This article has been published in *PLI Current: The Journal of PLI Press*, Vol. 3, No. 2 (Spring 2019), www.pli.edu/PLICurrent.

PLI Current
The Journal of PLI Press

Vol. 3, No. 2, Spring 2019

Tips from the Trenches to Make Your Company Less Attractive to Cyber Enforcement

Aimee Nolan
W.W. Grainger, Inc.

Jason N. Smolanoff
Kroll, a division of Duff & Phelps

Antony P. Kim
Orrick, Herrington & Sutcliffe LLP

Overview

Proactive risk management is a dynamic, multifaceted opportunity for companies of all sizes. In the cyber realm, the core issue is typically around calibrating investments in security to align with properly identified threats and vulnerabilities. This requires a holistic view drawn from key stakeholders across departments and disciplines. It also warrants tough debate on enterprise priorities and resources. Companies rarely get it 100% right. But they enhance their chances of doing so through structures and processes that account for the critical interplay between governance (input and accountability), operations (practical business considerations and capabilities), and controls (technical, physical, and administrative)—in that order.

At the end of the day, the goal is clear: to appropriately assess and mitigate risk to the enterprise and its key stakeholders. Unfortunately, that risk increasingly includes the potential for enforcement by a regulatory agency and/or the plaintiffs' bar. Nearly every U.S. state and federal agency has cyber at the top of its agenda. And statutes such as the California Consumer Privacy Act of 2018[1] portend a next-generation of laws that will inject *statutory* breach damages into the mix—ostensibly eliminating the need to show any actual harm to consumers, similar to other statutes with unbalanced punitive consequences like the TCPA.[2] Substantial fines and penalties, brand and reputational damage, and a host of other liabilities, including for directors and officers, are squarely on the table for the foreseeable future.

Against this backdrop, there is no "easy button" to push—but there are certainly some easy wins. And while there is no such thing as perfect security, there are some steps that make perfect sense. Our hope is that shared, common experiences and insight might help *lawyers* to positively influence the management and mitigation of cyber risk. In that regard, this article offers some lessons learned from the trenches in the form of seven actions that can help your company down the road.

1. Keep Good Company

It has never been more important to diligently vet, onboard, monitor, and audit critical third-party service providers and vendors. These third parties exist to make life easier, more efficient, and more innovative and to help you better serve your customers. To do so, they often have access to, ingest, and store tre-

mendous amounts of data for various processing purposes. Given this reality, it is hardly surprising that vendor-attributed data breaches are increasingly common. A recent study by Soha Systems found that 63% of data breaches may be directly or indirectly related to third-party access by contractors and suppliers.[3] And while there are certainly examples of bad press and enforcement activity against a service provider who suffers a data breach, by far, the rule is that the company bears the brunt of its service provider's cyber mistakes and mishaps. Continued corporate migration to the cloud, and the growth in outsourcing generally, set the stage for significant third-party risk going forward.

On this front, the Securities and Exchange Commission's 2018 cyber guidance is instructive.[4] Throughout the guidance, the Commission repeatedly cites to third-party "suppliers," "service providers," and "vendors" as critical to, among other things, enterprise risk, cyber incidents, and potential breach response and remediation costs. Companies are admonished to think long and hard about how service providers might be discussed in their public filings (*e.g.*, "Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk-factor disclosure."). Indeed, the fallout from a third-party breach can be significant for companies that have tight operational connectivity and integration with their vendors (*e.g.*, in the supply chain). Where companies rely on third parties not only for operational support but also for cybersecurity controls, the stakes may be even much higher. The same goes for companies that rely on service providers to provide critical e-commerce support. In these scenarios, a failure in the vendor's measures designed to protect against, identify, detect, or respond to major cyber events could materially impact the company.

Despite these warning signs, many organizations still struggle to get their arms around their service providers. A 2018 Ponemon study[5] found that 59% of survey respondents reported experiencing a data breach caused by a third party. That number increased 5% from 2017, and up 12% from 2016. More than 75% of respondents believe that third-party data breaches are increasing. But nearly one quarter of respondents admitted that they *did not know* if they had had a third-party breach in the previous twelve months. More troubling is that only 35% of respondents are confident that a third-party vendor would notify them if the vendor suffered a data breach. And only 11% are confident that a downstream fourth-party vendor would notify them of a breach.

