Bloomberg Law®

Patterson Belknap

Privacy & Data Security Practice Portfolio Series

Cybersecurity Governance: A Guide for Corporate Officers, Directors and General Counsel

Excerpt: Foreword, Introduction & Executive Summary

Craig A. Newman, Esq.
Peter A. Nelson, Esq.

Patterson Belknap Webb & Tyler LLP
New York, New York

Foreword by Myron E. Ullman III, Chairman, Starbucks Corp.

FOREWORD

''The cyber threat has transformed the business landscape for corporate America. Corporate officers and directors are now charged with overseeing their organizations' management of this emerging and multi-dimensional business risk. Patterson Belknap has distilled the complexities of cybersecurity oversight into a must read for corporate leaders, board members, and chief legal officers.''

Myron E. Ullman III
Chairman, Starbucks Corp.
Former Chairman & Chief Executive Officer, R.H. Macy & Co., Inc.
Former Chairman, CEO & Director, J.C. Penney
Former Chairman, Federal Reserve Bank of Dallas

INTRODUCTION

We have witnessed massive data breaches in virtually every sector of the American economy. At the same time, we have seen a heightened risk to our nation's critical infrastructure and even to our electoral process.

The legal and regulatory landscape, too, is changing almost constantly. Government regulators and legislators have created sweeping, and at times daunting, new legal and regulatory environments. Private litigants have also taken aim at organizations with class action and shareholder derivative lawsuits in cases of large-scale data breaches.

At the center of all of this is corporate leadership – members of a company's executive leadership team and its board of directors – responsible for the management and oversight of an organization's cybersecurity risk. Regulators have also demanded new levels of accountability from corporate leaders and board members. As former SEC Commissioner Luis Aguilar noted in a speech at the New York Stock Exchange,

> ''[B]oard oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks . . . [O]fficers and directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.''

This treatise is written as a practical guide for corporate leaders, board members, and others within an organization tasked with the governance of privacy and data security risks. We have sought to make this treatise ''user-friendly'' and have organized it into nine separate chapters. We begin with an executive summary which serves as an overview and quick reference guide for the key issues covered throughout this treatise. In each of the following nine chapters, we start with a summary of key issues – all of which is covered in the executive summary – and then dig deeper into the complexity and nuance of each topic. While many passages in this treatise refer to public companies, the same general principles apply to leadership teams in private and nonprofit organizations. It is our hope that you will find our treatise meaningful and will use it throughout the year as a reference guide.

Craig A. Newman
Patterson Belknap Webb & Tyler LLP
New York, New York

EXECUTIVE SUMMARY

Executive leadership teams and boards of directors are responsible for overseeing their organizations' management of cybersecurity risks. This responsibility has never been as important, or as complex, as it is today. With a continually changing legal and regulatory data security landscape, growing reliance on data in all aspects of business and society, and new and more sophisticated threats emerging each day, effective cybergovernance is now mission-critical. This treatise is organized into nine separate chapters to enable corporate leaders to take a ''deep dive'' into the complexity and nuance of key cybersecurity oversight issues. The executive summary distills the fundamental lessons and key practical takeaways found throughout the treatise.

CHAPTER I
BOARD CYBERSECURITY RESPONSIBILITIES & LIABILITY: WHAT THE BOARD DOES

Directors and officers should understand the nature and scope of cybersecurity risks facing their organization and the key elements of effective cybersecurity risk planning and oversight.

As a general matter, directors and officers have a legal duty to oversee the cybersecurity risks facing their organization. In a seminal legal case referred to as *Caremark*, the Delaware Court of Chancery set forth the legal standard governing a director's fundamental duty of oversight, often referred to as the duty to monitor. The bar for individual liability under the *Caremark* standard is quite high, requiring the officer, director or board to engage in a ''sustained or systematic failure'' to exercise oversight, ''such as an utter failure to attempt to assure a reasonable information and reporting systems exists.'' Systems or internal controls to address known risks – including cybersecurity risks – should be established to ensure lawful conduct and compliance with applicable regulatory regimes. When overseeing the organization's compliance regime, directors and officers should also consider applicable federal and state regulatory standards of conduct relating to cybersecurity and take steps to ensure the organization's compliance with those standards.

To avoid counterproductive second-guessing of well-informed decisions of officers and directors, courts have developed a legal mechanism called the ''business judgment rule,'' which, shields corporate leaders from liability so long as their decisions are well-informed and made in good faith and without conflicts of interest, and believed by the decision-maker to be in the best interest of the corporation. Again, the bar for overcoming the business judgment rule is quite high: directors must show a ''conscious disregard'' for their duties or ignore ''red flags'' in order to be held liable.

