

Get the Board on Board: Fulfilling Cybersecurity Governance Duties

Technology, Privacy, and eCommerce

Corporate, Securities, and Governance


B.O.D.
B.O.D.
B.O.D.


B.O.D.
B.O.D.
B.O.D.

CHEAT SHEET

- ***Facing the board.*** In-house counsel should fully educate board members about the potential consequences of a data breach and how best to protect against the possibility.
- ***Stop impending litigation.*** By executing data protection practices, board members can avoid impending civil suits regarding the victims of potential data breaches.
- ***Avoiding the ticket.*** With new data protection regulations around the world, it is becoming increasingly important for the board to evaluate the financial liability of a breach.
- ***Getting insured.*** The board should understand what cybersecurity coverage your company has and what requirements will minimize future risk with the carrier.

A company's board of directors has fiduciary duties, including a duty to oversee all aspects of the company's risk management efforts. This includes a duty to recognize and minimize the company's exposure to cyber attacks and to help ensure a company's confidential information and sensitive customer information is properly handled and protected. Both data privacy and data security issues make headlines regularly; this article will focus on how in-house counsel can help educate and engage the board of directors with regard to data security.

In today's digital age, it is no longer a matter of *if* most companies will face a data breach, but *when*. Most companies face a variety of risks related to confidential company information from various sources, ranging from sloppy or malicious current or former employees, to third party hackers and nation-state actors. Those executing these purposeful and targeted attacks are increasingly more sophisticated, highly organized, and financially motivated criminals, rather than amateur hackers or college pranksters. Such attacks not only put valuable assets and information at risk, but they also bring negative exposure and liability that can adversely affect a company's competitive positioning, stock price, goodwill, and shareholder value. To fulfill their fiduciary duties, directors must ensure their companies take reasonable security measures for threats that the company knows, or should know about. In-house counsel can and should assist in this endeavor.

Given the role the legal department should already play in developing a company's plans with regard to protecting its data and responding to any data breach, and in facilitating the highest levels of corporate governance, in-house counsel are in a good position to help facilitate the board's cybersecurity oversight obligations. As explained in detail below, in-house counsel can and must engage the board regarding their duties around cybersecurity to create best practices for cybersecurity governance. In-house counsel can help the board understand what is at risk. The board, advised by in-house counsel and their outside specialists, as well as other members of management, should understand the company's plan to address a data breach event, to help ensure the right plan is in place. In-house counsel should then advise the board on the legal consequences of a data breach event so that directors are able to put the risks in perspective and understand its members' own personal liability.

Helping the board understand what is at risk

The board cannot oversee or embrace an issue that it is not aware of or does not understand.

Therefore, a key role for in-house counsel is to partner with the chief information security officer (CISO) or a functional equivalent to help educate the board about the company's cybersecurity vulnerabilities. As a threshold issue, the board and in-house counsel should first understand that no company is immune to a cyber attack. While large companies may be targets given their higher profiles, midmarket companies (such as law firms) can have equally important and sensitive information about their clients. Often, these firms do not have the same level of resources dedicated to cybersecurity protections as larger companies do, making them an appealing target for an attack.

Next, the board should know, at a high level, what data is at risk. What does the company have that others may want? Where is it? Who can access it? For example, the protected information may include source code, personally identifiable information, money-related information (e.g., wire, escrow, credit card, or banking information), mergers and acquisition information, confidential information like trade and industrial secrets, intellectual property, and confidential information from other third parties (e.g., partners or customers).

In addition to identifying where that information exists within the company, it is also important for the board to ask who else possesses or has access to the information. Regardless of what internal protections a company has in place, its information may be vulnerable through its vendors. In-house counsel are often well positioned to have visibility into a company's contracts and relationships with outside vendors, and therefore in-house counsel can educate the board regarding where else a company's information or data should reside. With this information and understanding, the board can better fulfill its duties to ensure that management is selecting reliable vendors and doing the necessary due diligence about a vendor's policies and practices.