Much has been written about the design and execution of robust vendor management programs. We do not wish to duplicate that here. It goes without saying that vendor management can impose significant costs, and we are not advocating the outsourcing of vendor management to yet another service provider (*e.g.*, companies that offer website/online scanning technology). Rather, we offer three tips on less notorious but (in our experience) effective risk mitigation moves that counsel might consider vis à vis third parties:

- **Define "Breach" Strategically, Address Cooperation, and Seek a No-Past-Breach Representation.** In the United States, the scope of notifiable data breaches is actually quite narrow as only certain types of data and certain circumstances trigger mandatory notification regimes. In vendor contracts, companies should consider what types of cybersecurity events or incidents matter in terms of managing their risk, and negotiate for definitions consistent therewith. Moreover, in our experience, companies and their vendors must cooperate with each other when a cybersecurity incident occurs that affects them both. When third-party breaches happen, regulators look at not only the security commitments that a company obtained from the vendor, but also the speed and quality of information and cooperation that the company obtains from the vendor to help to more quickly and effectively mitigate harm to any impacted consumers. Finally, we have found that it can be very helpful to include a draft contractual rep that the vendor is not aware of facts or circumstances suggesting a past "breach" (defined as discussed above). This type of rep has two benefits. First, it usually prompts a discussion with the vendor around different types of incidents that the vendor has experienced, and whether or not they are covered by the rep. Second, because many breaches trace back to hacks and other events that occurred many months or even years ago, a no-past-breach rep can provide significant leverage should the rep turn out to be untrue.
- **When Bargaining Power Is Unequal, Implement Compensating Controls.** In many situations, a service provider is so large, powerful, and essential that companies are unable to negotiate for customized contractual protections. In these situations, counsel are well advised to work with their clients to identify and implement compensating controls. This can be as simple as turning on a multifactor authentication option that the vendor offers, or as complex as implementing supplemental encryption strategies.

- ❑ **Exercise Your Audit Rights.** In our experience, when regulators investigate a breach attributable to a service provider, the fact that the company had a contractual *right* to audit compliance is becoming less and less acceptable. Regulators want to see more. Counsel should take time to identify critical vendors and, to the extent no audit process is in place, consider the possibility of some (any) checks on whether vendors are living up to their security commitments. And as regulatory requirements and expectations evolve, they should be reflected in both vendor management practices as well as in updated contractual provisions.

2. Dig Before You Get Hitched

While vendor relationships are important, it gets "real" when your company contemplates a merger, acquisition, joint venture, or major partnership deal. Recall that Verizon cut $350 million off Yahoo!'s price tag after the latter revealed three breaches involving three billion accounts. It was a defining event in cyber history. And it continues to serve as a poignant reminder to all companies—buyers and sellers, large and small, public and private—about the criticality of robust cyber diligence. It is literally true that a company can *buy* a cyber incident that subsequently exposes it to potentially substantial liability. Marriott's 2018 disclosure of a Starwood breach that allegedly began in 2014 (prior to Marriott's acquisition of Starwood) proves this unfortunate point.

According to a 2016 New York Stock Exchange and Veracode survey,[6] 22% of directors said that they would *not* acquire a company that had experienced a high-profile data breach. Nearly half of the respondents in a 2016 Brunswick Insight survey[7] said that they would discount a target's valuation based on a data breach—whether the breach was discovered before, during, or after the transaction. More recent studies suggest that while more cyber diligence is being performed, it may be resulting in fewer deals. According to a 2018 study by West Monroe Partners,[8] which analyzed survey findings over the past three years: A greater percentage of dealmakers are discovering a cybersecurity problem at the target only *after a deal has closed*—up from 40% finding post-deal problems in 2016 to 58% in 2018; nearly half of corporate buyers are dissatisfied with cybersecurity due diligence—up from 3% dissatisfied in 2016 to 49% in 2018; and executives are citing cyber-related red flags as among the top reasons for abandoning a deal.

It is important to note that comprehensive soup-to-nuts diligence is often impractical and unrealistic. M&A transactions, for example, typically involve multiple suitors competing for the same target. Compromises and concessions are part of negotiating a complex deal. Timeframes are tight. Resources are limited. It is also exceedingly difficult to find an opening, or willingness, to perform the type of technical penetration tests and compromise assessments, and compliance reviews, that a buyer might otherwise pursue.

As with vendor management, the publicly available guidance on cyber diligence is plentiful. That guidance draws from diverse viewpoints, including but not limited to banking, consulting, accounting, legal, government, and academia. Here, we offer a few insights from the buyer's perspective that, in our experience, have helped to get at the heart of the issue:

