Hughes Hubbard & Reed

cybXsecure

Primer on Cybersecurity for Boards of Directors

By Roel C. Campos and David X Martin

Hughes Hubbard & Reed LLP
A New York Limited Liability Partnership
One Battery Park Plaza
New York, New York 10004-1482
+1 (212) 837-6000

HOW DO DIRECTORS COPE WITH THEIR OBLIGATIONS TO OVERSEE CYBERSECURITY?

A Practical Primer for Boards of Directors in the Age of Uber, Equifax et al.

By Roel C. Campos and David X Martin*

Directors' Cyber Checklist

Risk Assessment: Evaluate the Existing Cybersecurity Risks, and Prioritize

- ☐ Determine most valuable assets
- ☐ Seek effective strategies to protect them
- ☐ Review cybersecurity budget for appropriateness

Assess Corporate Culture and Set the Right Example

- ☐ C-suite and board must be more than involved, they should set the tone
- ☐ Training should be engaging
- ☐ Culture should be based on teamwork not surveillance

Develop Strategies and Internal Systems to Manage Cyber Risk

- ☐ Evaluate effectiveness of internal systems and controls
- ☐ Participate in selecting key cybersecurity personnel
- ☐ Make sure cybersecurity personnel have board access
- ☐ Understand and develop metrics for evaluating cybersecurity effectiveness
- ☐ Take a hard look at escalation protocols
- ☐ Request a security scorecard
- ☐ Develop an incident response plan
- ☐ Test the plan and consider simulated cyberattacks

Understand Disclosure Requirements and Third-Party Considerations

- ☐ Review disclosures with an eye toward cybersecurity
- ☐ Put mitigating controls in place for third-party contracts
- ☐ Review cyber insurance coverage

Stay on Top of Developments

- ☐ Regularly reassess your cyber plan in light of the shifting legal landscape
- ☐ Initiate standing review of cyber program on at least a quarterly basis
- ☐ Task general counsel and/or CISO with briefing board on regulatory developments
- ☐ Leverage preexisting relationships with outside counsel

---

* *Roel C. Campos is a former SEC Commissioner who practices SEC securities enforcement defense and regulation law as a partner at Hughes Hubbard & Reed LLP, and regularly advises boards of directors on securities issues. David X Martin is a well-known risk and business cybersecurity expert. Roel and David serve as co-chairs of the Directors and Chief Risk Officers Group (DCRO) Cyber Risk Governance Council. Together, their collaboration in this article has produced a practical common-sense approach, with the necessary legal background, to be useful to directors and management professionals to assist in evaluating the cybersecurity program at a company.*

The authors would like to thank Alyssa Johnson and Elizabeth Solander, also of Hughes Hubbard & Reed LLP, for their significant contributions to this article.

HOW DO DIRECTORS COPE WITH THEIR OBLIGATIONS TO OVERSEE CYBERSECURITY?

Many directors understand they have a responsibility to oversee cybersecurity at their companies. But more puzzling is what they should be doing now to contribute to the board's effort. What are the right questions they should be asking? Below we provide a short discussion of the major areas in cybersecurity compliance that you should be concerned with. We invite you to keep this article in your files for your director references and duties, and use the checklist at the beginning of this article when discussing cybersecurity at board meetings.

INTRODUCTION

On September 7, 2017, one of the nation's largest credit monitoring agencies, Equifax Inc., announced that over 143 million customers' accounts had been breached in what may be the most significant cyberattack to impact U.S. consumers to date.[1] The number of affected individuals has since risen to an estimated 145 million people—all of whom likely had their personal information, including their names, Social Security numbers, birth dates, addresses, and driver's license numbers, compromised in the attack.[2]

Amidst the Equifax controversy, the U.S. Securities and Exchange Commission ("SEC") made some striking disclosures of its own. The newly-arrived SEC Chair, Jay Clayton, announced on September 20, 2017 that the SEC's own EDGAR filing system had been penetrated by cybercriminals months previously, leading to questions about the safety of such systems and the risk of insider trading by individuals with advance knowledge of sensitive, nonpublic company information.[3]

Other recent high-profile cyberattacks abound. Much to the chagrin of fans of the popular television show *Game of Thrones*, the HBO television network was breached in July 2017 by a group that pilfered over 1.5 terabytes of information, including show scripts and full episodes of several prominent shows.[4] And on September 25, 2017, *The Guardian* revealed that Deloitte LLP, one of the "Big 4" accounting firms (whose advisory clients include large companies and government departments) had been the victim of a breach and had its internal email system compromised.[5] Deloitte has since notified six of its clients whose information may have been "impacted" by the breach, and an internal investigation into the incident is ongoing.[6]

In one of the more salacious stories, recent revelations from Uber Technologies, Inc. detail a 2016 breach of the ride-sharing company's systems, during which hackers stole the names, email addresses, phone numbers, and drivers' license numbers of millions of Uber's customers and drivers. Not only did Uber fail to disclose the breach for over a year—but it also purportedly paid a "ransom" to the hackers in exchange for a promise by the hackers to delete the purloined data and keep the cyber incident quiet.[7]

Although cybersecurity is not a new challenge for boards of directors, the sheer scope and volume of recent events suggest that we may be experiencing a watershed moment when it comes to directors' responsibility to oversee, and managers' duty to implement, adequate cybersecurity systems at companies. Following Equifax's public disclosure of the cyberattack affecting its systems, observers learned a good deal about what potentially went wrong at the company—including a series of red flags that senior managers and boards of directors at other companies may learn from. Taken together, the