Understanding the plan to address the risk, and occurrence, of a data breach

The board should consider requiring management to develop in advance plans for (1) protecting its information from cyber-theft, and (2) how the company will respond in the event of a breach. The board can help ensure the company's plans are properly tailored to the company's data, operations, industry, and relevant legal and regulatory environment; as well as address internal controls, information inventorying, and access protocols. In addition, the board can include a comprehensive, up-to-date incident response plan, including a crisis communication strategy. In-house counsel who are educated on the important aspects of data protection and data breach plans can play a key role informing the board and facilitating discussions.

In-house counsel might also suggest that the board should consider taking some or all of the following actions, depending on the company's circumstances and needs, to exercise its duties of oversight with regard to cybersecurity. Although in-house counsel may also be making related efforts, engaging the board in these areas can bolster the company's cybersecurity efforts:

- Ensure that the company has formal processes for providing cybersecurity training to employees and for requiring contractors and vendors with access to critical company systems to have adequate security measures in place;
- Ensure that the company obtains penetration testing from a reputable third party firm on a regular basis and shares the results with the board;
- Have the company explore cyber insurance, at least annually; and,
- Ensure that the company has considered technologies certified under the SAFETY Act.[*]

* This point is of particular interest to directors once they learn more about it. The Support Anti-Terrorism by Fostering Effective Technologies (Safety) Act was enacted post-9/11 to encourage innovation and production of anti-terrorist technologies, which Congress felt was being stifled by fears of litigation and liability. The Act eliminates or mitigates some tort liability for sellers and buyers of approved technologies should lawsuits be filed after an attack. Its legal protections include a cap on or immunity from damages arising out of or related to "acts of terrorism" (as declared by the department of Homeland Security) if a certified technology was deployed prior to the attack. Of course, selecting and deploying an approved technology can also be used to show reasonableness in fulfilling fiduciary duties. In 2015, FireEye became the first (and is currently the only) cybersecurity company to have its technology certified under the Act. This certification not only provided companies and their directors with an important defense to cyberattacks and the litigation that follows, but also signaled that the DHS considered cyberattacks to fall within the definition of terrorism under the Act.

The board should also recognize, or in-house counsel may help the board understand, that its company's *failure* to do the following will likely be found *unreasonable*:

- Remedy "known security vulnerabilities" such as allowing insecure server/network connections;
- Employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess;
- Adequately inventory computers to manage network devices;
- Employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations;
- Follow proper incident response procedures, including monitoring computer networks for malware used in a previous intrusion; and,
- Adequately restrict third party vendor access.

Understanding the legal consequences

The board can more fully and appropriately execute its cybersecurity governance duties when it has an understanding of what the implications are from a data breach event. In fact, this may be one of in-house counsel's most valuable roles with regard to getting the board's attention on, and advising the board about, cybersecurity. Lawsuits and disputes arising from data breaches come in a variety of forms and attempts to recover under a variety of theories. The company will potentially face plaintiffs in civil lawsuits, as well as government actions and disputes with insurance carriers. Increasingly, the targets of those civil lawsuits have included not only the company but also the board of directors. In particular, recent litigation has highlighted the need for directors to demonstrate they took "reasonable" steps to fulfill their duties with regard to cybersecurity. In-house counsel must help ensure the board understands these consequences and the related best defenses at least at a high level.

Civil lawsuits

The most likely plaintiffs a company will face after suffering a data breach are the individual victims of the breach. These include consumers, employees, banks, and other financial institutions that may face unauthorized charges. Although plaintiffs' lawyers are increasingly creative with their causes of action, claims typically center around allegations that the breach resulted from the company's (and/or the board's) unreasonable or insufficient measures to protect the information in question. Causes of action include negligence, breach of contract, breach of fiduciary duty, unfair business

practices, negligent misrepresentation, products liability theories of breach of warranty and strict liability, and various statutory causes of action.

Plaintiffs' strategies to obtain relief continue to evolve as this area of the law develops, but damages sought typically include amounts for unauthorized charges, damage to credit, cost of credit monitoring, time and expenses to deal with the breach including preventative costs, anxiety and emotional distress, unjust enrichment, and increased risk of future harm. Successful legal challenges to these types of lawsuits have included a lack of standing or a lack of actual or imminent injury, and causation. However, where lawsuits are allowed to proceed, the best defense will be the ability to demonstrate a thoughtful, comprehensive, and well executed — even if not perfect — cybersecurity plan. As discussed above and highlighted in the sidebar, in-house counsel can help engage the board to make sure the company's plans are as robust and comprehensive as possible.