- **Nonpublic Cyber Incidents:** Because most cyber attacks and data breaches do not trigger mandatory notification rules, as with the vendor discussion above, it is important to understand whether the target has experienced broadly defined data "incidents" (*e.g.*, ransomware, DDOS, data corruption/loss, theft of proprietary information or trade secrets) and the associated remediation strategy and results. Equally important is assessing any history of noncompliance fines or penalties that are not public, such as those involving the card brands and PCI.
- **Validating Publicly Made Representations:** As discussed further below, what a company publicly says about cybersecurity in its privacy policy, terms of use, or even marketing materials is classic fodder for regulator and class action complaints. Opposing parties point to allegedly "deceptive" statements that customers and consumers relied on to their detriment. These are low-hanging fruit for enforcement cases and can be challenging to defend.
- **Reverse Vendor Management:** Where the target is a service provider/vendor, the buyer should assess whether and how the target anticipates and addresses (including through contractual protections) its own customers' compliance requirements. This is particularly important where the target's customer base or data-types are highly regulated—*e.g.*, financial services, healthcare, defense contracting, PCI/payment card data, children's data, data subject to prescriptive rules such as the EU's General Data Protection Regulation (GDPR).[9]

3. Thoughtfully Deploy Privilege

Legal counsel's role in cybersecurity has evolved significantly over the past ten to fifteen years. While lawyers traditionally were called in to reactively handle lawsuits and regulatory actions, they now contribute to shaping proactive cyber planning, assessment, and resiliency efforts, including incident response.

Apart from their legal knowledge, lawyers have always provided clients a safe place for hard debate and even harder decision-making. The American Bar Association explains that the "underlying purpose" of the attorney-client privilege is "to encourage persons to seek legal advice freely and to communicate candidly during consultations with their attorneys without fear that the information will be revealed to others."[10] It is also well established that disclosures of information to experts/consultants—who are necessary for a lawyer to render legal advice to a client—do not waive the privilege.

In the cyber context, too, the case law strongly supports privilege (and attorney work-product) protections over consultants engaged by counsel *in the aftermath of a data breach.* For example, in early 2015, the District Court for the Middle District of Tennessee denied Visa's discovery requests relating to materials produced by two security firms that Genesco's counsel engaged to, respectively, (i) investigate alleged past violations of PCI DSS, and (ii) assist in efforts to comply with PCI DSS. The court ruled that both sets of materials were protected, holding that "attorneys' factual investigations fall comfortably within the protection of the attorney-client privilege," and privilege "extends to [third-party forensic consultants] that assisted counsel in its investigation."[11] Similarly, in late 2015, the U.S. District Court for the District of Minnesota rejected class plaintiffs' move to obtain core investigative materials and communications from an internal "Data Breach Task Force" and third-party consultant Verizon—both of which were engaged and directed by Target's lawyers following the retailer's high-profile breach in 2013.[12] The court upheld Target's privilege and work-product assertions for all materials related to its "dual-track" investigation, except for a few documents that reflected CEO updates to Target's board of directors.[13]

With respect to *proactive (non-breach) cyber risk assessments*, a recent February 2019 decision from the Premera Blue Cross breach litigation[14] provides critical insights into how courts are likely to address privilege assertions. The *Premera* case stems from a data breach disclosed in 2015. Class actions were filed and discovery battles ensued. The court considered a broad range of document categories

set forth in Premera's privilege log; the highlights included analyses of privilege assertions over security audits and assessments. In this regard, the court noted as follows:

> Regarding Premera's audits and investigations of their information technology and security, Premera's general information technology and training . . . the Court is *not persuaded that these were primarily done with legal purpose and not business purpose*.[15]

Observing that "[a]s a business, Premera needs periodically to audit its information technology and security and training," the court stated that the audits "would have happened regardless of any pending litigation or regulatory investigations."[16] The court was particularly skeptical of two audits that occurred years *before* Premera's breach, referring to such audits as simply "normal business functions," and while Premera claimed that its counsel was involved in the audits, the court flatly remarked that "Premera cannot shield them from discovery by delegating their supervision to counsel."[17]

The fact that case law is now developing on the issue of cyber-related privilege makes clear that lawyers are increasingly playing a meaningful role in this space. However, there are some key lessons learned that are food for thought for both in-house and outside lawyers:

- **Non-Breach Cybersecurity Audits or Assessments:** Counsel should carefully manage client expectations and differentiate between audits or assessments that are routine "normal business functions" versus those that are truly directed by counsel for purposes of rendering legal advice. Proactive (pre-breach) work always involves trade-offs between remediation and resources (*i.e.*, tough choices are made about what to do now versus put off until later). Debates like these can generate prejudicial documents. Counsel should seek to shield them from potential discovery to the extent they are properly subject to the privilege.
- **Deploy Privilege Through "Drafts":** Even if a cyber audit or assessment might not qualify for attorney-client privilege or work-product protections, there are strategies to shield the debate and decision-making from disclosure. For example, emails to counsel that discuss the pros and cons of an audit, items to investigate or focus on, trade-offs and compromises, priorities, and key risks are legitimately privileged. In addition, as

the Premera court recognized, "[a] draft report sent to counsel seeking legal advice and input on the draft also would be privileged."[18] Another practice is to conduct oral read-outs before things are reduced to writing.