---

* *Roel C. Campos is a former SEC Commissioner who practices SEC securities enforcement defense and regulation law as a partner at Hughes Hubbard & Reed LLP, and regularly advises boards of directors on securities issues. David X Martin is a well-known risk and business cybersecurity expert. Roel and David serve as co-chairs of the Directors and Chief Risk Officers Group (DCRO) Cyber Risk Governance Council. Together, their collaboration in this article has produced a practical common-sense approach, with the necessary legal background, to be useful to directors and management professionals to assist in evaluating the cybersecurity program at a company.*

The authors would like to thank Alyssa Johnson and Elizabeth Solander, also of Hughes Hubbard & Reed LLP, for their significant contributions to this article.

recent breaches reveal a series of lessons and warnings that boards of directors simply cannot afford to overlook anymore.

The first lesson is that companies must pay attention to routine alerts warning of cyber vulnerabilities in the company's systems and in software the company uses. In Equifax's case, hackers apparently exploited a known network vulnerability in the Apache Struts web-application software, which Equifax used to build its web applications. The U.S. Department of Homeland Security's United States Computer Emergency Readiness Team ("US-CERT") notified Equifax and many others of this vulnerability and the need to patch the software on March 8, 2017. Although the company disseminated the US-CERT notification internally by email and requested that appropriate personnel apply the patch, the patch was apparently not installed, or not installed correctly, and follow-on scans of the system one week later failed to reveal the error.

The second lesson is that companies must ensure they have appropriate systems in place to escalate information about potential cyber incidents and ensure, for example, that the general counsel imposes a freeze on trading in the company's securities by individuals with insider knowledge of material breaches during key windows. In Equifax's case, it was revealed that several executives had traded in the company's stock after the breach had been reported internally but before the public had knowledge of the breach. This raised questions about possible insider trading and a lack of internal controls at a time when Equifax was already subject to intense public scrutiny over the breach itself. (The executives have since been cleared of wrongdoing by a special committee at Equifax tasked with analyzing the breach.)[8]

The third lesson is that boards of directors must have a public response plan in place should a catastrophic cyberattack occur on their watch. Equifax's public handling of the incident has been widely criticized from virtually all angles. Many, for example, have complained that it took the company a full month to disclose the incident publicly after the company first learned of the breach in late July 2017. Others have ridiculed Equifax for directing consumers, in the immediate aftermath of the breach, to an insecure "spoofed" website mimicking the one Equifax had set up to engage with customers anxious to learn if their personal information had been compromised. Still others lamented that the company appeared to be in "PR mode" following the breach, and made missteps such as offering credit monitoring services to affected individuals for a fee, rather than free of charge. (The company later moved to offer victims free access to credit monitoring services, but forced those customers to agree to lengthy arbitration provisions which would limit the customers' ability to sue Equifax in connection with the services. Equifax later abandoned the arbitration clause after a public outcry.)[9] All of these events suggest that Equifax was ill-prepared to deal with the public fallout that would predictably ensue following a disclosure of this magnitude.

The fourth lesson is that companies should carefully consider when and how they will disclose a breach. The recent disclosures of cyber incidents at Equifax and Uber provide valuable guidance to boards of directors in this regard. A company must consider not only its legal disclosure obligations, but also the court of public opinion when assessing when, and what, to disclose. In a similar vein, some have pointed out that the SEC's public disclosure of a cyber incident involving its EDGAR database came months after internal reports of the event were raised, illuminating just how difficult it is for any actor—including those charged with overseeing disclosure-based conduct—to balance the competing needs for a speedy public disclosure and a thorough internal review. The SEC's own less-than-ideal response to a cyber breach (and a resulting delayed cyber disclosure) raises questions about how the agency will pursue companies for cyber-related disclosures in the future and balance the competing needs for prompt disclosures on one hand, and rigorous internal reviews on the other.

A final lesson is that companies should be aware of the risks posed when third parties handle

sensitive company data. The events at Deloitte provide yet another data point and reinforce the notion that companies must be concerned not only with their own cybersecurity systems, but also those of third-party vendors and consultants (and even, perhaps, the government) when those entities handle sensitive company data.

Given these recent high-profile events, we discuss below a series of practical considerations and principles that a board member can use to help the board build an effective and dynamic cybersecurity program at his or her company. These considerations will also help a director test the current status and effectiveness of the cybersecurity program.

PRACTICAL CONSIDERATIONS FOR DIRECTORS

As a first principle, directors should understand their fiduciary duties when it comes to cybersecurity and the overarching legal terrain guiding their companies. In addition to business and reputational risks, a lapse in cybersecurity can result in significant legal consequences for a company, its management, and, in certain cases, its board of directors. Companies must be aware of and understand various federal and state statutes, some of which regulate specific industries or types of sensitive information. Companies must also be aware that federal and state regulators, such as the SEC, DOJ, and FTC, may increasingly focus on cybersecurity when enforcing otherwise non-cyber-specific laws, such as federal consumer protection and securities laws. In addition, directors must also heed the risk of shareholder and consumer lawsuits, which are commonly initiated in the wake of the disclosure of cybersecurity incidents. As discussed below, the company's general counsel and internal cyber personnel should schedule regular briefings for the board to assess these developments.