Key areas for an incident response plan

Although the board may not be responsible for the details of the incident response plan, in-house counsel likely will have responsibility to help ensure the company has a well-conceived plan that includes the following six areas. In-house counsel should help evaluate each of these when planning, executing, and maintaining the response plan.

Capability	Description
GOVERNANCE	• An organizational structure that aligns with overall business organization and mission statement • Clear security policy and guidance that safeguard critical systems and information sharing between internal and external entities
COMMUNICATION	• Mechanisms and processes that promote effective information sharing between internal and external entities
VISIBILITY	• Technologies and processes that keep organizations aware of activities occurring on systems and networks • Methods by which the computer incident response team (CIRT) remains aware of the threat landscape and applies that understanding to defending critical infrastructure
INTELLIGENCE	• Cyber threat intelligence capabilities that enable a detailed understanding of the adversary's capabilities, techniques, and intent • Intelligence that informs and enhances security planning, vulnerability management, and incident response
RESPONSE	• Process and technologies that the CIRT uses to identify, categorize, investigate, and remediate adverse security events
METRICS	• Objective measures of the efficiency of people, processes, and technology using a system that can be easily tracked and automated • Focused incident response metrics that are tied to overall business and security goals and objectives, driving continuous improvement

Notably, boards should also understand that shareholders are increasingly pursuing lawsuits against officers and directors for breaches of fiduciary duty related to a data breach, and in particular for failing to adequately protect a company's valuable information in the current world of cybersecurity risks. Directors can be held personally liable for failing in their duties of oversight. In-house counsel can help directors fully understand these additional, personal consequences. Given all that is at stake for both the company and for the directors as individuals, all parties should be aligned to work together on prevention and risk mitigation.

Boards should be equipped to execute the best practices and ask the right questions, as outlined above. The more a board can demonstrate its engagement and diligence with cybersecurity efforts, the better chance a company has of preventing significant data breaches. If a breach occurs, those same efforts can help provide the company and directors with their best possible defense.

Regulatory actions, fines, and standards

The US government and regulatory bodies are increasingly focusing on data security. The Federal Trade Commission leads the way with its enforcement actions, however the SEC and FCC have also fined companies for alleged failures in the company's data security practices and procedures. The SEC requires regulated entities to disclose material risks related to cybersecurity in their SEC filings and make adequate disclosures in the event of a breach. Europe is also increasingly regulating data security. The General Data Protection Regulation is expected to go into effect in 2018, and will provide the potential for increased fines for insufficient data protection measures in the European Union.