- **Engaging Public Relations (PR) Firms:** The typical incident response playbook contemplates PR/crisis communications teams being engaged through counsel for privilege purposes. However, there is mixed case law on this point. For example, some courts have distinguished between "standard" public relations services aimed at preserving a public image or reputation and PR firm communications or work product that are directly related to legal advice or litigation strategy.[19]

4. Take Your Communications Team to Lunch

In the wake of a data breach, companies must navigate a host of legal, risk, and reputational landmines. However, perhaps nothing influences liability—and drives the appetite of public and private enforcers—more than the first *external communication* that a company makes about a cyber incident.

For example, offering credit-monitoring and identity-protection services in the wake of a breach has become standard playbook practice. Indeed, consumers and employees often expect these types of services, regardless of the nature or scope of the information that was compromised. This can create tension between legal counsel who are concerned about litigation risk and business/communications professionals who want to protect brand loyalty and demonstrate the company's commitment to customers or employees.

Interestingly, the mere offering of these services may send an unintended signal—for example, where the breach does not involve Social Security numbers or other data used for identity theft (*e.g.*, medical information). In that situation, a company may face questions such as: "Was more data compromised than the company reported?" or "Does the company have evidence of identity theft attributable to the breach?" or "Are consumers at real risk of identity theft?" This is not to say the scales should tip in favor of foregoing a credit-monitoring remedy. However, a string of cases over the past several years should prompt lawyers to spend more time with their corporate communication colleagues.

- In upholding the plaintiffs' standing to sue, the Seventh Circuit in *Neiman Marcus*[20] specifically cited to the company's offer of one year of credit monitoring and ID theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. According to the court, it was "unlikely that it did so because the risk is so ephemeral that it can safely be disregarded," noting that "these credit monitoring services come at a price that is more than de minimis."[21] In other words, the court effectively used Neiman Marcus's decision to broadly offer free credit monitoring as a concession that plaintiffs faced nonspeculative and imminent risk of harm, warranting their mitigation expenses.
- In the *P.F. Chang's*[22] case, the Seventh Circuit likewise pointed to what it described as an "implicit" admission that compromised card data could be used to open new cards because P.F. Chang's "encouraged consumers to monitor their credit *reports* (in part for new-account activity) rather than simply the statements for existing affected cards."[23] Thus, the company's cautionary reminder to monitor credit reports—a statement that many states statutorily require companies to include in breach notifications—rendered the plaintiffs' purchase of a credit-monitoring service and efforts to guard against ID theft reasonable mitigation expenses sufficient for standing purposes.
- In *Nationwide Mutual Insurance*,[24] the Sixth Circuit relied, in part, on Nationwide's offer to provide credit monitoring as evidence of the reasonableness of mitigation expenses for standing purposes. But the court further noted that Nationwide had recommended that consumers consider putting a freeze on credit reports, explaining that such freezes could impede the ability to obtain credit and that it could cost a fee between $5 and $20 to place and remove such freezes. Notwithstanding that some states require companies to advise consumers about the availability of a credit freeze (*e.g.*, Massachusetts), the Sixth Circuit, in ruling for the plaintiffs, pointed to Nationwide's credit freeze advice, the associated costs, and Nationwide's failure to offer coverage for those costs.

This is not to say that lawyers should ring the alarm bells on post-breach notifications. Rather, in our experience, early brainstorming, sharing of case law (such as the cases mentioned above), and coordination can help to reduce the risk that breach notifications catch company stakeholders by surprise when they are later

quoted in legal briefs and court orders. In addition, we offer the following lessons learned, which can be included in every lawyer's next discussion (hopefully over lunch) with her communications colleagues:

- **Early Announcements Can Be Risky.** The above cases serve as a cautionary tale for making public announcements regarding a security incident before the internal and forensic investigation is complete. To the extent that reputational and other considerations (*e.g.*, leaks) demand early communications, organizations should be very careful in disseminating information too broadly (*e.g.*, sending an email alert to all employees about a potential security incident) or in over-disclosing to external stakeholders.
- **One Size May Not Fit All for Precautionary Messages.** It is critical to understand the nuances of the state-specific notification requirements. Many states (including Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming) explicitly require that the reporting company include specific recommendations to consumers on risk mitigation, including encouragement to monitor credit reports. However, notwithstanding variations across state rules, a commonly accepted practice is for organizations to issue a standard notification that complies with substantially all of the states' various requirements (except Massachusetts), and supplement certain notifications based on state-specific requirements (*e.g.*, instructions on contacting a specified state agency/regulator). This means that all of the various state-required language and disclosures are often provided to all individuals, even if not entirely applicable. Although they often reflect sound security practices that consumers should follow in any circumstance, organizations should recognize the risk in making risk-mitigation recommendations, and consider whether to provide them only to consumers whose individual state's law explicitly requires it.
- **Carefully Describe Protective Measures.** Certain state statutes require disclosure of the measures taken to contain, mitigate, or minimize the incident. For example, Michigan directs that notifications "generally describe what the [company] providing the notice has done to protect data from further security breaches."[25] Wyoming requires a description in general terms of "the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches."[26] Similar requirements exist in North Carolina, Vermont, Virginia, and elsewhere. However, these types of statements

have been used to infer the scope of individuals who were affected. Thus, although statutorily required, these cases demonstrate why organizations should thoughtfully articulate the containment/remedial measures taken in response to an incident.