Cyber Breaches by the Numbers. The *2017 Data Breach Investigations Report* by Verizon provides useful data on the type and frequency of common cyber breaches. For example, the report found that cyber breaches often involve:

- Some form of hacking (62%)
  - stolen or weak credentials (81% of hacking-related breaches)
- Malware (51%)
  - malicious email attachments (66% of all malware installed);
- Physical actions (8%)
- "Social" tactics (43%)
- Privilege misuse (14%)

Source: Verizon, 2017 Data Breach Investigations Report 3 (10th ed. 2017), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

1. Take Stock of Existing Cybersecurity Risks and Prioritize

Cybersecurity is a "first order" risk in many industries. If they have not already done so, boards of directors should invest in a formal briefing to discuss the range of existing cybersecurity risks facing their companies and weigh the pros and cons of various mechanisms that may help protect the company's most valuable assets in light of those risks.

The board should first identify the company's most valuable assets and evaluate how those assets might be compromised by a cyber incident. For some companies, their most valuable asset is customers' private financial information, personally identifiable information, or possibly health records. For others, it might be intellectual property, or perhaps a proprietary database, or even a cache of sensitive emails. Any cybersecurity program must be geared towards protecting these most important corporate assets.

Directors should have a baseline understanding of the various types of cyber breaches that may occur on company systems and be familiar with the technical terms frequently used in the industry. Common cyber incidents at companies may range from malware to phishing attacks, and from unpatched software vulnerabilities to advanced persistent threats ("APT"). Additionally, vulnerabilities in a company's physical security may allow actors to penetrate the company's cyber defenses.

While it is not necessarily incumbent on the board to study the technical mechanisms of a cyberattack or response thereto, the board should have enough familiarity with these concepts to enable productive discussions with management and effective oversight of the company's cybersecurity program.

In taking stock of existing cybersecurity risks, boards should pay close attention to trends and recent events in their particular industry and impacting companies of a similar size. Particular types of cyberattacks appear more frequently in some industries, and less in others. If you are a small retailer, for example, your most pressing cybersecurity concern may be point of sale intrusions, where attackers exploit weaknesses in remote-access applications (often provided by third-party vendors) in order to siphon your customers' credit card payment information.[10] On the other hand, if you are a large financial institution with sprawling and accessible physical infrastructure (*i.e.*, ATM machines), then you may face a broader range of cyber vulnerabilities, including the risk of "skimming" attacks on individual nodes in the network.[11]

Directors should also have a broad understanding of who or which groups are most likely to target their companies, and for what purpose. As a starting point, the *2017 Data Breach Investigations Report* by Verizon ("2017 Verizon Report") suggests that the majority of cyber breaches are perpetrated by external threat actors (75%), while a smaller percentage are perpetrated by insiders, such as employees or former employees (25%).[12] A growing number of breaches can be traced to state-affiliated actors (18%), while a smaller percentage involves business partners (2%).[13]

Once the board has a good handle on the company's existing cyber threat profile, it should prioritize strategies to mitigate the risk of an actual cyber breach. An effective director will help the company determine which assets are most valuable and evaluate the key controls in place to protect them.

He or she will also plan for contingencies and ensure there is an appropriate response framework in place to deal with potential cyber incidents. Part of this exercise will inevitably entail reviewing the company's budget related to cybersecurity to determine whether it is appropriate in light of existing threats and the robustness of existing company systems. (Keep in mind that it is less expensive to prevent a problem than it is to fix it.)

One key takeaway is that there are no offensive strategies in cybersecurity—only defensive strategies. In addition, you cannot protect everything. Even the most technologically advanced organization in cyber—the National Security Agency ("NSA")—could not protect its deepest secrets.[14] It is therefore critical for the company to (1) reflect on which company assets are most valuable, (2) determine which systems are most vulnerable, and (3) consider what available mechanisms and strategies are both business-critical and cost-effective in view of this calculus.

Understanding Motive. What motivates perpetrators of cyber breaches? The answer is straightforward in some cases, and more complicated in others. (In short, "it depends.") Below is a basic framework a director may consider.

Financial

- Attacker wishes to obtain sensitive nonpublic market-changing information to facilitate profitable trades using that information.
- Attacker wishes to obtain personally identifiable information to facilitate identify theft.
- Attacker wishes to obtain corporate or trade secrets to undercut competitors or other market participants.

Espionage/Surveillance

- State actor wishes to obtain personal or proprietary information for political or economic uses.
- The unusual case: State actor wishes to retaliate against a company or shut down controversial operations (e.g., the 2014 hack of Sony Pictures).

Ideological

- "Hacktivist" or similar group seeks to obtain nonpublic information in order to release it to the public on ideological grounds.

2. Assess Corporate Culture and Set the Right Example

Firms that really "get it" in cybersecurity have adaptive cultures. However, most corporate cultures do not change quickly—they evolve at a slow pace. As a result, the security culture in many organizations has not kept pace with the threat landscape in which they operate.

Security needs to be framed as a critical enabler that helps the company deliver its promise to customers. It also needs to be viewed by all levels of the company's workforce as a shared endeavor based on *teamwork, not surveillance*.

> *According to a recent survey by Diligent Corporation presented at the NYSE Governance Services Cyber Risk Forum,* ***60% of directors say they regularly use personal email to conduct company business****, while* ***49% report it is a "common practice" to download board books and company documents on personal devices****.*
>
> Source*:* NYSE Governance Services & Diligent, The Price of Convenience: Communications, Cyber Risk, and Cybersecurity Practices of Corporate Boards (2017), https://www.nyse.com/publicdocs/Diligent_Board_Comm_Report_2017.pdf.

