Bloomberg Law

Professional Perspective

Lessons for In-House Counsel from Cybersecurity's Front Lines

Peter M. Marta, Asmaa Awad-Farid, Harriet Pearson and Michelle Kisloff, Hogan Lovells

Lessons for In-House Counsel from Cybersecurity's Front Lines

Contributed by Peter M. Marta and Asmaa Awad-Farid, of Hogan Lovells. The authors would like to thank Harriet Pearson and Michelle Kisloff for their contributions to this article.

Recent developments reinforce the urgent need for general counsel and legal departments to deepen their focus on cybersecurity. In today's environment, any organization can be the target of a cyberattack, regardless of industry, size, or geographic footprint. Indeed, in just the past few years, a variety of cyber adversaries have attacked financial institutions, social media sites, a movie studio, hospital systems, a peer-to-peer ridesharing company, the Democratic National Committee, hotel chains, city governments, educational institutions, telecommunications and energy utilities, prominent retailers, manufacturers, and even the mobile app of a well-known coffee and donut chain.

All of us are potential victims. As a result, many senior executives have come to the realization that cybersecurity is perhaps the most serious—and existential—risk facing their companies. But some organizations are well behind the curve.

Officers' and directors' duties of care, loyalty, and good faith extend to the oversight of cybersecurity issues, but what constitutes a sufficient level of understanding, focus, and action? The answer remains in a state of flux given the proliferation of laws, regulations and regulatory expectations in this space. Accordingly, cybersecurity can no longer be viewed as strictly an IT or compliance issue, but rather as an essential element of any organization's overall enterprise risk management program. And importantly, cybersecurity should also be considered one of the most significant legal issues that companies face today.

This overview summarizes key developments, suggests their implications, and offers a perspective on the practical steps in-house counsel can take to ensure that their organizations' cybersecurity programs are properly aligned with evolving laws and regulations, industry practice, and regulator expectations. Taking a closer look at three areas—breach response, risk management, and regulatory compliance—we cover 10 topics that general counsel should be addressing.

On responding to breaches:

1. Coordinate internal communications and notification timelines on a global scale
2. Develop response plans to account for different type of incidents
3. Review scope of insurance coverage for cyber incidents

On managing risk:

4. Assess and explore active defensive measures
5. Engage in cyber due diligence
6. Evaluate insider threats
7. Invest in a dedicated cyber legal role

On complying with regulations:

8. Learn from past incidents
9. Monitor regulatory changes
10. Review SEC disclosure statements

Breach Response

1. Coordinate internal communications and notification timelines on a global scale

In today's environment, international coordination and speed are two of the most important elements to build into an organization's cybersecurity incident response plan. For global companies, an IRP with an established and tested process to identify, analyze, and mitigate cyber threats will have limited efficacy if those capabilities exist in only one region. In the same way, it is essential that a company's IRP facilitates coordination on a global scale among the various operational,

compliance, regulatory-facing, and line-of-business stakeholders. The IRP should also mandate escalation to the legal department once certain thresholds are crossed.

These challenges are even more pronounced for larger companies with an international presence due to the rapidly evolving regulatory landscape. Size and bureaucracy can make coordination particularly difficult. For example, if a company's cybersecurity operations center in New York identifies a serious incident potentially requiring notification to various global regulators, a seamless process needs to be in place to communicate known details of the incident to the organization's various global teams that are responsible for discharging the applicable notification obligations. Many companies have found that, in practice, this endeavor is much more difficult than it sounds.

Speed is also an increasingly important consideration. Not so long ago, the potential obligation to notify various stakeholders of a data breach was measured in weeks, which gave companies time to assess the situation, "stop the bleeding," and determine the extent of the damage before addressing whether notifications were required. Today, that luxury no longer exists in many jurisdictions, as notifications can be required in hours—not weeks.

For example, the European Union's General Data Protection Regulation (GDPR), which went into effect in May 2018, now requires data controllers to notify the appropriate authority within 72 hours after having become aware of it. The New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500), which went into effect in 2017, imposes a similar 72-hour breach notification obligation on covered entities (23 NYCRR 500.17), as does the California Consumer Privacy Act, which becomes effective Jan. 1, 2020, for residents of California.