Despite this high standard for liability, a number of cases have successfully proceeded against officers and directors, holding them accountable for issues ranging from explicitly illegal behavior to doing nothing to ensure that their organizations' reporting mechanisms were accurate. This underscores the importance of ensuring that effective internal controls and reporting systems are in place so that senior leaders can adequately oversee the company's cybersecurity compliance regime and are made aware of material cybersecurity events and risks in a prompt manner.

An emerging issue for corporate leaders is whether to establish dedicated technology and cybersecurity committees to oversee an organization's cybersecurity risk. While few public companies have adopted this approach thus far, there is a slow but growing trend in that direction. In some organizations, oversight of cybersecurity risk is assigned to the risk or audit committee, while other organizations have established a new committee dedicated to the issue. In any event, regulators have made clear that simply establishing a standing cyber board committee or sub-committee does not serve as a substitute for full board engagement. Accordingly, even with a dedicated cyber committee, the full board should be involved to some extent in the oversight of cybersecurity risk.

CHAPTER II
KEEPING THE BOARD INFORMED: WHAT THE BOARD NEEDS TO KNOW

By now it should be clear to corporate officers and directors that cybersecurity is no longer ''just an IT issue.'' Directors must routinely engage management to understand the organization's vulnerabilities in the event of a cyber-attack and, in particular, the specific data that could be the target for such an attack. As discussed in Chapter One, the board should, under appropriate instances, consider assigning specific members or a dedicated board committee with cybersecurity oversight, especially those with expertise or specialized cybersecurity knowledge or training.

Successful oversight at the board level also requires clear directives for the responsible individual or committee and periodic updates to the board as a whole. In some circumstances, retaining an outside cybersecurity expert to advise the board can be invaluable, to provide an objective and disinterested perspective much in the same way that a company's independent auditors meet privately with the audit committee. Such an arrangement has the added benefit of keeping committee members up to speed on recent cybersecurity trends and developments from an outside observer's perspective. It also provides an important record that demonstrates the board's commitment to ongoing cybersecurity oversight. In a similar manner, these board members or committees should consider meeting with the organization's Chief Information Security Officer on a regular basis to keep pace with activities and initiatives within their organization.

As discussed in Chapter Six about public company disclosures, the U.S. Securities and Exchange Commission stated in recent guidance that clear reporting lines should be in place to allow cybersecurity information to filter through to all affected stakeholders. This means clear reporting and responsibility lines need to be established not just within an organization, but also at the senior management and board levels.

An often-overlooked issue is the board's oversight role in ensuring that an organization has sufficient resources to protect its IT infrastructure and digital assets. Depending on the organization, this might include a review and analysis of the budget for cybersecurity risk management. It should come as no surprise that these budgets are generally on the rise to keep up with the risk environment and growing sophistication of cyberattacks. Regularly reviewing a company's cyber resources – from at least a top line perspective – should assist a board in keeping abreast of its cybersecurity program.

CHAPTER III
INCIDENT RESPONSE: THE BOARD'S ROLE

Effective cyber governance includes input from the board of directors in planning and preparing to respond to a cyber incident. Directors should encourage rigorous incident response planning, as well as updating and testing of the incident response plan. As appropriate, senior leaders and board members may play roles in the testing and planning for a data security incident – often called a ''table-top exercise'' or a ''mock data breach.'' This type of simulation enables organizations to test their response plan and make any needed adjustments during a simulation rather than during an actual data security incident.

Senior leaders and the board will sometimes play a prominent role in incident response, ranging from interfacing with regulators and law enforcement to acting as the ''face'' or public image of an organization undergoing a data security crisis. In consultation with legal counsel and crisis communications professionals, senior leaders and board members often play instrumental roles in shaping the organization's outward-facing message and narrative during a data breach. In such instances, leaders should work closely with legal counsel to ensure compliance with legal and regulatory obligations under various laws and regulations – including U.S. securities laws – in the timing and substance of breach disclosures. With an uptick in both securities fraud and shareholder derivative lawsuits, compliance with applicable laws and regulations is essential.

Organizations operating in critical sectors that collect sensitive business or personal information including personally identifiable information – referred to as ''PII'' – or protected healthcare information – referred to as ''PHI'' – often face increased risks and potential liabilities and that may require heightened oversight of cybersecurity and incident response planning. There are separate laws and rules of which the board should be aware that govern the unauthorized disclosure of such information.