Also consider the "tone at the top" of your company and the messages that are being sent to employees related to cybersecurity practices. Encourage senior management to cultivate an environment where everyone has shared responsibility for cybersecurity.

Ideally, employees should have a direct line of communication with someone in the department of the company's chief information security officer ("CISO"), and understand they can reach out to that person for judgment and hassle-free guidance.

It is also crucial that company management invest in quality employee training related to cybersecurity. It is now considered a best practice that employees receive a general security awareness training, which may focus largely or exclusively on cybersecurity. Also, training should not be a "one-and-done" exercise. The CISO's department or the GC should regularly provide updates to employees via email on recent developments in cybersecurity and issues they should be aware of. This is the kind of constant reinforcement that cultivates a true culture of cyber "wellness."

A good place to start in evaluating a company's cybersecurity culture is to review the company's written and formal guidance on the use and protection of company systems. Does the company, for example, have a written policy regarding employees' use of personal email to conduct company business? How is that policy implemented and observed? Does the board abide by the same standard, or are there exceptions made? Ideally, directors will be able to lead by example. Understand that as a director, you may be a particularly attractive target for a cyber breach, as it is known that directors often use personal devices to download board books and communicate about sensitive, non-public company information.

In all, a culture of cyber wellness needs to become a strategic focus embedded in the day-to-day operations and core values of the company. The new paradigm should be that cybersecurity is an ongoing risk that needs to be managed by everyone in the organization. When employees (of your company or of other companies) make missteps on this front, use these experiences as textbook examples of what not to repeat—anywhere in the firm. Because breaches often result in legal action, the board should include lawyers in their discussions and make sure their efforts to change corporate culture are seasoned with a legal perspective. After assuring that the tone at the top is one of integrity and effective compliance, the board should turn to strategic considerations.

3. Engage Key Cybersecurity Personnel

The board should participate in selecting key personnel, such as the CISO. They should also ensure that adequate systems are in place to monitor those individuals' performances. In times past, companies often delegated responsibility for cybersecurity to the company's chief operations officer or chief technology officer. Consider the officer who currently has primary responsibility for cybersecurity at your company. Is that person C-suite level? Is cybersecurity only one of many

pressing demands they are currently juggling? If the answer to the first question is "no," and the second "yes," you may consider creating a new role in the form of a CISO.

The board should also consider the internal reporting structure for the CISO (or other officer with primary responsibility for cybersecurity) to ensure this individual has the independence and authority needed to succeed in this mission-critical role. The CISO may report to the company's chief information officer, chief operations officer, chief technology officer, or even the chief executive officer—but in any case the CISO should have access to senior management and the board as needed. Company management should also consider establishing an information security committee chaired by the company's CISO, and invite C-suite officers to attend the committee's meetings. Directors, for their part, should understand who fills the CISO role and engage directly with that individual as appropriate.

Does Board Membership Itself Require Cyber Expertise? On March 7, 2017, a bill was introduced in the U.S. Senate that would require the SEC to issue a rule requiring registered issuers to disclose whether any member of its board of directors "has expertise or experience in cybersecurity," and if no director has such expertise, "to describe what other cybersecurity steps taken by the [company]" were considered by those in charge of identifying and evaluating nominees for the board of directors, such as a company's nominating committee. The bill, titled *The Cybersecurity Disclosure Act of 2017* (S. 536), was introduced by Sen. Mark Warner (D-Va.), Sen. Jack Reed (D-R.I.) and Sen. Susan Collins (R-Me.). If passed into law, it would allow the SEC, in coordination with the U.S. Department of Commerce's National Institute of Standards and Technology, to define terms such as "expertise."

Source: S. 536, 115th Cong. § 2 (2017).

4. Evaluate Risk Management Strategies

From the board's perspective, the key to effective oversight is to hold senior management responsible for articulating and monitoring the company's strategy and risk tolerance related to cybersecurity. In most cases, board members should have their noses, but not their fingers, in the company's cybersecurity program.

One area where boards can, and should, play a crucial role is in developing the company's strategic plan related to cybersecurity. Following this initial effort, the board should oversee company management in implementing the strategic plan.

The board should also work with management to develop a cyber incident "response playbook" mapping out how the company would respond to various contingencies in the event of a breach or serious cyber incident impacting company systems. For example, in the wake of the Uber scandal, a company may want to consider how it would approach a ransom request, weighing the pros of potentially mitigating some of the damage associated with a breach against the cons of rewarding criminal behavior in this manner. Any such analysis should be flexible enough to take into account of-the-moment law enforcement recommendations and a legal analysis of the company's disclosure obligations. To avoid an Equifax problem, the public response plan should designate an internal and external team of professionals to investigate the causes and make appropriate disclosures.

There are various frameworks that company management can use to develop appropriate risk management strategies related to cybersecurity. For example, in October 2013, the U.S. Department of Commerce, National Institute of Standards and Technology ("NIST") issued for comment a set of voluntary standards and best practices for reducing cybersecurity risk. The final version was released in February 2014, titled *Framework for Improving Critical Infrastructure Cybersecurity*.[15]

The NIST framework includes five "functional areas," which directors may consider in developing an overarching cybersecurity plan for their companies. These functions include:

- **Identify**: Develop the organizational understanding to manage cybersecurity risk to

systems, assets, data, and capabilities.