- **Rigorously Analyze Voluntary Notifications.** In our experience, even if a cyber incident does not technically trigger a notification requirement, companies often "voluntary" notify affected parties. They do so for a host of different reasons. We see counsel's role as helping stakeholders to assess the pros and cons of voluntary notification through decision trees that account for downside and upside (*e.g.*, the likelihood that voluntary notice will enable customers to take meaningful self-help steps).

5. Don't Forget About Privacy

A few years ago, the Federal Trade Commission wrote a blog post that highlighted key issues companies should expect to be asked about in cyber investigations. Among other things, the FTC explained that the agency looks at "privacy policies and any other promises the company has made to consumers about its security."[27] Indeed, most FTC cyber enforcement cases turn on allegations that a company made misleading statements regarding the type, strength, or even presence of security measures associated with its product or services. Offending statements can appear in a variety of contexts, including privacy policies, terms of service, marketing materials, and even investor-relations materials, just to name a few.

In this vein, the Third Circuit's landmark decision in *FTC v. Wyndham Worldwide Corp.*[28] is instructive. On three occasions in 2008 and 2009, hackers allegedly exfiltrated payment card data of more than 619,000 Wyndham guests. The FTC brought an enforcement action under the unfairness prong of section 5 of the FTC Act,[29] arguing that Wyndham's security practices "unreasonably and unnecessarily" exposed personal data to unauthorized access and theft. The complaint also raised a deception claim for allegedly misleading statements in the company's privacy policies. Those policies contained allegedly false representations that data was protected according to "industry standard practices" and "commercially reasonable efforts," such as using "128-bit encryption," "fire walls," and "other appropriate safeguards."

Although the FTC's deception claim was *not* on appeal, Wyndham's privacy policy emerged as a critical factor in the decision upholding the unfairness claim. The court noted that a company does not act equitably when it "publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business." Moreover, "consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a misleading privacy policy that overstated its cybersecurity."[30] Finding it plausible that consumers were misled by Wyndham's privacy policy, the court deemed the policy "directly relevant" to whether the company's conduct was "unfair."

Private plaintiffs routinely allege that companies not only fail to protect data (thereby resulting in a breach) but deceive consumers in privacy policies with security-related misrepresentations. For example, these types of allegations featured heavily in complaints against Marriott following its 2018 announcement that Starwood databases had been breached starting in 2014 (*e.g.*, "Ultimately, Marriott could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations Marriott made to the public in its marketing materials and privacy statements, and compliant with industry standards, best practices, and the requirements of [ ] State law. Unfortunately, Marriott failed to do so, and as a result, exposed the personal and sensitive data of hundreds of millions of consumers.")[31]

We offer the following tips for identifying potential privacy-related cyber exposure points:

- ❑ **Check What Your Company Publicly States About Security.** Be thoughtful about the fine line between transparency that informs customers on the ways in which you collect, use, share, store, and transfer data and vague language or catch phrases—such as "industry standard security," "bank-level encryption," or "we do everything we can do to secure your data"—that can land a company in hot water. Decide whether detailed statements about your plans, protocols, processes, and tools are necessary and generate any value. Avoid overstating your security practices or implying that a high level of security is applied across the board

if in fact it is applied in more limited circumstances (*e.g.*, subsets of data, data in-transit versus at-rest, applied by the company but unknown for service providers).

- ❑ **Regularly Refresh Assessments of Publicly Made Statements.** All external (consumer-facing) representations should be reviewed no less than twice per year. Reviews should be accelerated as part of privacy-by-design processes any time new products or services will be deployed. Counsel should conduct these reviews as group exercises with mandatory participation by IT/InfoSec and Marketing/e-commerce (which often have first line-of-sight to new tools and technology being considered and deployed).
- ❑ **Consider Reasonable Security Disclaimers.** We regularly see privacy policies that trumpet claims like "Security Guaranteed" and "Bank Level Security" (often by nonfinancial services entities!). Given the shifting cyber threat landscape, virtually any assurance regarding security is susceptible to legitimate scrutiny. This is why many companies include blanket disclaimers that security measures may change, be unavailable from time to time, or even circumvented by sophisticated actors (*e.g.*, "We cannot guarantee 100% security. No security is fail-proof."). Competent judgment is required to strike a thoughtful balance: Any legal benefits that disclaimer language may provide should be weighed against the PR/business impact of being viewed as shifting risk to the consumer. And even though disclaimers are not a panacea, they can at least provide arguments regarding what consumers should reasonably expect.