Companies also need to consider contractual breach notification obligations, which have become increasingly common in the past few years. Companies should establish a process to keep track of contractual obligations to notify clients or others in the event of a cyber incident, which can be a daunting effort for organizations with thousands of contracts across numerous jurisdictions and in various languages.

Because of this new reality, a global organization's IRP should facilitate coordination across various business functions and corporate groups on a global scale. It should contain a list of all relevant stakeholders (and their contact information), delineate clear roles and responsibilities, and include appropriate triggers so that the response team can be assembled rapidly. A cyber incident response team for most organizations should be limited in size but include representatives from legal, cybersecurity operations, regulatory engagement, privacy compliance, media relations, internal corporate communications, and line of business stakeholders.

As a best practice, many companies find it useful to include pre-approved "starter" templates for the variety of potential communications that may have to be made, including those to regulators, customers, employees, investors, business partners, media outlets, insurers, and law enforcement.

2. Develop response plans to account for different type of incidents

The most commonly used framework for understanding cybersecurity attacks is the "CIA" triad, which stands for Confidentiality, Integrity, and Availability breaches. Most of the focus to date, both in terms of the evolution of law and regulator interest, has been on breaches of personal information through confidentiality attacks. This is not surprising given the fact that most of the high-profile cyber attacks over the past several years have been of the confidentiality variety.

However, there has been an increased focus on integrity and availability attacks over the past few years by global regulators, a trend which will surely continue. Availability attacks, such as ransomware and Distributed Denial of Service (or DDoS) attacks, attempt to deny access to the victim's data and/or systems, whereas in an integrity attack an adversary is potentially able to change or delete data inside a victim's infrastructure.

While the breach of confidential information remains a serious concern, there is a good argument that in some industries integrity and availability attacks pose even greater overall risks. For example, imagine what would happen if an adversary broke into a bank's infrastructure and started zeroing out account balances, changing numbers, and initiating transactions. Even if limited in duration, this type of attack would likely cause considerable concern—and potentially panic—over the soundness of the global financial system.

As a result, the maturity of an organization's cyber resilience and business continuity efforts are increasingly facing serious regulatory scrutiny. Indeed, the Federal Deposit Insurance Corporation adopted cyber resilience as a strategic goal in its own Information Security and Privacy Strategic Plan for 2018-2021.

In addition, recent law and regulation requires notification of these other types of attacks in a manner that may not be required in the U.S. for personal data breaches. See, for example, the Philippines Data Privacy Act of 2012, where a "security incident" is defined as "an event or occurrence that affects or tends to affect data protection, or may compromise availability, integrity or confidentiality."

Accordingly, companies may want to consider developing separate playbooks, or adding appendices to their IRPs, that address the unique challenges that will have to be navigated by an organization that experiences an availability or integrity attack.

3. Review scope of insurance coverage for cyber incidents

While a full discussion analyzing the efficacy of cyber insurance is outside the scope of this overview, companies should consider whether certain types of cyber-related incidents may be excluded from the policy.

Most insurance policies contain war exclusions, which are provisions that specifically exclude coverage for acts of war, such as invasion, revolution, coup d'état, or terrorism. For the exclusion to apply, the insurance company has the burden of proving that the event in question was an act of war. This is particularly difficult to achieve in the context of a cyber incident, however, as the adversary's identity, actions, and motivation may be suspected but are very difficult to prove given the inherent challenges of determining attribution in cyberspace.

One recent example of this debate can be seen in an insurer's denial of coverage to a large global food and beverage company that was impacted by an unprecedented cyberattack. Many governments have attributed the attack to Russia, and in denying coverage, the insurance company pointed to the war exclusion in the all-risk property policy. The insurance company will have the burden of proving that the activities conducted by the (presumably) Russian hackers constituted an act of war or terrorism.

Regardless of how this particular case is decided, it highlights a few takeaways:

- Organizations should carefully review their policies—potentially with the assistance of external advisers—to determine whether they will adequately protect them against losses from cyber incidents.
- For new policies, or renewals, companies should insist on narrowly tailored exclusionary language.
- Companies should look beyond the organization's cybersecurity insurance policy. Coverage may be available under standard business interruption or theft and fraud policies.