- **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[16]

*Consider engaging an **independent third party to conduct an attack and penetration assessment** at your company. This is an effective way to test your company's current systems and monitor existing vulnerabilities—without experiencing an actual incident.*

Guidelines from the SEC also provide valuable assistance to directors, given the agency's considerable influence in markets. Cybersecurity has long been a priority of the SEC's National Exam Program, which is overseen by the Office of Compliance Inspections and Examinations ("OCIE"). In August 2017, OCIE posted a risk alert highlighting the results of its Cybersecurity 2 Initiative.[17] Although this initiative focuses only on broker dealers, investment advisers, and funds—entities over which the SEC has primary jurisdiction—the findings of OCIE provide a template that directors of companies in other industries and their management can use to evaluate their own efforts in cybersecurity.

As part of the Cybersecurity 2 Initiative, OCIE assessed how companies managed their cybersecurity programs in the following areas:

i) governance and risk assessment;

ii) access rights and controls;

iii) data loss prevention;

iv) vendor management;

v) training; and

vi) incident response.[18]

From a broad perspective, OCIE found that while firms were doing more to establish cybersecurity programs, they were not doing enough to maintain and update those programs in light of the constantly changing cyber threats and attacks.[19] For example, OCIE noted that nearly all firms had plans that address access incidents, such as denial of service incidents and unauthorized intrusions; however, less than two-thirds of advisers and funds surveyed appeared to adequately maintain such plans.[20]

5. Develop Systems to Monitor Cybersecurity Efforts

Directors should approach monitoring their companies' cybersecurity efforts like ongoing maintenance of machinery. Regular checks and adjustments will be needed, and it is not a one-time exercise. Technical means for conducting and preventing cyberattacks will constantly evolve. Moreover, old tactics and systems may be deemed irrelevant or insufficient as the company moves towards different operating systems or expands its business portfolio.

Accordingly, it is wise for directors to have a standing review of the company's cybersecurity program at quarterly meetings, at the very least. There should also be a procedure in place for briefing the board more frequently if new and serious issues emerge. The company's board minutes should accurately reflect when cybersecurity is discussed at such meetings so that the board's diligence is documented and demonstrated. Boards should also regularly receive a cybersecurity scorecard that highlights the company's progress mitigating cyber risk, including external metrics, gap remediation, emerging risks, trade-offs, and other issues. The scorecard does not need to include highly technical key performance indicators to be effective. Instead, examples of good metrics for the board include: customer satisfaction

(customer system downtime caused by information security incidents); reputation (number of information security incidents reported in the media); and financial (information security budget as a percent of IT budget).

As an important principle, boards should ensure that management and company employees collect, analyze, and share data regarding cybersecurity incidents—both large and small—to help inform the effectiveness of ongoing cybersecurity efforts. The company should also prioritize collecting, analyzing, and sharing internally any information the company may receive from government, private, or non-profit sources regarding cyber vulnerabilities and possible exposure.

Following Equifax, it is important for all companies to take a hard look at their information escalation protocols. Who is informed when a possible cyber incident is first picked up on the company's radar? Oftentimes, more junior employees will be best-placed to observe the first signs of a cyber breach. When it comes to installing critical software patches—such as in Equifax's case—ensure there are systems in place for appropriate supervision and peer review such that one person's human error does not result in a catastrophic (and preventable) breach.

Directors should also ensure the company has a system in place to encourage employees and management to learn from past mistakes. Acknowledging mistakes and learning from them leads to better decision making. Cybersecurity post mortems should be encouraged in briefings about the company's security model and vulnerabilities.

When a mistake occurs, this is also a good time to consult a lawyer. Certain mistakes come with legal responsibilities. For example, a company may have to disclose cybersecurity risks and adverse cyber events to its shareholders. Boards should make sure any post mortem, and any policy that grows out of it, include the necessary legal response.

6. Review Adequacy of Cyber Disclosures

More and more public companies are describing cybersecurity as a risk in their financial disclosures each year.[21] But what to disclose, and when to disclose it, remain thorny issues for many.

Equifax received significant criticism for waiting until September to disclose a breach it discovered in late July. But companies and regulators alike are realizing that there is a major tension between disclosing early on one hand, and waiting to learn all material facts in order to avoid making misleading or inaccurate disclosures, on the other. The SEC itself was subject to criticism for its perceived missteps in handling the EDGAR data breach. The SEC first reported that no personally identifying information was taken; it later had to revise these statements.[22] Also, the breach happened in 2016, but was reported to the public in September 2017.

It is critically important for companies to have appropriate escalation protocols in place. Do not lose precious time waiting for the report of a breach to slowly make its way up the chain to decision-makers. Instead, any time between a material breach and disclosure should be well spent investigating the facts and analyzing the issues.
The SEC has provided some guidance in this area. In 2011, the SEC's Division of Corporation Finance published guidance for public companies concerning disclosure obligations related to cybersecurity threats and adverse cyber events.[23] The guidance recommends that material information regarding cyber risk and adverse cyber events should be disclosed if necessary to make other disclosures not misleading. In particular, a company should review its cyber risks in light of the severity and frequency of prior cyber events. Companies should also consider the adequacy of their cyber defenses in light of the risks present in its particular industry. Companies should avoid generic risk factor disclosure and instead should consider their unique facts and circumstances. For example, a disclosure that a threat *may* occur may be insufficient if a company has *already* experienced that threat. A company should also consider including a discussion of cyber risks

and incidents in the management discussion and analysis (MD&A) portion of its regular filings if the costs or consequences associated with the cyber risk or incident are likely to have a material effect on the company's financial condition.