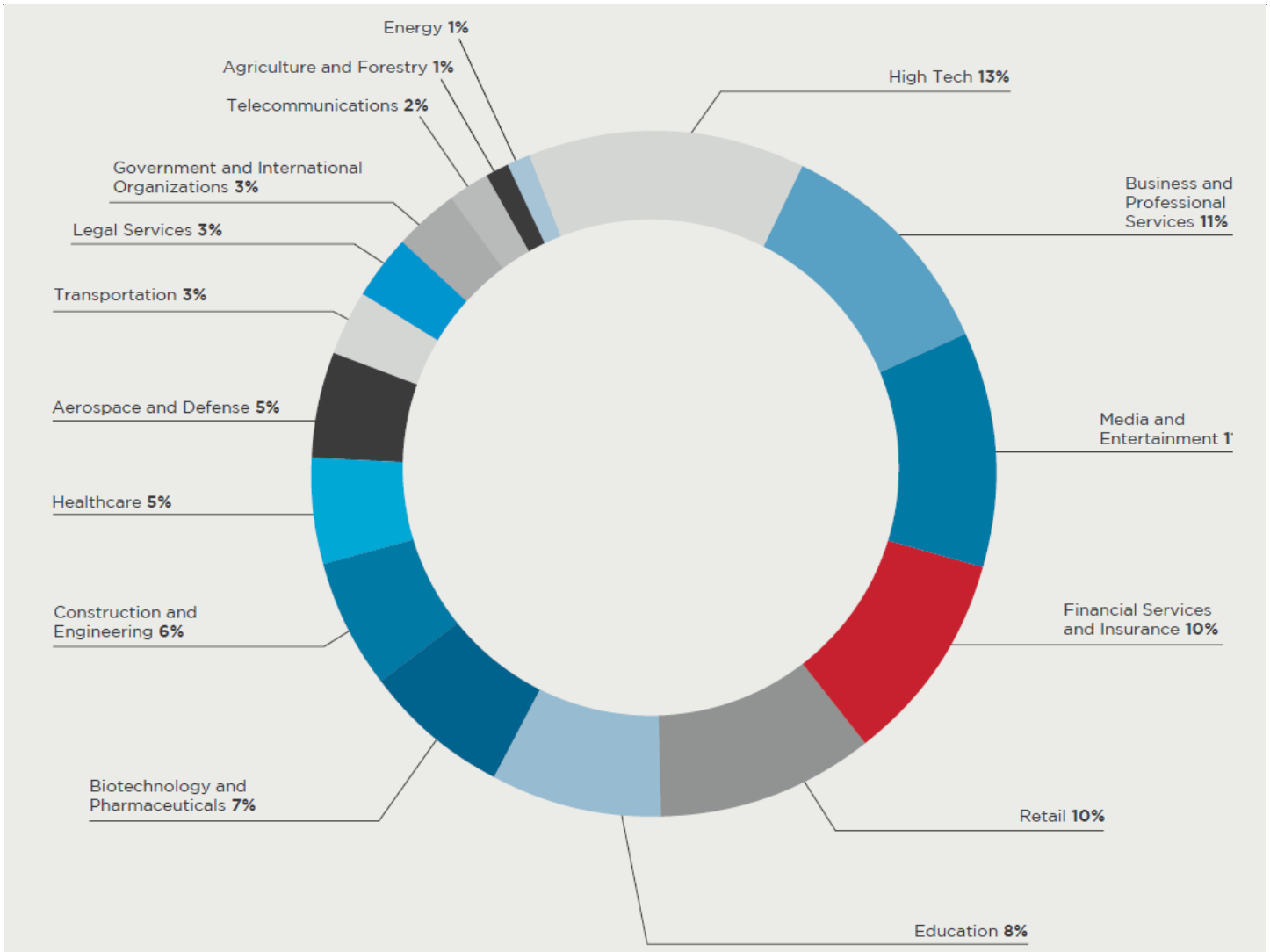
States have also started to take action. For example, California Attorney General Kamala Harris released a data breach report in February 2016, addressing and analyzing the data breaches that have been reported to her office. In the report, the attorney general noted, for example, that California's information security statute requires businesses to use "reasonable security procedures and practices … to protect personal information from unauthorized access, destruction, use, modification, or disclosure." The report then goes on to list as a "recommendation" that:

> "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security."

Although it is not yet clear exactly how much protection from liability a company may enjoy by complying with the controls, a company that fails to undertake the recommended measures faces increased risk of liability. In addition to the recommendation above, the report specifically stated that: "The set of 20 controls constitutes a minimum level of security — a floor — that any organization that collects or maintains personal information should meet." The board should understand that this type of benchmark and guidance exists for what constitutes "reasonable security."

By the numbers

Source: M-TRENDS 2016, Mandiant, a FireEye Company, February 2016



Disputes with insurance carriers

Finally, even with comprehensive cyber insurance, a company may still find itself in a dispute with its carrier regarding whether coverage in fact exists for a data breach event. For example, insurers have attempted to include conditions or exclusions about meeting certain standards for data security. When a policy holder suffers a data breach and tries to obtain coverage, the insurance company can try to point to that exclusion and argue that the company did not follow the minimum required practices. These efforts by insurance companies effectively negate the coverage that the policy was supposed to provide. Companies should try to avoid such conditions or exclusions, or be prepared to litigate the issue.