Risk Management

4. Assess and explore active defensive measures

Many C-suite executives recognize that the private sector—not the government—owns 85% of the critical infrastructure in this country and, as such, U.S. companies are on the front lines of an active cyber war. Yet the law that addresses what actions private companies can take to protect themselves—the Computer Fraud and Abuse Act (CFAA)—was written before the internet existed.

Accordingly, private companies are increasingly exploring a number of cyber-defensive measures to protect themselves. Among the various measures are so-called "active cyber defense" initiatives, which can be thought of as a spectrum of increasingly sophisticated and aggressive actions that can be taken to prevent or disrupt attacks and mitigate damages.

The most aggressive measure—"hacking back"—is quite controversial, fraught with potential legal risk, and is often mistakenly viewed as the only option available to private sector companies. But there are several other self-help measures that companies may want to consider, and the central question in that analysis is where the line is (or should be) drawn to separate permissible activities from those that likely violate the law.

While a full legal analysis of active cyber defense in the private sector is beyond the scope of this overview, it is important to note that some cyber-defensive measures can implicate a number of federal laws in the U.S., including the CFAA, the Wiretap Act, the Electronic Communications Privacy Act, and the Cybersecurity Information Sharing Act of 2015. At least one U.S. state has proposed its own "hacking back" legislation as well. In addition, because most cyber-defensive measures will inevitably come into contact with computers and servers in other countries, a careful analysis of international law and regulation should also be conducted.

Against this backdrop and in the face of the rapidly evolving nature of the cyber domain, some private sector companies may decide to take matters into their own hands. Before doing so, however, they would be prudent to take these discussions beyond the IT department to senior management, including the general counsel, and potentially even to the board. In that forum, a number of considerations should be evaluated.

- First, companies should conduct a full legal analysis of cyber-defensive measures before any such activities are implemented. While there is a great deal of debate, most believe that current U.S. law clearly prohibits private companies from engaging in measures on the more aggressive end of the active defense spectrum. Nevertheless, some active cyber defensive measures, such as information sharing, honeypots and tar pits, are almost certainly permissible.

- As with so many issues, companies also need to consider reputational risk. If made public, how could it affect the brand? Would it make the organization a villain or target of derision? Or would investors, business partners, customers, and others view these activities more favorably? And inevitably, what are peers doing or considering?

- Even where the legal analysis concludes that certain defensive measures are permissible and senior management has accepted potential reputational risk, companies would be prudent to coordinate these initiatives with law enforcement to ensure, for example, that certain activities would not interrupt existing law enforcement investigations

5. Engage in cyber due diligence

Pre- and post-closing due diligence has long been an established component of a wide variety of commercial transactions. Taking all reasonable steps to learn as much as possible about the counterparties to a transaction is not only common sense, but in some cases required to meet fiduciary duties to clients and shareholders.

Due to the central importance of cybersecurity, conducting due diligence on a company's cybersecurity program is increasingly common. Relevant topics for cyber due diligence include the cyber maturity of the organization and its management, the nature and risk profile of the data it holds (and where it is stored), its exposure to third-party cyber risk, and its own cyber incident preparedness.

Unfortunately, some companies have not sufficiently engaged internal and external cyber expertise—both legal and technical—in the due diligence phase of a transaction. The traditional due diligence framework has been in place for many years, and at times there has been a lack of appetite for meaningful change. As a result, it can often be the case that lawyers and bankers who don't understand cybersecurity negotiate these important issues with counterparts on the other side of the transaction who similarly do not possess the right level of cyber expertise.

When that happens, very serious issues can be glossed over simply because there's no one at the table who understands what questions to ask, the responses to those questions, and the appropriate follow-up. Accordingly, companies in every industry should take note of this shortcoming and seriously consider incorporating the appropriate technical and cyber legal diligence into the traditional pre-closing framework and post-closing integration of commercial transactions.