While the SEC has yet to dip its toe, other regulators have already been active in enforcing cyber-related disclosure obligations. For example, in August 2017, Uber settled charges brought by the Federal Trade Commission ("FTC") relating to a 2014 breach. The FTC alleged that the company made deceptive claims about its efforts to safeguard customer information and failed to undertake "reasonable, low-cost measures" to prevent unauthorized access to customers' personal data. Meanwhile, the FTC has confirmed that it is currently scrutinizing Uber's response to the 2016 breach, which the company only recently disclosed.[24]

Determining when and what to disclose can be even trickier when law enforcement is involved. Oftentimes when a cyberattack occurs, law enforcement will need time to investigate before the breach is made public. Experienced legal professionals should be consulted.

The FTC also previously brought a case against Oracle for disclosure issues, claiming that the company failed to inform consumers that newer software updates would not automatically remove older (and potentially exploitable) versions of Oracle's Java software. Last year the Consumer Financial Protection Bureau ("CFPB") ordered Dwolla, Inc., a company that operates an online payment system, to pay a penalty and improve its security practices after the company allegedly misrepresented to consumers that its networks were "safe" and "secure," and that its data security practices "exceed" or "surpass" industry security standards.

Additionally, while there is no national "data breach notification" law as of yet, the vast majority of states have enacted laws that require entities to notify affected individuals in the event of certain cybersecurity breaches involving sensitive consumer and personally identifiable information.[25]

Uber may well be the most egregious example of delayed disclosure and "what not to do." The company failed to notify regulators and individuals affected by the breach for nearly a year, possibly in violation of state notification laws. Moreover, Uber allegedly made non-disclosure of the breach a condition of its ransom payment to the cybercriminals, only further perpetuating the image of a cover-up. Several states' attorneys general have already initiated investigations into the breach.

The key takeaway is that it is absolutely essential for companies to review the adequacy and timeliness of their cyber disclosures on an ongoing basis. There is no "one-size-fits-all" answer. The advice of experienced disclosure counsel is crucial.

7. Understand Third-Party Vulnerabilities

If recent events have taught us anything, it is that a company's cybersecurity protocols are all for naught if the company fails to ensure that third-party service providers also implement adequate cyber risk management systems. All too often, the entry-point for the cyber criminals is a third party who has access to the company's systems or nonpublic data.

Home Depot, for example, is still feeling the reverberations from a 2014 cyber incident in which hackers took advantage of a security flaw in a third-party payment processor to steal email and payment information of more than 50 million Home Depot customers. Hackers similarly used a third-party vendor to access Target's customer database in 2013 and stole payment information from approximately 40 million customers.[26]

The recent example of Deloitte demonstrates why companies should pay attention to professional service firms in particular when it comes to third-party cyber risk. Professional service firms—such as law firms, auditors, and consultants—are particularly vulnerable because their databases and cloud computing applications often contain sensitive information from many different clients and business partners, all in one convenient location for cyber

criminals to exploit. The information professional service firms possess is an appealing target for cyber criminals because it is relatively easy to monetize through illegal trading. Such information may also be an attractive target for hacktivists.

The 2015 "Panama Papers" scandal was one of the first major incidents to shed light on law firm cyber vulnerabilities. The compromised firm, Mossack Fonseca, had helped hundreds of U.S. clients establish offshore businesses. The hack compromised the sensitive information of Mossack Fonseca's high-profile clients, dating as far back as the 1970s, and left many companies who had worked with the firm exposed.[27] We see a similar set of circumstances currently unfolding in the "Paradise Papers" scandal involving the release of the law firm Appleby's confidential client information.[28]

Because third parties often have access to highly sensitive company information, they should be subject to a rigorous third-party cyber risk assessment before companies engage them. Directors do not need to be aware of the nitty gritty details of each and every contract for services, but they should ensure that the company has a written vendor risk management policy in place for addressing third parties' access to company systems and sensitive nonpublic data. At bottom, the policy should ensure that management conducts proper due diligence and is aware of the risks of doing business with particular vendors. The company should also routinely reassess third-party risk and ensure that third-party service providers are in fact complying with their obligations.

Boards should also be aware of the risks associated with providing the government with sensitive nonpublic information. The breach of the SEC's EDGAR database raises serious questions about how much sensitive company data should be held by market regulators and whether the government, with its limited resources, can protect such data.[29] When possible, companies should consider providing information on encrypted physical media versus through secure file transfer.

8. Consider Methods to Transfer Cyber Risk

Cybersecurity is not a problem to be solved—it's an ongoing risk to be managed and, where prudent, transferred. As part of the risk management effort, the board should carefully review existing contracts with third-party vendors and insurance policies. These agreements must clearly state who is liable and what is covered in case of a breach.

Although cyber insurance is still in its nascent stages, with little actuarial data, it is one of the fastest growing types of coverage among U.S. companies—and with good reason.[30] The costs associated with a cyberattack can be game-changing for a company. A recent study conducted by Ponemon Institute shows that the average cost globally of a data breach is $3.62 million.[31] Victims of large-scale cyberattacks could expect to add several zeroes to that figure, as damage to reputation, costs of notification and protracted litigation quickly add up.