At the very least, the board should understand what coverage the company has and what notification requirements are needed to minimize the risk of future disputes with the carrier. While cyber insurance helps offload some risk, it should not be counted on to offload risks completely. For example, cyber insurance may apply to economic costs and damages, but it cannot make up for resulting damage to a company's brand or core business. The board should understand which risks may be covered, and where gaps or challenges remain.

Helping the board understand the potential implications of a data breach will help directors more

accurately understand and evaluate the sufficiency of managements' plans and the allocation of resources toward cybersecurity efforts.

When a breach occurs

Although every company and every breach is different, here are some things to immediately consider when your company experiences a data breach. The level of involvement by in-house counsel, the executive team, and the board will vary depending on the company.

- Call a meeting of the incident response team, which should include representation from the executive suite, IT, communications, and legal counsel. Review procedures and priorities from the incident response plan and assign team members specific tasks.
- Maintain legal counsel's involvement to establish and preserve attorney-client and work product privilege, which the company may want to assert to protect its positions in future litigation.
- Determine if the insurance carrier should be notified, and if so, provide notice in accordance with the coverage contract. Obtain consent from the carrier to proceed in accordance with response plans and coverage guidelines, and obtain consent where appropriate to retain necessary outside consultants.
- Assess the need for outside consultants and engage necessary outside parties. Consider retaining and directing consultants through outside counsel to maintain the attorney-client and work product privileges to the extent possible.
- Take stock of the incident, including the timeline, how the breach occurred, what systems were compromised, the access points, and any destinations of data sent out. Communicate with the appropriate team member, likely in IT, to be sure someone is preserving all information and evidence that may exist regarding what happened.
- Ensure the appropriate team members are taking any identifiable steps to prevent additional intrusion or loss. Trigger password changes and access code changes immediately if necessary.
- Work with the appropriate team member to determine what data was compromised and whether it was password protected and/or encrypted.
- With counsel, determine which local, state, federal, and/or international laws govern the incident. Confirm which agencies and individuals (including government agencies, employees, customers, investors, and/or other third parties) must be notified and develop a notification plan that considers the appropriate timing and content of all notices. Ensure that there is an agreed upon procedure in place, and the necessary personnel, to respond to inquiries.
- Ensure the appropriate team member(s) develops a public relations and communications plan.

Conclusion

Although boards function differently depending on the size and the characteristics of the companies they serve, in-house counsel can help ensure the board is structured in a way to most effectively understand and treat the issues set forth above. Specifically, in-house counsel can help ensure the board itself is able to designate which member is responsible for taking the lead on cybersecurity

issues. This may mean, among other things, delegating review of cybersecurity risks to a committee that is best suited to do so, be it the Audit Committee (as part of its general oversight of enterprise risk management), or another committee. For some companies, this issue may be spearheaded by the full board.

To help facilitate the board's ongoing involvement, cybersecurity should be a routine item on the board's agenda. Moreover, the board's work and attention on these issues should be documented in board minutes. Such documentation can help illustrate as necessary that the board was properly functioning in its oversight role.

While the definition of "best practices" related to cybersecurity governance is evolving, the one thing that is clear is that boards cannot ignore this issue. In-house counsel can and should ensure that the board is addressing these data concerns, educating itself with input from internal and external experts and advisors, and overseeing management's cybersecurity measures and plans. The more engaged and educated the board is on cybersecurity issues, the better positioned it will be to execute its oversight duties. Ignoring the issue is not an option. The board, like the company, must be focused, but also flexible, to continually improve and update its cybersecurity practices. In-house counsel can be a leader in doing so.

Alexa King



Executive VP, GC, Corporate Secretary, and Chief Compliance Officer

FireEye

Since she joined the company in 2012, she has built a department from zero to over 30 members worldwide, guided the company through a successful IPO, and completed a $1 billion acquisition.

Carly O'Halloran Alameda



Business Litigation Partner

Farella Braun + Martel in San Francisco

Her practice includes litigating complex business disputes in CA state and federal court and alternative dispute resolution processes, and also state and federal appellate work. Her practice is complemented and enriched by her position on the BOD of Mammoth HR, a private company focused on helping businesses with HR compliance and employee management.

Olga V. Mack



Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).