- In 2017, Verizon lowered the purchase price it was willing to pay to acquire Yahoo by $350 million after Yahoo disclosed it had been the victim of one of the largest security breaches of all time. Yahoo was subsequently assessed significant fines by regulators and settled a number of civil lawsuits.

- In Nov. 2018, Marriott disclosed a security breach in the Starwood Hotels' guest reservation database, which it had failed to identify when conducting due diligence prior to its 2016 acquisition of Starwood. Marriott is now facing significant litigation, regulatory scrutiny, and associated fines and expenses. Indeed,

the UK Information Commissioner's Office—which has announced its intention to fine Marriott more than £99 million for violating provisions of GDPR—noted that Marriott failed to undertake sufficient due diligence when it bought Starwood and should have done more to secure its systems.

6. Evaluate insider threats

By 2019, many senior executives have realized that cybersecurity is one of the most serious and existential risks facing their companies. Some have dedicated enormous resources to addressing the rapidly evolving range of cyber threats and the accompanying regulator and investor expectations. However, more attention should be paid to the activities of an organization's employees and contractors. Indeed, studies have consistently concluded that employee activity constitutes the greatest risk of all. Accordingly, executives and board members should be focused on the issue of insider risk—both malicious and negligent—when evaluating their organizations' overall cyber incident preparedness.

Prior to developing an insider threat program, an organization will need to consider the various laws and regulations that address the monitoring of its workforce. For example, is it required to notify its employees that they are being monitored? Does the organization need to obtain consent, and if so, in what form (express or implied)? Is consent considered valid in the workplace? For what purpose can employees be monitored, and by what means? And on a more practical level, what would the company do if some employees refused to provide consent

The answers to these questions vary by jurisdiction, and the relevant laws and regulations are evolving at a rapid pace. Accordingly, a survey of the legal and regulatory landscape in countries where employees are located is a prudent step to take before deploying an insider threat program.

Companies should also approach the development of an insider threat program with basic privacy principles in mind. Effective insider threat programs may involve automated decision-making tools (including artificial intelligence) and developing profiles of individual behavior. Conducting data privacy impact assessments and incorporating privacy by design are both prudent steps to take when implementing programs that involve such tools and practices. And with GDPR in force and similar legislation likely to follow in other jurisdictions, those privacy practices are essential, if not in some cases legally required.

To some, the proposition that public companies may want to consider developing insider threat programs may seem Orwellian. But what may be considered excessive today could be deemed reasonable at some point down the road, and indeed even required in some form by regulators. For "critical infrastructure" organizations (as defined by Executive Order 13636), these questions are even more important to consider, and executives and board members would be prudent to start having those conversations today.

7. Invest in a dedicated cyber legal role

Five or six years ago, many general counsel would have disagreed with the notion that cybersecurity required significant involvement by the legal function. Indeed, for many years it was conventional wisdom that responsibility for cybersecurity was solely the province of IT and compliance departments. Today, after several years of well-publicized breaches affecting a number of different industries, many companies have come to understand that cybersecurity should be viewed not merely as a technology issue but as an essential element of an organization's overall enterprise risk assessment program.

However, companies should also be viewing cybersecurity as a legal issue. A company's legal department has a key role to play in helping to establish, develop, periodically uplift, benchmark, test, and guide the organization's overall cyber incident preparedness.

Moreover, in the event the organization experiences a cyber incident, the legal department will often play "quarterback" and assume a central role across different activities to include the retention of external advisers; analysis of breach notification obligations globally; regulatory outreach; engagement with law enforcement and other government agencies; and preparation, review, and approval of communications to regulators, customers, employees, media and other stakeholders.

And of course, the legal department and outside counsel will be responsible for handling any post-breach litigation and/or regulatory investigations. Indeed, many companies have realized that some of the most important decisions that may need

to be made in the initial hours and days after the discovery of a breach will not be made by its chief information security officer (CISO), but rather by the general counsel, or by the chief executive in close consultation with the general counsel.

Given that reality, companies—especially those in critical infrastructure industries—should consider creating a position in the legal department that is focused on cybersecurity. In some organizations, the remit for such a role may also cover privacy legal issues. However, a growing number of companies have realized that the myriad challenges that organizations face in the area of cybersecurity—some of which are addressed in this overview—justify the formation of a separate, cyber-related role, or even team. In addition, having a cyber lawyer located physically with an organization's cybersecurity management team can be particularly beneficial given the constant prospect of incidents and the need for rapid escalation when they occur.