In its annual report filed with the SEC earlier this year, Target Corporation reported that it had incurred $292 million in cumulative expenses in connection with the 2013 data breach of its systems, which resulted in the massive theft of customers' credit card information. According to the company, this total amount was offset, in part, by $90 million in insurance payments.[32] Similarly, early this year, FedEx's Dutch subsidiary was hit by the "NotPetya" virus, which caused a temporary shutdown in the company's operations and led to a $300 million hit to its quarterly profit.[33] FedEx did not have insurance coverage for the attack, and FedEx's chief financial officer has since revealed that the incident triggered an internal re-evaluation as to whether the company should purchase cyber insurance moving forward.[34]

In addition to the obvious potential benefit of a monetary insurance recovery, seeking cyber insurance may result in ancillary advantages for companies. A company that is in the market for cyber insurance will be incentivized to use best practices, as premiums will be based, at least to some extent, on the company's effective use of protective measures. The application process alone may

require an in-depth evaluation of a company's existing cyber program. Through this process, the company may gain a better appreciation of its own cyber risks and opportunities. Boards should also be aware that insurance carriers often offer tools to help companies respond to cybersecurity incidents and mitigate post-breach losses, should the need arise.

Boards are commonly in a position to have the final say on whether a company should purchase cyber insurance. Making this decision as a board may require navigating some new terrain. You must determine what is, and should, be covered, and what is not, and need not, be covered. You also need to determine whether a particular premium is fair. One question boards should ask is whether existing insurance policies may cover certain events. Traditionally, most commercial general liability (CGL) policies did not contain cyber "exclusions"; however, these days, insurers may be more likely to include such provisions in their policies. Directors should ensure there are no critical gaps in coverage and consider what coverage makes the most sense based on their company's own risk profile (for example, coverage options may include coverage for costs of data breaches; extortion; forensic analyses; theft; litigation costs and expenses; and business interruption, to name a few). Boards should also confirm that their directors and officers (D&O) policies include coverage of cybersecurity-related events.

9. Stay on Top of Developments

There is nothing stagnant about cybersecurity. The hacks are ever evolving, and defensive practices that are industry standard one month may be obsolete the next. Legislators and regulators, in turn, strive to keep pace with new laws and regulations, spurred in no small part by public outcry following high-profile breaches. The State of New York, for example, has responded to the recent Equifax breach by proposing regulation to expand the state's first-of-its-kind cybersecurity rules, which currently require all financial institutions in New York to register with the state and implement programs to protect consumer data, among other things.[35] The new regulation would extend the requirements to credit reporting agencies.[36] New York's Attorney General also proposed new legislation to amend the state's existing data breach notification law.[37] Notably, the proposed legislation would expand the definition of "private information" and apply to any entity that holds the private information of New Yorkers, even if that entity does not conduct regular business in the state.[38]

The shifting legal landscape governing cybersecurity may itself be considered a cyber "vulnerability" for a company. Boards need to be cognizant of their companies' compliance obligations, but that is easier said than done. Companies today operate in a fragmented system of cybersecurity regulation. State, federal, and foreign regulators all come with their own rules and guidance. Certain states, such as California and New York, have taken a particularly aggressive tack in recent years to regulate and enforce cybersecurity standards within their jurisdictional limits. On the federal level, agencies such as the FTC and SEC are on the vanguard of cybersecurity enforcement within their own designated areas of focus and guidance, as well. The European Union, for its part, recently implemented its General Data Protection Regulation, which imposes reporting and other requirements on companies that collect credit card data or other personal information from EU citizens.[39]

Boards should ensure their companies continue to comply with the latest array of state and federal laws and regulations concerning cybersecurity. This is especially true for companies in certain industries that are frequently targeted by cyber criminals (*e.g.*, financial institutions), and those that handle sensitive personal information, such as personally identifiable information, financial information, or protected health information, as these companies are often subject to scrutiny by regulators and legislators. One obvious first step for the board may be to ask the company's general counsel and CISO to brief the board regularly on legislative developments and provide their recommendations. With many law firms growing their data privacy and cybersecurity practices, companies can also draw on the expertise of outside counsel to develop individualized programs to manage

cybersecurity risk, in view of the company's needs.

Boards can also be valuable weapons in combating "compliance fatigue," in which personnel performing the day-to-day compliance functions lose sight of the broader picture as they navigate disparate, daily demands and multiple moving targets. It is important to "check the boxes," but that is not enough. With their high-level perspective and status, boards can play a major role in encouraging management to think critically and innovatively when it comes to improving existing processes and cybersecurity measures. In the end, boards should try to ensure that the lion's share of the company's effort is spent on actual cybersecurity, and not on merely demonstrating compliance.

CONCLUSION

To implement an effective cybersecurity program, a director should understand the full range of cyber risks facing his or her company and encourage management to develop appropriate strategies tailored to the company's specific needs and goals. Any effective cyber program includes careful planning, smart delegation, and a system for monitoring compliance—all of which directors should own. It's no longer a question of whether a company will be attacked but more a question of when—and what the company is going to do about it. Smart network surveillance, early warning indicators, multiple layers of defense, and learning from past events are all critical components of true cyber resilience. When things go wrong, whether in a major or minor way, the ability to quickly identify and respond to a problem will determine the company's ultimate recovery. Cybersecurity cannot be guaranteed, but a timely and appropriate reaction can.

[1] *See* Prepared Testimony of Richard F. Smith before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017).

