology Research and Development (NITRD) program, which coordinates the federal government's goals for developing advanced computing, networking, and software activities." (H.R. 967)

Federal Information Security Amendments Act of 2013, which "enhances the Federal Information Security Management Act of 2002 (FISMA) by improving the framework for securing federal information technology (IT) systems"; "establishes stronger oversight of federal agency IT systems by focusing on 'automated and continuous monitoring' of cybersecurity threats and by regular 'threat assessments'"; and "reaffirms the authority of the Director of the Office of Management and Budget (OMB) to oversee agency information and security policies and practices." (H.R. 1163)

This sampling of Congressional activity signifies that cybersecurity compliance remains a top priority. General counsel are encouraged to stay abreast of continued congressional action in order to ensure organizational compliance with these changing obligations.

VII. Prosecuting Cyber Crimes

In addition, general counsel generally play a vital role in the decision about whether a cyber-attack should be criminally prosecuted. General counsel should determine whether criminal prosecution is feasible and, if so, whether prosecution is in the best interest of the organization. Among the considerations weighing in favor of prosecution are deterrence and possible recovery of stolen information assets. Among the considerations weighing against prosecution are cost, additional business disruption, inability to identify the cyber-thief, and possible increased public relations exposure.

Prosecutors have been successful in prosecuting major cyber-crimes. For example, a former employee of a major automotive company was recently sentenced to 70 months in federal prison and ordered to pay a fine of $12,500 after pleading guilty to two counts of trade secret theft. The former employee, on the eve of starting a new position at a Chinese competitor, downloaded 4,000 company documents, including sensitive design specification documents, onto an external hard drive. The downloaded, stolen trade secret information had been developed by the company through decades of research, development, and testing and its theft cost the company an estimated $50 million. More recently, federal prosecutors issued indictments in the biggest cyber-crime case in U.S. history, charging five men with a hacking and credit card fraud scheme that cost companies more than $300 million. The hackers are thought to be responsible for security breaches at Nasdaq, Visa Inc., J.C. Penney Co, JetBlue Airways Corp and Carrefour SA, a French retailer.

VIII. How Cybersecurity Compliance Can Protect Management, Board Members and Organizations

Given the recent Executive Order and increased governmental attention to cybersecurity issues, general counsel can help implement effective cybersecurity measures that protect an organization's valuable information assets. Below are key areas in which general counsel can make an impact:

A. Advise Board of Director/Senior Management Regarding Cybersecurity Duty of Care

Inform executives, members of the board of directors, and employees about the growing legal responsibilities in this area. A plaintiff injured by a cyber-breach—i.e., a customer or supplier whose private information was stolen and misused—may invoke failure to adopt the Framework, the lack of cyber-preparedness, or a response plan generally, to argue that the organization and/or board breached their duty to secure data. Better understood responsibilities make breaches less likely. It is important that all levels of the organization understand their responsibilities to minimize risk of legal vulnerabilities.

B. Lead in Preparedness, Response, and Compliance

Typically, technology teams are viewed as the logical leaders of initiatives that involve system network security. Cybersecurity compliance, however, has implications well beyond the technical ones because a major cyber-breach can halt business operations and trigger legal obligations that further affect the company's stability. Therefore, general counsel must take an active role in leading preparedness, response, and compliance in this area. General counsel should consider appointing a cybersecurity point person on their legal team to stay up-to-date on new laws, regulations, court decisions and plaintiffs' trends, so as to ensure the organization and its preparedness and response plans are protected, up-to-date, and ahead of cyber-threats. General counsel should also consider facilitating simulations of the response plan to confirm that leadership, employees, and attorneys at the organization understand and can satisfy their roles and responsibilities in the event of a real threat.

C. Include Cybersecurity Terms in Intellectual Property and Supply Chain Contracts

Organizations are connected to supply chain and outsourcing partners at all levels. General counsel must include cybersecurity protection provisions in all contracts that deal with the electronic sharing of their organizations' intellectual property and information assets. For example, if a vendor or outsourcing organization will receive or store trade secrets or customer information of any kind—i.e., automotive design requirements stored by a supplier or utility company, customer data stored by an outsourced call center—general counsel need to include contractual terms that require the partner to comply with all cybersecurity compliance obligations, including an obligation that the partner maintain a suitable best practices plan, equivalent to the Framework. General counsel should at least consider including contract terms that would require indemnification from any claims or lawsuits that arise due to data breaches that occur because of the contracting partners' insufficient cybersecurity practices.

D. Anticipate and Manage Civil and Criminal Lawsuits

Inevitably, new compliance areas bring with them the risk and usually the reality of related lawsuits. In the area of cybersecurity, organizations can file lawsuits against hackers or breaching parties and will need to defend claims brought by a variety of plaintiffs. General counsel should prepare a litigation assessment checklist, which could be built into the cyber-plan or stand-alone, that will allow the legal team to perform critical first steps and determine whether a cyber-breach by a hacker, employee or vendor, warrants a civil or criminal lawsuit, or both.

For possible civil claims, general counsel should seek advice from outside counsel who specialize in cybersecurity claims, such as trade secret and employment agreement violations. For possible criminal prosecution against hackers, general counsel should consult with local United States Attorneys Offices to assess the possibility of success with criminal claims. General counsel may also wish to utilize outside counsel to act as liaisons with the United States Attorneys Office. Depending on the nature of the breach, general counsel, or outside counsel, should also work with the United States Attorneys Office to contact other federal authorities, such as the Federal Bureau of Investigation, for assistance with investigating the breach.

VIII. Practical Advice to Identify, Assess and Respond to Cybersecurity Risks and Attacks

In addition to the categories of involvement described above, here are ten tangible actions that general counsel can take now to help minimize risk and limit legal vulnerabilities in their client organizations:

1. Brief your legal team on cybersecurity compliance and appoint a cybersecurity point-person;
2. Partner with key members of appropriate business units to proactively develop a team to address cybersecurity issues;
3. Define roles and responsibilities of the members of a cybersecurity response team;

4. Gather statistics to know how cyber-attacks are impacting your organization at operations and legal levels;
5. Review and revise intellectual property and supply chain contracts for cybersecurity preparedness and response terms and conditions;
6. Brief C-suite or senior management on upcoming cyber-compliance programs;
7. Develop a litigation assessment checklist for civil and criminal lawsuits;
8. Establish an outside cybersecurity response team by establishing relationships with outside counsel and the U.S. Attorneys Office;
9. Meet with your training coordinator about cyber-compliance training for employees;
10. Perform a baseline due diligence review of cyber legal preparedness and response plans;
11. Schedule recurring due diligence reviews; and
12. Stay plugged in as a leader in developing and executing your organization's cyber-preparedness and response plan.

IX. Conclusion

Cyber-threats have been called "one of most serious economic and national security challenges" facing corporate America. With more and more of an organizations' critical information assets—i.e., trade secrets, corporate strategies, consumer information—being stored electronically, the private sector's interest in developing robust cybersecurity preparedness and response plans is equally if not more serious. As a result, general counsel and their legal teams should be proactive about taking a leadership role on cybersecurity teams. By becoming and staying informed in the area of cybersecurity compliance, general counsel can provide added protections to the company's Board of Directors, senior management, and the organization itself. With proper cyber-protocols in place, general counsel can ensure that their companies' most important business assets remain secure and their risks—legal and otherwise—are kept at a minimum.

For more information, please contact Sherrie Farrell, Susan Asam or your relationship attorney at Dykema.

Sherrie L. Farrell
Member
313-568-6550
sfarrell@dykema.com

Susan E. Asam
Associate
313-568-5332
sasam@dykema.com