Furthermore, the board should be informed of and oversee the incident responses for incidents of sufficient magnitude, including assessments of business, legal, and regulatory exposure resulting from the incident and participation in decisions about disclosure. While it is not required, where public companies have formed board committees or subcommittees tasked with the oversight of cybersecurity risk, these committees often work with outside advisors to ensure that an organization has taken sufficient steps to guard itself against the increasingly likely risk of a cyber-attack.

CHAPTER IV
KEY LEGAL CONCEPTS: WHAT EVERY CORPORATE LEADER SHOULD KNOW

While directors and officers are by no means expected to become legal experts, they should familiarize themselves with the basics, especially in highly-regulated sectors such as financial services, healthcare, and insurance. Because cybersecurity regulation remains a patchwork with varying laws in different states and sectors, this means identifying the specific laws and regulations that apply to your organization.

A basic understanding of an organization's fundamental legal and regulatory obligations provides leaders with a meaningful perspective on the organization's compliance obligations and provides a basic framework for overseeing an organization's cybersecurity risk management.

It's also helpful for executive leadership teams and board members to be familiar with the key regulatory players in their business sector. In the U.S., for instance, the top cyber regulators at the federal level are the U.S. Securities and Exchange Commission, with responsibility over publicly traded companies, and the U.S. Federal Trade Commission, charged with protecting consumers against companies that fail to keep their promises to safeguard customer information. There is also significant regulation at the state level, including both industry specific and general data breach notification laws. Organizations should be especially cognizant of state regulation as it often affects businesses that are domiciled elsewhere but have some connection to that state.

Although a comprehensive discussion is beyond the scope of this treatise, corporate leaders also should be aware of the growing importance of international regulation and its impact on U.S. companies. Right now, the European General Data Protection Regulation – or ''GDPR'' – is front page news. The GDPR affects a substantial number of U.S. organizations with its broad territorial reach. Chapter Four provides an overview of general principles under the GDPR for informational purposes only, but organizations generally rely on legal experts to provide counsel on such specialized regulation.

Finally, there is a growing trend of data breach shareholder derivative lawsuits filed against corporate officers and directors. This is a new and developing area of law that should be monitored. A derivative lawsuit is a legal mechanism that enables owners of a company – the shareholders – to hold corporate directors and management accountable for their actions. To date, the shareholder derivative lawsuits against corporate officers and directors have only been filed after major data breaches, charging that there was a failure of oversight at senior levels of the organization. While the law in this area is in flux, several general propositions should be kept in mind:

- For the most part, derivative cases against officers and directors have been unsuccessful and have settled based on a combination of data security governance changes and a modest award of attorney's fees.
- The proactive engagement of a board – as in the *Wyndham Worldwide Corp. Derivative Action* – can provide a defense against claims of negligence or failure by the board to satisfy its oversight obligations. While every case is different, proactive engagement might range from frequent board discussions of cybersecurity preparedness and monitoring of cyber threats to participation in ongoing data security investigations.
- As a general proposition, directors should take ''reasonable'' action to ensure that a company has proper cybersecurity systems, policy, and procedures; their oversight of cybersecurity need not ''be perfect.''
- Of particular note, in January 2019, former officers and directors of Yahoo! Inc. agreed to pay $29 million to settle charges that they breached their fiduciary duties in the reckless handling of customer data during a series of

cyber-attacks from 2013 until 2016 that compromised three billion Yahoo! user accounts, one of the largest reported hacks in U.S. history. The settlement ended three derivative shareholder lawsuits and, while the tab will likely be covered by insurance, this marks the first publicly-reported monetary award – as opposed to governance change and modest attorneys' fees – in a data breach-related derivative lawsuit.

CHAPTER V
APPLICABLE LAWS, REGULATIONS, AND OTHER OBLIGATIONS

Although we mention specific data security laws and regulations throughout the treatise, Chapter Five provides a high-level overview of the laws, regulations and other legal requirements that will play an important role in cyber enforcement over the coming years. As we have noted, officers and directors aren't expected to become expert in this area but should at least become familiar with the most prominent regulatory schemes affecting their organization.

One issue of particular significance is the U.S. Federal Trade Commission's (FTC) regulation of cybersecurity issues pursuant to its authority to prohibit ''[u]nfair methods of competition'' or ''unfair or deceptive actions or process in or affecting commerce.'' Over the past several years, the FTC has commenced enforcement actions against 60 companies based on data security issues. At present, however, there are some questions as to the scope of the FTC's authority in this area. In cooperation with counsel, significant FTC actions in the data security space should be monitored.