In addition, external advice can be essential to help legal departments, senior executives, and boards evaluate the "reasonableness" of a company's cybersecurity program, which is a target that will not stop moving anytime soon given that regulations (and regulatory expectations) are rapidly changing in response to the expansion of the cyber "attack surface," the evolution of threat vectors, and the emergence of new threat actors. External counsel may also be able to assist companies with engaging the appropriate officials in law enforcement and the intelligence community, which is particularly important if the facts suggest the incident may involve nation-state actors.

Regulatory Compliance

8. Learn from past incidents

Companies would be wise to apply, as relevant, the numerous lessons learned from past incidents when establishing, developing, and updating their cybersecurity incident and resiliency efforts. Recent incidents have brought to the fore key legal and regulatory risks that were not as prominent even just a few years ago. One incident underscored the importance of considering the risk of insider trading before an event is disclosed publicly. Another served as a reminder that it is crucial to conduct robust third-party oversight of a company's suppliers and other business partners where infrastructures may be connected. Other incidents, such as Capital One, have highlighted the risk posed by employees or other corporate insiders, both of the victim company itself or its vendors.

In addition, past incidents have shown that employees can either be a company's pivotal first line of defense or its weakest link; the extent to which an organization has established a culture of security and trained its workforce on cybersecurity awareness often determines which role employees play. Phishing, credential compromise, and social engineering directed at employees are common vectors of cyber attacks, and as such companies will be better positioned by requiring all employees and contractors to take cybersecurity training upon the start of employment and annually thereafter. In addition, tabletop simulations are a particularly useful tool for employees who would be involved in an actual incident to help ensure their understanding of the various roles and responsibilities, and to more generally evaluate the effectiveness of the company's incident response plan.

These examples and others demonstrate that "lessons learned" from prior breaches should be considered well beyond an organization's IT department. A company's senior leadership—particularly its general counsel—should ensure that the organization's cyber incident program and practices are periodically reviewed and updated to incorporate the long and growing list of lessons learned.

Such an undertaking is even more critical in light of the significant fines being imposed by U.S. and global regulators, the large settlements in recent post-breach civil litigation, and the near certainty of class action litigation following the disclosure of a major cyber breach. Further still, the California Consumer Privacy Act (CCPA includes a private right of action for consumers whose personal information is subject to a breach, and several other states have expressed interest in following California's model.

9. Monitor regulatory changes

Even the most sophisticated global companies struggle with how to address the rapidly evolving legal and regulatory environment in the area of cybersecurity. Over the past few years, regulators around the world have responded to the dramatic increase in cyberattacks with a cascade of new cybersecurity laws, regulations, implementing guidelines, informal guidance, and industry standards. And unfortunately, to date there has been a lack of harmonization, resulting in numerous

regulations—some of which appear to be in conflict—on an international scale and leading to a great deal of confusion in the legal and compliance departments of many multinational organizations.

In addition to the compliance burden, the confusion over how regulations will be implemented and enforced can have a serious impact on the business. As one example, consider the Chinese Cybersecurity Law, which came into force in June 2017. As of October 2019, implementing guidelines for the CSL have still not been released. For companies seeking to establish a greater presence in the Chinese market, this lack of clarity can result in delays in decisionmaking on operational, personnel, logistical, and other business matters that can have significant and costly impacts on an organization.

Due to this rapidly evolving environment, companies may want to consider seeking the assistance of outside advisers. Not only is it critically important to understand the current state of regulation in all countries in which the organization does business, but it is equally necessary to have a process in place to keep the advice "evergreen." Even for sophisticated global companies, this endeavor can be a daunting and resource-intensive challenge.