6. Mind Your Directors and Officers

In-house counsel, and outside counsel who work with them, technically represent the company. They are fiduciaries to the corporate entity, which has as its highest authority the board of directors. Accordingly, an important part of the general counsel's role is to provide sound legal compliance and legal risk-mitigation advice to the board.

While it is a new risk, cybersecurity falls squarely within the traditional "risk oversight" obligations of corporate directors. Directors have fiduciary duties to act in good faith and with care and loyalty, which, in the cyber context, includes directing management to design, implement, and enforce a robust cybersecurity compliance program. To effectively do so, directors must be educated and

informed about the company's risk profile, threat actors, and strategies to address that risk; they must receive regular briefings from management and metrics to understand progress toward the desired state.

Indeed, the Securities and Exchange Commission recently emphasized the criticality of the board's cyber activities to the marketplace.[32] In its 2018 cyber guidance, the SEC stated that disclosure in annual reports or proxy statements of the board's role in risk oversight of a company pursuant to Item 407(h) of Regulation S-K *should* include a discussion of the nature of the board's role in overseeing the management of cybersecurity risks that are material to a company's business. In addition, the SEC observed that disclosures on how the board engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility in cybersecurity matters.

The foregoing is not surprising given the potential severity that breaches can have on a company's performance and value, including its brand and reputational assets. That has spurred shareholder derivative suits against directors and officers in the aftermath of major data breaches. In these suits, plaintiffs allege that the directors and officers failed to ensure effective cybersecurity programs, recklessly ignored security warnings and various red flags, and, as a result, the company had inadequate controls and procedures to protect personal and financial information against unauthorized access and acquisition.

We offer three insights from the frontlines of governance work that we believe have the dual benefit of not only helping to mitigate risk for the company, but also helping directors and officers to fulfill their cyber fiduciary duties:

- **Practice with Your InfoSec Team.** While cyber risk is not "new," its high level of board attention is certainly new. InfoSec teams, often for the very first time, are in the boardroom and are responsible for educating the board on the company's risk profile, vulnerabilities, current security state, and road map for remediation and sustained risk management. Accordingly, the InfoSec team needs practice and guidance from counsel (*e.g.*, regulatory and litigation perspectives) to be most effective in communicating with the board. Counsel's early involvement is particularly important when the board will assume a more active role—for example, where InfoSec conducts a board-level incident response tabletop or discusses ransomware attacks and the issue of who in the company decides whether to pay.

- **Vertically Integrate InfoSec with the Governance/Disclosures Team.** From a governance perspective, many companies do not involve their InfoSec teams in the risk disclosures process and committee. Especially for public companies, lawyers can help to establish a channel for reporting cyber events, and the appropriate board committee (whether the Audit, Risk, or even Cybersecurity Committee) can thereby gain experience around assessing events for disclosure filing purposes.
- **Implement Trading Blackout Protocol for Cyber Events.** Based on the 2018 SEC cyber guidance, lawyers should assess whether procedures are in place to determine whether implementing a trading blackout period while the company investigates and assesses the significance of a cyber incident is appropriate and should review insider trading policies to ensure they prohibit insiders from trading when in possession of material non-public information relating to cyber risks or incidents.

7. Assess Your Risk Assessments

Cyber risk assessments come in dozens of flavors. They can involve enterprise or product level analyses; focus on people, processes, or technology (or all three); be limited to certain systems or all of them; and relate to the company or its service providers (or both). But what *all* risk assessments have in common is that they identify lots of "opportunities" for improvement. For that reason, both regulators and private plaintiffs demand them in discovery. The absence of a risk assessment can be a red flag, *and* the presence of unaddressed recommendations arising out of risk assessments can form the basis for alleged liability in a data breach or even a security-vulnerability case.[33]

For legal counsel, risk assessments are relevant and useful in a number of respects. For example, risk assessments can play a key role in helping to evaluate the vendor management program, as well as helping to assess the vendors' own security programs. They can also be leveraged to evaluate cyber or privacy issues related to an acquisition target, or leveraged by a target company to ready itself for acquisition or other major transaction (or even a cyber insurance underwriting). Risk assessments can also be used to benchmark a company's overall security program or elements of its incident response against regulatory requirements, industry standards/best practices, or customer requirements. In some cases, an enforcement agency may request a risk assessment in the aftermath of a breach or

as part of a settlement. Having a recent assessment already done in the ordinary course of operation can go a long way in demonstrating diligence and mitigating regulatory scrutiny.