There is an array of federal law governing privacy and data security, including the Gramm-Leach-Bliley Act and its implementing regulations, which we review in Chapter Five. Organizations that handle health-related data or information must also comply with of federal healthcare data security law – focusing on the Health Insurance Portability and Accountability Act or ''HIPAA'' and the Health Information Technology for Economic and Clinical Health Act or ''HITECH'' – key aspects of which we also summarize in Chapter Five.

Additionally, states have individual data breach reporting laws that, depending on the state, require the reporting of a cyber-attack to regulatory authorities, law enforcement, and affected individuals. And state-level privacy laws are on the rise. Most recently, the State of California introduced what might be the most stringent data security law in the United States. We summarize the California law in Chapter Five, but it does not become ''operative'' until 2020 and will likely be revised before then. These state laws are highly nuanced and require specialized expertise to interpret and comply with.

Finally, New York recently implemented a groundbreaking cybersecurity regulation for financial institutions, including banks and insurance companies. To date, the New York law has been the most detailed and sweeping state-level, sector-specific data security law in the country. It was implemented in early 2017 by New York's powerful Department of Financial Services and phased in over a two-year period. A key aspect of the New York law is that it requires a board member or senior officer to formally attest to its organization's compliance with the regulation on an annual basis. Some have likened the compliance certificate under the New York regulation to the requirement under the Sarbanes-Oxley Act of 2002 that management certify the accuracy of the company financial statements.

CHAPTER VI
SECURITIES AND EXCHANGE COMMISSION (SEC) PUBLIC COMPANY DISCLOSURE REQUIREMENTS

In February 2018, the U.S. Securities and Exchange Commission released updated interpretive guidance, urging companies to be more transparent in disclosing cybersecurity risks in their public filings; to disclose material data security incidents in a ''timely fashion;'' and to implement safeguards such as trading bans to prevent insiders from selling securities after a breach is detected but before it is publicly disclosed. The guidance underscores the responsibilities of senior management and boards in cyber risk oversight. It also makes clear that cybersecurity risk disclosure and management is now one of the top priorities for the Commission.

The SEC's updated guidance reiterates and reinforces the Commission's staff guidance issued in 2011 by the Division of Corporate Finance, which called for companies to assess what disclosures might be required about cybersecurity risks and incidents. The new guidance – issued by the Commission itself – underscores the ''grave threats to investors'' and our financial systems posed by cybercrime and the uptick in the sophistication and severity of cyber-attacks on public companies. It also encourages focused and tailored cyber disclosures based on an assessment of a company's risk profile rather than general boilerplate disclosures.

The updated guidance focuses on four key areas:

(1) Pre-Incident Public Disclosure –

Although the updated guidance does not require detailed disclosures about a company's IT systems or vulnerabilities – to avoid giving a roadmap for mischief – it advises a holistic assessment based on the overall materiality of cyber risk to an organization and its operations. In particular, the Commission advises companies to consider among the following in preparing cyber risk disclosures:

- Prior cybersecurity incidents, including their severity and frequency
- Probability of incident occurrence and potential magnitude of an incident
- Limitations on the company's ability to prevent or mitigate cyber risk
- Particular industry specific or third-party vendor/supplier risk
- Potential for reputational harm
- Legal risks and costs of enforcement actions by other regulatory bodies (specifically referencing New York's new cybersecurity regulations for financial institutions and insurance companies)

When deemed material, the Commission advises that proxy statements contain disclosures about a board's role and

engagement in cyber risk oversight. The Commission also noted that cyber risk disclosures might, depending on the circumstances, be reflected not only in risk factor disclosures but in the company's MD&A, description of its business, disclosure of legal proceedings, and financial reporting ''to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements. . . .''

(2) Data Security Incident Disclosure –

One of the most challenging and practical questions for any organization is the public disclosure of a data security incident. Although the guidance makes clear that timely disclosure of material cybersecurity incidents is required, it concedes that ''some material facts may not be available at the time of the initial disclosure.'' Cooperation with law enforcement and incident investigation – which the Commission acknowledges is ''often . . . lengthy'' – will affect the scope of any disclosure. That said, the guidance warned that cooperation with law enforcement or ongoing investigations does not, ''on its own,'' provide a basis for not disclosing a material cybersecurity incident.