10. Review SEC disclosure statements

Public companies should take note of the Security and Exchange Commission's increasing focus on cybersecurity. A close review of the company's cyber-related disclosures is essential. Risk factors and other public disclosures should be reviewed and confirmed for accuracy. In addition, the organization's disclosure controls and procedures should be "designed to analyze or assess incidents involving misuse of user data for potential disclosure in the company's periodic reports," (noted by the SEC in its July 24, 2019 complaint against Facebook for the unauthorized transfer of user personal information to Cambridge Analytica). Facebook's $100 million settlement with the SEC related to its disclosures about cyber risk underscores the critical importance of these considerations.

The SEC issued guidance in early 2018 that outlined its expectation that public companies develop effective controls and procedures to inform investors about material cybersecurity risks and incidents in a timely fashion. Perhaps the most significant recommendation addressed insider trading in the context of a material cyber incident that has not yet been made public. In such a situation, knowledge of the incident would likely be considered material nonpublic information, prohibiting those directors, officers, and other corporate insiders with knowledge of the event from trading the company's stock. A public company's incident response planning should therefore consider potential insider trading risk.

In Oct. 2018, the SEC issued a separate report urging public companies to consider cyber-related risks when designing and implementing accounting controls. The report was based on an investigation into several successful Business Email Compromise fraud schemes that cost the victim companies tens of millions of dollars. While the SEC ultimately did not pursue enforcement actions against the victim organizations, the report clearly indicates that public companies without proper internal controls to combat these threats may be found to be in violation of their obligations under Section 13(b)(2)(B) of the Securities Exchange Act of 1934.

Finally, the SEC may become more closely involved in the evolving guidance on the topic of cyber expertise on companies' boards. In Feb. 2019, the Cybersecurity Disclosure Act of 2019 was introduced in Congress by Sen. Jack Reed (D-RI). The draft legislation would direct the SEC to issue final rules requiring a registered issuer to:

- Disclose in its mandatory annual report or annual proxy statement whether any member of its governing body has expertise or experience in cybersecurity, and
- If no member has such expertise or experience, describe what other company cybersecurity aspects were taken into account by the persons responsible for identifying and evaluating nominees for the governing body.

Over the past several years, many private sector companies and industry groups have lobbied against the imposition of prescriptive laws or regulations that contain obligations to adopt specific cyber-related policies and procedures, including the makeup of a company's board. However, as cyber attacks continue to proliferate at an exponential pace, the proposed Cybersecurity Disclosure Act of 2019 may be an indication of where regulation is moving.

Conclusion

As this overview illustrates, cybersecurity is a rapidly evolving space that demands the attention of the senior management of every organization—regardless of industry, size, or regional footprint—including chief executives, directors, and perhaps most importantly, general counsel. The number of complex legal issues that companies need to navigate before, during, and after a cyber-related incident continues to grow as the lessons learned from each new reported breach highlight areas of legal risk and regulatory scrutiny not previously considered. And in 2019, we are still in the very early days of where these challenges are going to take us.

While budgets are routinely cut, priorities shift, and resources are often limited, corporate executives and directors do not have the luxury of treating cybersecurity risk management as merely one of the numerous IT and compliance issues competing for their attention. Cyber is an existential threat, and failure to adequately focus on it can not only damage a company's reputation and bottom line, but also have a detrimental impact on the jobs, and indeed careers, of senior executives. Some companies have already accepted this reality, but unfortunately many still need to go through the paradigm shift that is necessary to adequately address today's cyber threat environment.

Making this even more difficult is the fact that defining and valuing the success of any organization's cybersecurity program is inherently difficult—"success" is the absence of a major cyber incident. Much like intelligence agencies, an organization's success in the cyber space is invisible, while its failure will be front page news. Moreover, executives who are accustomed to being able to calculate return on investment will find it difficult to determine the right level of investment and calculate "return" on it.

Nonetheless, as Aldous Huxley said, "facts do not cease to exist because they are ignored." Cyber risk is here to stay, as is the need for corporate leaders to prioritize it. Officers' and directors' duties of care, loyalty, and good faith extend to the oversight of cybersecurity issues, and courts and regulators are increasingly scrutinizing such oversight. Accordingly, a general counsel's broader remit puts him or her in a unique position to articulate the risk and advocate for the organization's commitment to develop and regularly review and improve its cybersecurity risk management program.