[2] *See e.g.*, Bloomberg News, *Equifax Says 2.5 Million More Americans May Be Affected by Hack* (Oct. 2, 2017), https://www.bloomberg.com/news/articles/2017-10-02/urgent-equifax-2-5-million-more-americans-may-be-affected-by-hack.

[3] *See* Statement on Cybersecurity by Chairman Jay Clayton (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

[4] *See e.g.*, Newsweek, *HBO Cyberattack Is "Seven Times Worse" than the Sony Hack* (Aug. 2, 2017), http://www.newsweek.com/hbo-cyberattack-sony-hack-leak-game-thrones-645450.

[5] *See* The Guardian, *Deloitte Hit By Cyber-attack Revealing Clients' Secret Emails* (Sept. 25, 2017), https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.

[6] *Id*.

[7] *See* N.Y. Times, *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data* (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html?mtrref=www.google.com&gwh=34D070015500C54F741A1922ED2C7834&gwt=pay.

[8] *See* Press Release, *Equifax Board Releases Findings of Special Committee Regarding Stock Sale by Executives* (Nov. 3, 2017), https://investor.equifax.com/news-and-events/news/2017/11-03-2017-124511096.

[9] Time, *Equifax Says You Won't Surrender Your Right to Sue by Asking for Help After Massive Hack* (Sept. 11, 2017), http://time.com/4936081/equifax-data-breach-hack/.

[10] *See* Verizon, 2013 Data Breach Investigations Report 13 (2013), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[11] *Id.*

[12] Verizon, 2017 Data Breach Investigations Report 3, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (2017).

[13] *Id.*

[14] *See* N.Y. Times, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core* (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

[15] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[16] *Id.* at 8-9.

[17] OCIE Risk Alert, Observations from Cybersecurity Examinations (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[18] *Id.* at 1.

[19] *Id.* at 3-4.

[20] *Id.* at 3.

[21] *See* Bloomberg BNA, *Corporate Cyber Risk Disclosures Jump Dramatically in 2017* (July 26, 2017), https://www.bna.com/corporate-cyber-risk-n73014462313/.

[22] *Compare* Testimony on "Oversight of the U.S. Securities and Exchange Commission" by Jay Clayton before the Committee on Banking, Housing and Urban Development of the United States Senate (Sept. 26, 2017), https://www.banking.senate.gov/public/_cache/files/929816e6-9372-404f-ba97-c9d9ed453501/ADC20EE6B81BD706BEE66812F71FADDB.clayton-testimony-9-26-17.pdf, at 3 (testifying the SEC "believe[s] the intrusion did not result in unauthorized access to personally identifiable information"), *with* Press Release, Chairman Clayton Provides Update on Review of 2016 Cyber Intrusion Involving EDGAR System (Oct. 2, 2017), https://www.sec.gov/news/press-release/2017-186 (observing the breach resulted in the unauthorized disclosure of names, dates of birth, and social security numbers of two individuals).

[23] *See* SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[24] Reuters, *FTC says it is evaluating 'serious issues' raised in Uber's handling of a data breach* (Nov. 22, 2017), https://www.reuters.com/article/us-uber-cyberattack-ftc/ftc-says-it-is-evaluating-serious-issues-raised-in-ubers-handling-of-a-data-breach-idUSKBN1DM2EC.

[25] *See e.g.*, National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 21, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[26] *See e.g.*, Wall Street Journal, *Home Depot's 56 Million Card Breach Bigger than Target's* (Sept. 18, 2014), https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[27] N.Y. Times, *Panama Papers Show How Rich United States Client Hid Millions Abroad* (June 5, 2016), https://www.nytimes.com/2016/06/06/us/panama-papers.html?mtrref=www.google.com.

[28] N.Y. Times, *Paradise Papers Shine Light on Where the Elite Keep Their Money* (Nov. 5, 2017), https://www.nytimes.com/2017/11/05/world/paradise-papers.html.

[29] Wall Street Journal, *Regulators Fret About Cyber Risk After SEC Hack* (Oct. 3, 2017), https://www.wsj.com/articles/regulators-fret-about-cyber-risk-after-sec-hack-1507049048.

[30] Wall Street Journal, *Insurance Grows for Cyberattacks* (Sept. 17, 2017), https://www.wsj.com/articles/insurance-grows-for-cyberattacks-1505700360.

[31] *See* IBM Release, 2017 Ponemon Cost of Data Breach Study, https://www.ibm.com/security/data-breach.

[32] Target Corp., 2016 Annual Report 44 (2017), https://corporate.target.com/_media/TargetCorp/annualreports/2016/pdfs/Target-2016-Annual-Report.pdf?ext=.pdf.

[33] Bloomberg Technology, *FedEx Cuts Profit Forecast on $300 Million Hit from Cyberattack* (Sept. 19, 2017), https://www.bloomberg.com/news/articles/2017-09-19/fedex-cuts-profit-outlook-on-300-million-blow-from-cyberattack.

[34] *Id*.

[35] N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

[36] N.Y. COMP. CODES R. & REGS. tit. 23, § 201 (proposed Sept. 18, 2017).

[37] Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), Senate Bill S6933, 2017-2018 Reg. Sessions (N.Y. Nov. 1, 2017).

[38] *Id.* § 3.

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Roel C. Campos
Hughes Hubbard & Reed LLP
roel.campos@hugheshubbard.com

David X Martin
cybXsecure
dxm@cybxsecure.com