(3) Controls and Procedures –

As has been the trend with state-level data security regulations, the guidance also focuses on the role of senior corporate leaders and a company's board of directors. To that end, the guidance encourages the following steps:

- Assess existing disclosure controls and procedures to ensure that cyber risk and incident information ''is processed and reported'' to critical stakeholders ''including up the corporate ladder'' so that senior management is able to make informed disclosure decisions and compliance certifications, together with controls to assess compliance with such controls and procedures on a regular basis.
- If such controls are lacking, develop and implement a process so that important cyber risk and incident information is collected and elevated to senior levels for appropriate decision-making and oversight.

(4) Insider Trading and Regulation FD –

Finally, the guidance reminds companies of the risk posed by insiders who trade securities between the time a breach is discovered and when it is publicly disclosed. The Commission ''encourages'' public companies to put in place policies and procedures to prevent trading on material non-public information relating to cybersecurity risks and incidents including trading restrictions to avoid even the ''appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.'' The Commission encourages ''companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents.'' The guidance also warns against disclosing cybersecurity incident information selectively and reminds companies to disclose incident information on Form 8-K to manage the risk of selective disclosure.

CHAPTER VII
IMPORTANCE OF PRIVILEGE

Consideration of the applicability of the attorney-client privilege and work product doctrine should be ''top of mind'' in both data security preparedness and data breach response. Retaining and involving counsel in assessments of cybersecurity preparedness and incident responses preserves the ability of the board (or the organization it oversees) to assert a privilege in appropriate circumstances to protect sensitive information from being disclosed. The critical steps taken in the immediate aftermath of a cybersecurity incident may determine the availability of privilege in litigation and government investigations years into the future.

In Chapter Seven, we discuss the sensitivity and legal ramifications of an organization's cyber governance regime and consider the involvement of both outside and in-house counsel in cybersecurity work. We also review the developing case law in the area and several recent court rulings that underscore the care that must be exercised in making privilege determinations in the context of data security.

In addition, the board – at times with its own counsel – should consider potential legal privileges that may apply to its cybersecurity oversight and investigatory work, separate and apart from the company.

Although we review the attorney-client privilege, work product doctrine and common interest privilege in this chapter, these are highly nuanced legal issues and are discussed in this treatise for informational purposes only. Privilege decisions are fact-specific and should be made in consultation with legal counsel.

CHAPTER VIII
CYBERSECURITY INSURANCE

Cybersecurity insurance is an important risk mitigation tool in an area where the extent of potential harm to an enterprise is particularly difficult to quantify. As regulators have become more aggressive in investigating data breaches and levying fines, data breach costs have risen. In the U.S., the average cost of a data breach in 2018 was approximately $7.91 million, a substantial increase from the prior year. Insurance can mitigate some of these costs. As with any insurance policy, in considering various options, companies should look carefully at what is covered and what is excluded from coverage, including any sub-limits that might restrict coverage in certain areas.

In Chapter Eight, we discuss at a high level key issues to consider in assessing the use of cybersecurity insurance as a risk mitigation or transference tool, including a list of general considerations and questions to consider when evaluating insurance coverage. From a board or leadership team perspective, cybersecurity insurance should be an agenda item in most cases, but it is generally handled by an organization's risk committee or other appropriate governing body. Important considerations include the degree and level of risk insured, and, to the extent available, an assessment of what peer organizations might be doing in terms of cyber insurance, which might include self-insurance. As with many highly complex legal issues, organizations generally work with cyber insurance experts and brokers in assessing the need and scope of an organization's potential needs in this growing area.

CHAPTER IX
CYBERGOVERNANCE FOR TAX-EXEMPT ORGANIZATIONS

In our final chapter, we turn our attention to nonprofit organizations. As we have seen over the past few years, nonprofits can be unique targets for cyber-attacks because many collect, store, and transmit confidential donor and program participant information but may have relatively limited resources to invest in cybersecurity. Directors and officers of nonprofits should recognize cybersecurity as an organizational and fiduciary priority and take reasonable measures to protect the nonprofit against data security risks. Fiduciaries should work with the organization's staff, outside counsel, and providers to craft and implement an overall approach to cybersecurity that is tailored to address the specific needs of the organization.

Many of the lessons and key takeaways discussed in the first eight chapters of this treatise apply in varying degrees to nonprofits.

About Bloomberg Law

Bloomberg Law helps legal professionals provide counsel with access to action-oriented legal intelligence in a business context. Bloomberg Law delivers a unique combination of Practical Guidance, comprehensive primary and secondary source material, trusted content from Bloomberg BNA, news, timesaving practice tools, market data, and business intelligence.

For more information, visit pro.bloomberglaw.com.

For more information on Bloomberg Law, contact your account representative or our 24/7 Help Desk at 888.560.2529

help@bloomberglaw.com