As with any audit or assessment, the challenge for companies is prioritizing and executing on the remediation plan. While some companies have robust processes for identifying corrective actions, road maps, milestones, and funding requirements, many companies struggle—and thereby, unintentionally create an unfavorable paper trail and precedent.

This last point was driven home in the Financial Industry Regulatory Authority's (FINRA) investigation and consent order against Sterne Agee in 2015.[34] Sterne Agee is a registered broker-dealer based in Alabama. The company found itself embroiled in one of FINRA's very few cyber enforcement actions, largely due to the following fact pattern:

- In May 2014, an employee inadvertently left a laptop with personal data related to over 350,000 consumers in a public restroom, and it was stolen. The laptop was not encrypted.
- Previously, as early as March 2009, the company recognized the need for laptop encryption but considered it a "moderate risk," due to a low laptop count. As the number of laptops grew, the associated risk of not implementing encryption also grew.
- By 2010, the company had approved the purchase of Microsoft's BitLocker encryption software.
- In 2010 and 2011, BitLocker was not installed on any laptops because the company needed additional IT personnel. Funding for those personnel was not approved until 2012.
- In 2012, when the newly hired personnel attempted to install BitLocker, it was found to be incompatible with the company's laptops.
- Employee turnover subsequently delayed the company's identification of a compatible encryption solution, but funding for the solution was not approved until June 2014—*after* the unencrypted laptop was stolen.

The *Sterne Agee* case is an extreme example of a simple proposition familiar to every lawyer: Repeated identification of the same risk can expose the company to potential liability. This proposition has made its way into regulator actions and

class action complaints. For example, the FTC has explained that in cyber investigations, the agency requests and reviews "materials like audits or risk assessments that the company or its service providers have performed."[35] On the class action side, plaintiffs in the Equifax breach litigation alleged that the company failed to remediate known security deficiencies and repeatedly ignored warnings from third-party consultants. One senator summarized her findings on this point following congressional hearings and investigative activities:

> Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability—but then failed to confirm that the fixes were made. . . .
>
> Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems . . . and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed—or was unable to effectively heed—these warnings.[36]

While it is certainly easy for outsiders to critique in hindsight, the tone and tenor of the allegations clearly set forth a road map for identifying key exposure points. We offer three thoughts on how lawyers might leverage cyber assessments to help proactively manage enterprise risk:

- Focus on Repeat Items: Lawyers should hone in on documented weaknesses, warnings, and action items that continue to show up from audit to audit or assessment to assessment, particularly those that map to noncompliance with a specific law, regulation, or contractual requirement (*e.g.*, PCI DSS). Depending on their criticality and remedial potential (*e.g.*, if fixes are reasonably available), these repeat items can form the basis for serious regulatory and private liability—particularly if any even arguably contribute to a future data breach. Of course, context is always relevant to assessing liability exposure. For example, remediation recommendations must be viewed in the context of whether the risk item was deemed "accepted risk" by the company; the probability of the risk event occurring is also relevant; and counsel should probe whether compensating controls exist to mitigate the risk item's criticality for prioritization purposes.

- Deploy Privilege Via Emails and "Drafts": As discussed above, risk assessments are a double-edged sword—helping to *identify* security risks while simultaneously *creating* remediation risks for the enterprise. Thus, it bears repeating that even if a cyber audit or assessment might not qualify for privilege or work-product protections, there are strategies to shield legitimate debate and decision-making. Lawyers should be consulted *precisely* in situations where trade-offs must be made between remediation and resources—as these choices often carry significant legal compliance, regulatory, and litigation risk repercussions. Drafts of reports sent to counsel for legal advice, as well as emails and conversations that occur outside the four corners of an assessment, are almost always covered by the attorney-client privilege.
- Focus on Assessments That Are Tightly Linked to Strict Legal Requirements: In our experience, risk assessments produce broad recommendations that cover a lot of ground, including actions that range from necessary to advisable to nice-to-have. Counsel should work with business and security teams to develop a defined schedule on the corporate calendar for conducting risk assessments in areas like HIPAA and PCI that produce specific, targeted remediation recommendations. In addition to being able to identify specific issues, there is value in being able to demonstrate a culture of compliance should the company experience a public breach or regulator investigation.

* * *

Cyber risk is constantly evolving, intensifying the enforcement risk that companies face from both regulators and private litigants. As lawyers are increasingly involved in proactive risk management, our hope is that at least some of the "easier" wins discussed in this article allow counsel to add value to the process. Of course, there is never enough time, enough money, or enough people to do everything. But prioritized, targeted work holds the best potential for mitigating cyber risk for the enterprise and its stakeholders.

Aimee Nolan is Vice President, Associate General Counsel and Chief Intellectual Property Counsel at W.W. Grainger, Inc. **Jason Smolanoff** is a former FBI Supervisory Special Agent, and currently is a Senior Managing Director, Global Cyber Risk Practice Leader at Kroll. **Antony (Tony) Kim** is a partner and co-founder of Orrick, Herrington & Sutcliffe LLP's Cyber, Privacy & Data Innovation Practice.
A version of this article has been published in the Course Handbook for PLI's Twentieth Annual Institute on Privacy and Data Security Law.

NOTES

1. The CCPA provides that any consumer whose non-encrypted or non-redacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure due to security failures on the company's part can sue "to recover damages in an amount not less than $100 and not greater than $750 per incident or actual damages, whichever is greater." Cal. Civ. Code § 1798.100 *et seq.*
2. The Telephone Consumer Protection Act (TCPA) provides a private right of action for "actual monetary loss from such a violation [or] $500 in damages for each such violation, whichever is greater." 47 U.S.C. § 227(b)(3) (also providing for trebling of damages if a court finds willful or knowing violations).
3. Soha Systems, Third Party Access Is a Major Source of Data Breaches, Yet Not An IT Priority (Apr. 2016) (online survey of over 219 IT and security C-level executives, directors, and managers).
4. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. pts. 229, 249 (2018).
5. Ponemon Institute, Data Risk in the Third Party Ecosystem (Nov. 2018).
6. Cybersecurity and the M&A Due Diligence Process: A 2016 NYSE Governance Services/Veracode Survey Report (2016), www.nyse.com/publicdocs/Cybersecurity_and_the_M_and_A_Due_Diligence_Process.pdf.
7. Brunswick Insight, Brunswick Data Valuation Survey (Oct. 2016), www.brunswickgroup.com/media/2365/2016-brunswick-data-valuation-survey.pdf.
8. West Monroe Partners, Cybersecurity Issues in M&A Continue to Grow (White Paper 2018).
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), 1.
10. Am. Bar Ass'n, Task Force on the Attorney-Client Privilege, Task Force Report to the ABA House of Delegates 4 (2005), www.americanbar.org/content/dam/aba/directories/policy/2005_am_111.authcheckdam.pdf.
11. Genesco, Inc. v. Visa USA, Inc., No. 3:13-cv-00202 (M.D. Tenn. Mar. 25, 2015).
12. *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522 (D. Minn. Oct. 23, 2015).
13. *See also In re* Experian Data Breach Litig., No. 15-01592 (C.D. Cal. May 18, 2017) (reports created by Mandiant consultants retained by outside counsel deemed to be attorney work product).
14. *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 2019 WL 464963 (D. Or. Feb. 6, 2019).
15. *Id.* at *7 (emphasis added).
16. *Id.*

17. *Id.*
18. *Id.* at *8.
19. *Compare* McNamee v. Clemens, 2013 WL 6572899 (E.D.N.Y. Jan. 30, 2013) (no privilege; PR firm only provided standard services not necessary in order to provide legal advice, and therefore disclosing documents to firm resulted in waiver), *with* King Drug Co. v. Cephalon, Inc., 2013 WL 4836752 (E.D. Pa. Sept. 11, 2013) (privilege applied; consultants preparing business and marketing plans were the client's "functional equivalent").
20. Remijas v. Neiman Marcus Grp. LLC, 794 F.3d 688 (7th Cir. 2015).
21. *Id.* at 694.
22. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).
23. *Id.* at 967.
24. Galaria v. Natiowide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016).
25. Mich. Comp. Laws Ann. § 445.72(12)(6)(e).
26. Wyo. Stat. Ann. § 40-12-502(e)(v).
27. M. Eichorn, *If the FTC Comes to Call*, Fed. Trade Comm'n Bus. Blog (May 25, 2015), www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call.
28. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
29. 15 U.S.C. § 45(a).
30. *Wyndham*, 799 F.3d at 245–46.
31. Complaint, Hiteshew v. Marriott Int'l, Inc., No. 8:18-cv-03755 (D. Md. Dec. 6, 2018).
32. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. pts. 229, 249 (2018).
33. The FTC has exercised its prosecutorial discretion to investigate and bring actions against companies for security vulnerabilities even in the absence of any data breach. *See, e.g.*, Complaint, FTC v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. Jan. 5, 2017).
34. FINRA Letter of Acceptance, Waiver and Consent, Sterne, Agee & Leach, Inc. (Respondent), No. 2014041619501 (May 22, 2015).
35. *See* Eichorn, *supra* note 27.
36. Sen. Elizabeth Warren, Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information 1 (Feb. 2018), www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf.