

DOCKET MEDIA LLC
PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM

CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

TEN CYBERSECURITY CONCERNS FOR EVERY BOARD OF DIRECTORS

BY JOHN REED STARK AND DAVID R. FONTAINE[1]

Every board now knows its company will fall victim to a cyber-attack, and even worse, that the board will need to clean up the mess and superintend the fallout.

Yet cyber-attacks can be extraordinarily complicated and, once identified, demand a host of costly responses. These include digital forensic preservation and investigation, notification of a broad range of third parties and other constituencies,[2] fulfillment of state and federal compliance obligations, potential litigation, engagement with law enforcement, the provision of credit monitoring, crisis management, a communications plan – and the list goes on.

And besides the more predictable workflow, a company is exposed to other even more intangible costs as well, including temporary or even permanent reputational and brand damage;[3] loss of productivity; extended management drag; and a negative impact on employee morale and overall business performance.

So what is the role of a board of directors amid all of this complex and bet-the-company workflow? Corporate directors clearly have a fiduciary duty to understand and oversee cybersecurity, but there is no need for board members (many of whom have limited IT experience) to panic.

---

[1] John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. See www.johnreedstark.com. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11of which as Chief of its Office of Internet Enforcement. He has also served for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he has taught several courses on the juxtaposition of law, technology and crime. He also served for five years as managing director of a global data breach response firm, including three heading its Washington, D.C. office. David Fontaine is Executive Vice President, Chief Legal & Administrative Officer and Corporate Secretary of Altegrity, a privately held company that among other entities, owns Kroll's data breach response services.

[2] Constituencies that may require notice, briefings, and other information include customers, partners, employees, affiliates, insurance carriers and a range of other interested parties.

[3] Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks," available at http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf.

Below we compile a list of ten cybersecurity considerations that provide a solid bedrock of inquiry for corporate directors who want to take their cybersecurity oversight and supervision responsibilities seriously.[4] This "cybersecurity top ten list" provides the requisite strategical framework for boards of directors to engage in an intelligent, thoughtful and appropriate supervision of a company's cybersecurity risks.

By using these ten concerns as a guide, boards of directors can not only become more preemptive in evaluating cybersecurity risk exposure but they can also successfully elevate cybersecurity from an ancillary IT concern to a core enterprise-wide risk management item, at the top of a board's oversight agenda.

1. Cybersecurity Policies and Procedures.

The best place to begin a review of a company's cybersecurity is with a review of the company's cybersecurity policies and procedures. It is a good starting point to facilitate meaningful board oversight and supervision of a company's cybersecurity risks and vulnerabilities. Some areas to review are:

- Overall approach to information technology risk and cybersecurity. Cybersecurity is a business imperative, yet too often cybersecurity is too far down on a C-Suite priority list—or because it is so complex, simply delegated to lower level technical personnel.

  Is there a commitment from the top down, both culturally and financially, to rigorous cybersecurity? Who in leadership is driving the agenda? Is it a C-level accountability and part of the day-to-day business focus? Do current reporting lines and assigned areas of responsibility make sense? Given the responsibilities and accountability needed to execute the incident response plan, are the right employees, possessing the appropriate skillsets, adequately empowered? Is the individual charged with overseeing cyber-defense the same person who reports up the chain about breaches and who would oversee any response–if so, does that dual-role indicate a conflict of interest?

- Incident response plan. In cybersecurity, most companies allocate significant resources to fortifying their networks and to denying access to cyber-attackers. However, it is now a cliché, well founded in reality, that data breaches are inevitable.[5] Along those lines,

[4] Shareholders are not the only constituencies that expect boards of directors to supervise cybersecurity issues; the federal government takes a similar posture. For instance, Andrew Ozment, assistant secretary, Office of Cybersecurity and Communications at DHS, recently said DHS endorsed the principles spelled out in the "NACD Directors' Handbook on Cyber-Risk Oversight" published by the National Association of Corporate Directors, which has over 14,000 members who are directors for public, private and non-profit organizations. The DHS will include the NACD's handbook on the U.S. CERT website as a source of information for businesses. In any organization, the board of directors is there to oversee its general direction, including how well upper management is performing. "Homeland Security Wants Corporate Board of Directors More Involved in Cyber-security," by Ellen Messmer, NetworkWorld.com (July 29, 2014), available at http://www.networkworld.com/article/2458975/security0/homeland-security-wants-corporate-board-of-directors-more-involved-in-cyber-security.html

[5] As cybersecurity experts have noted, "There's a saying in the cybersecurity industry that there are two types

just like a fire evacuation plan for a building, a company should have a plan in place to respond to data breaches; an art form less about security science and more akin to "incident response." Due to the absence of such a plan, many organizations unfortunately allow what could have been a relatively contained incident to become a major corporate catastrophe because they neither thought through all of the elements necessary for an effective response nor put the necessary mechanisms in place to ensure these elements were addressed in their plans.

Is there a current incident response plan? If so, when was the plan last updated? Who prepared the plan? Who approved the plan? What is the general approach and what are the general principles of the plan? Has the company ever run any mock or tabletop exercises to test the plan's efficacy and efficiency? Is there an accurate and current network topology diagram that is adequately documented, and if so, is it periodically re-assessed and revised as internal systems and external factors change?

- Business continuity plans in case of a cyber-attack. The critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks.

  Has the company properly evaluated the effectiveness of its business continuity plan in the context of a cyber-attack? Does the business continuity plan need to be reconsidered and refreshed with these additional considerations in mind?

- Personnel continuity. Competition for talent in the information security space is intense, while the pressure on IT security senior executives is infinite and exhausting. Moreover, despite their rapidly rising salaries, turnover remains constant and there is a serious shortage of experienced and capable IT senior executives, especially chief information security officers (CISOs).[6]

  What is the company doing to recruit and retain IT security talent?

  Relatedly, when a company loses key senior IT security personnel, it is not only a red flag but also an opportunity for a board to examine succession plans and to obtain an unbiased, albeit possibly disgruntled, view of any cybersecurity flaws. The art and the benefit of the exit interview is lost on so many companies today–too often because departing employees are dismissed as resentful and unreliable. In the case of a resigning IT executive, a proper exit interview may reveal critical cybersecurity weaknesses.

  Are there threats or known risks that are contributing to the decision to leave? Is the departure a potential "red flag"? Who is best placed to assume (even on an interim

---

of businesses today: Those that have been breached and know it and those that have been breached and just don't know it." "What's Next for Cyber Insurance?" By Andrea Wells, Insurance Journal (April 21, 2014) available at http://www.insurancejournal.com/magazines/features/2014/04/21/326382.htm.

[6] "More CISOs Needed to Battle Cybersecurity Threats in 2015," by Clint Boulton, Wall Street Journal (December 18, 2014) available at http://blogs.wsj.com/cio/2014/12/18/more-cisos-needed-to-battle-cybersecurity-threats-in-2015/?KEYWORDS=ciso.

basis) the day-to-day IT security responsibilities? Is there a succession plan? What steps are in place to reduce turnover and retain talent?

- Keeping up with cybersecurity threats. Not all companies face the same cybersecurity risks. There is no "one size fits all" approach. Companies that house and maintain large amounts of personal information and data need to tailor any defense, mitigation and response plans accordingly. By taking steps to insure that information flow about data breaches within the industry and the latest intelligence about rising threats are considered by management on an ongoing basis, companies can stay current on the latest threats and prepare accordingly – preparedness is the key.

  What steps does the company undertake in the realm of security science to stay current about the latest cybersecurity intrusion modus operandi, cybersecurity-related software patches,[7] data breach trends, etc.? Does the company have any PCI compliance[8] issues and if so, how are PCI-related concerns addressed?

---

[7] Of course, the need to update software when a patch is issued to address exposed software security flaws seems as basic as the need to take out the trash at the end of the day – and may not at first glance, seem worthy of specific board oversight. Yet, many security breaches still occur because software was not updated in a timely manner. In other words, software versions with known security vulnerabilities continue to be used in spite of their risk. Basic procedures to update software with patches offering the latest protection are a necessity and basic expectation of all company stakeholders – so it is worth, at least, probing management about its software patching practices.

[8] When a cyber-attack targets electronically transmitted, collected or stored payment card information, so-called Payment Card Industry Data Security Standards ("PCI-DSS") compliance is often one of the first aspects investigated. The Payment Card Industry Security Standards Council is the international organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. in 2006, which develops and manages certain credit card industry standards, including the PCI-DSS. PCI-DSS is a set of requirements created to help protect the security of electronic payment card transactions that include PII of cardholders, and operate as an industry standard for security for organizations utilizing credit card information. PCI-DSS applies to all organizations that hold, process or pass credit card holder information and imposes requirements upon those entities for security management, policies, procedures, network architecture, software design and other critical measures that help to protect customer credit and debit card account data. If a cyber-attack against a company involves credit cards or other similar modes of payment and triggers PCI-DSS compliance, the workflow involving the PCI-DSS can be extremely costly, cumbersome and disruptive. For instance, merchants are responsible for all costs associated with any system modifications required to achieve PCI-DSS compliance and the card brands may levy significant fines and penalties on merchants that are not in compliance with PCI-DSS. Such penalties and fines, imposed separately by each card association, can include:

- Hefty fines (in multiples of $100,000) for prohibited data retention;
- Significant additional monthly fines (can be $100,000 or more per month depending on the nature of the data stored) assessed until confirmation is provided indicating that prohibited data is no longer stored;
- Separate fines (in multiples of $10,000) for PCI-DSS non-compliance;
- Additional monthly fines (likely $25,000 per month) assessed until confirmation from a qualified security assessor that the merchant is PCI-DSS compliant;
- Payment of monitoring (can be as high as $25) and reissuing (up to $5) assessments for each card identified by the card association as potentially compromised; and

- IT security budgeting. Most budgeting at companies is conducted annually and planned carefully and thoughtfully before execution – yet cybersecurity budgetary priorities can shift very quickly. Thus, a one-year budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats. Moreover, the average cost of a data breach continues to increase. According to one study:

  > Throughout the world, companies are finding that data breaches have become as common as a cold but far more expensive to treat. With the exception of Germany, companies had to spend more on their investigations, notification and response when their sensitive and confidential information was lost or stolen. . . . the average cost to a company was $3.5 million in US dollars and 15 percent more than what it cost [in 2013].[9]

  How does cybersecurity budgeting work? How are emergency items identified and funded? Does the budget appropriately provide for contingencies in the event of a cyber-attack or cybersecurity need?

- Training programs. The most significant cybersecurity vulnerability at any company will always be its employees. If employees do not adhere to cybersecurity rules and requirements, an attacker's exploit becomes all the more effective and capable of doing damage.

  How often and how effective are the firms' cyber-safety training programs? Who participates in the training and how does the company handle policy violations, especially violations by senior executives, who studies have shown are typically the least compliant with cybersecurity policies?

- Processes for sharing and obtaining information about cybersecurity threats. Keeping up with the latest developments in cybersecurity and the latest tools and techniques being utilized by cyber-attackers is a career within itself – and requires building relationships with law enforcement, including the Federal Bureau of Investigation ("FBI"), U.S. Air Force, Department of Homeland Security, the U.S. Secret Service and others.

  How will the company deal with the competing constituencies? On one hand, there are the FBI, Secret Service, and other law enforcement agencies who want to help find the intruders, and on the other hand, there are the myriad attorneys general and other state regulatory agencies who will be issuing requests and demanding answers about the safety of the personally identifiable information of their respective citizenries? Has the company considered the rules, practices and procedures that govern the sharing of intelligence with government agencies?

- Reimbursement for any and all fraudulent activity the card association identifies as being tied to a security data breach.

[9] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," available at http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

2. **Data Mapping.**

Every cyber-attack response begins with the simple notion of preservation, *i.e.* collecting and preserving, in a forensically sound and evidentiary unassailable manner, any "electronically stored evidence" ("ESI"), devices, logs, etc. that could become relevant to the cyber-attack.

Preservation is a critical workstream during a cyber-attack because incident responders will be scrutinizing every byte of data, including any fragments, artifacts or remnants left by the attacker in all sectors of any relevant device, including "deleted recoverable files,"[10] "unallocated and slack space"[11] or the boot sector.[12] These artifacts can include: Internet addresses; computer names; malicious file names; system registry data; user account names; and network protocols.

Gathering the data and devices relating to a cyber-attack is the first and one of the most critical steps of an incident response. The most effective investigative methodology of a cyber-attack is one based on targeted incident response practices and does not solely rely on "signature detection" technologies, such as antivirus software. Rather, careful investigators employ an iterative process of digital forensics, malware reverse engineering, monitoring and scanning. As

---

[10] A "deleted recoverable file" is a file that is typically easily recovered with forensic software, such as a Microsoft Word document, PowerPoint presentation, PDF file, or other data where, perhaps unbeknownst to the user, a file record for that data still exists within the file system.

[11] The unallocated space and file slack of desktop or laptop personal computers typically provide important leads for digital forensic examiners. Here's why: Files saved to the hard drive of a computer are typically described as residing in ''allocated space,'' i.e., space on the hard drive allocated by the file system. When a user deletes these so-called ''active files,'' the files usually do not disappear from the hard drive. Rather, the operating system no longer allocates or saves that hard drive space for the file and simply designates that area of the hard drive as unallocated (i.e., unused) space. The data actually stay still—the file system just marks that portion of the drive as usable for other files. Within unallocated space, a digital forensic examiner can usually extract file artifacts, such as deleted files, temporary files (created when a user opens a file), file fragments, deleted internet history and other, albeit disorganized, but readable, bits of data. Indeed, evidence gleaned from unallocated space has become so important in the context of litigation that using a ''wiping program'' to render unrecoverable the artifacts from the unallocated space can even draw a discovery sanction from a judge. See also *TR Investors LLC v. Genger*, No. 3994-VCS (Del. Ch. Dec. 9, 2009) (finding defendant Arie Genger in contempt of court for ''wiping'' the ''unallocated space'' of the hard drive of his work computer and file server in the face of an order that prohibited him from ''tampering with, destroying or in any way disposing of any Company-related documents, books or records''). This approach similarly applies to so-called ''slack space'' (that portion of a cluster unused by an active file), which can also contain similar information.

[12] A boot sector is a small piece of hard disk or external storage device space and the first file a Basic Input/Output System ("BIOS") loads when a computer is turned on. There are two main types of sectors: the Master Boot Record ("MBR") and Volume Boot Record ("VBR"). The Boot sector can contain computer viruses, which are most commonly spread using physical media. An infected floppy disk or USB drive connected to a computer will transfer when the drive's VBR is read, then modify or replace the existing boot code. The next time a user tries to boot their desktop, the virus will be loaded and run immediately as part of the master boot record. It's also possible for email attachments to contain boot virus code. If opened, these attachments infect the host computer and may contain instructions to send out further batches of email to a user's contact list. Improvements in BIOS architecture have reduced the spread of boot viruses. Kaspersky Lab, "What is a Boot Sector Virus," available at http://usa.kaspersky.com/internet-security-center/definitions/boot-sector-virus.

analysis of known or suspected compromised systems identifies new so-called *Indicators of Compromise* ("IOCs), investigators will examine network traffic and logs, in addition to scanning hosts for these IOCs. When this effort discovers additional systems, those systems are forensically imaged and analyzed, and the process repeats. Armed with the information gathered during this phase of "lather, rinse, repeat," a victim company can begin efforts to remediate the malware, rebuild compromised systems, reset compromised account credentials, block IP addresses and properly initiate network and host monitoring in an effort to detect additional attempts by the attacker to regain access.

Preservation is also critical because investigators will likely need to scour all so-called *electronically stored evidence* or "ESI" in search of so-called *personally identifiable information* or "PII." The search for PII is necessary to determine whether the attacker exfiltrated (removed from a corporate IT environment) any data containing personal information relating to any individuals, who may require notice of the cyber-attack, credit monitoring services and other remedial action.[13] Finally, just about every cyber-attack response also involves the forensic imaging and reviewing of emails and other relevant communications from laptop computers, desktop computers, network servers, backup tapes, mobile devices, iPads and other systems.[14]

Yet, preserving ESI after a cyber-attack can quickly become a challenging, costly and resource intensive task. Most companies have ESI in so many locations (both physical and virtual) that, after a cyber-attack, it becomes an onerous struggle to locate and preserve relevant ESI and to piece together information about sometimes complex and disparate systems – all under the intense pressure of an active digital forensic investigation (with serious consequences for error or omission). Relatedly, it can sometimes take days after learning of a cyber-attack before a company realizes that they maintain an electronic purging process that deletes data (such as relevant logging information) on a regular schedule. Without having proactively made the effort to map information sources, assets and their key characteristics, these purging schedules can become unintended and latent causes of spoliation.

---

[13] Protecting PII relating to individuals from identity theft has become a significant focus of U.S. state and federal agencies, and of new state and federal laws and regulations. In the U.S., laws and regulations vary from state to state, and between state and federal law, as to exactly what information comprises PII. Generally, the definition requires both a name and some additional item of information that could be used to steal a person's identity or access his or her financial accounts (or, in some cases, healthcare information) without authorization. N.B. that for purposes of this article, we refer generally to protected information about an individual as PII, even though some state or federal statutes may use a different nomenclature or categorizations. See infra "Workstream: Individual Notifications/Monitoring Services."

[14] The cyber-attack investigation may have sprouted from a customer who complained that his or her data was used for a fraud; from a report that a computer system was found to be communicating with an unscrupulous Internet address; from the FBI, U.S. Air Force Office of Special Investigations ("OSI"); US Secret Service or other law enforcement agency notifying a company of a possible cyber-attack into its systems; or a slew of other sources. Under any circumstance, investigators will first analyze whatever initial information is presented and use the preliminary evidence to help identify the likely locations of additional evidence. An investigator will consider all computer devices as likely locations to target for investigation. These devices will typically include: company laptops and workstations; network storage servers; firewalls; intrusion detection systems; webservers; customer databases; and e-mail servers.

Boards should probe a company's data practices because where information relevant to identifying and describing potentially accessed/target/exfiltrated systems has never been data-mapped, establishing a strong and effective incident response plan for addressing cybersecurity risks can become challenging. Without any sort of responsible system overview or asset classification exercise, companies not only make mistakes in their cyber incident response plans, but companies can also make mistakes when applying available resources for security.

In addition, boards should press to identify and understand the most critical pieces of company information. What are the company's most valuable intellectual property assets and consumer/customer based informational assets, and how are they currently being protected? Where are these assets stored or located? Internally, at a third-party data center (in the U.S. or overseas), or in a cloud-based environment? Asking these and other similar questions will help a board better understand the company's posture with respect to securing its virtual assets and inform what additional steps, if any, management can take to improve such practices.

3. Cyber Insurance.

Just like with other hazards of doing business, today's public and private companies have begun taking into account cybersecurity concerns when considering overall enterprise risk management and insurance risk transfer mechanisms. Clearly, cyber insurance will eventually become yet another basic element of a company's insurance coverage, just like property insurance for companies and health insurance for individuals.[15]

Interestingly, companies who maintain cyber insurance might also have the best cybersecurity policies and practices – probably because before obtaining cyber insurance coverage, a company is typically subjected to a fairly rigorous review by the proposed insurance company. Just like the physical exam typically required by insurance companies before issuing life insurance, which can prompt better personal wellness practices, a *cyber insurance exam* might trigger or prompt better *corporate cybersecurity wellness*. According to one recent study,

> In most countries, the primary root cause of the data breach is a malicious insider or criminal attack. It is also the most costly. In this year's study, we asked companies represented in this research what worries them most about security incidents, what investments they are making in security and the existence of a

[15] See e.g. "Within six years, we're going to be well on our way to everyone having cyber insurance as just a basic set of insurance, just like property insurance," said Ari Schwartz, director for cybersecurity on the White House National Security Council, during a Sept. 8, 2014 panel discussion at the Nextgov Prime conference. "Cyber Coverage Will be a Basic Insurance Policy by 2020," by Aliya Sternstein, September 8, 2014 available at http://www.nextgov.com/cybersecurity/2014/09/wh-official-cyber-coverage-will-be-basic-insurance-policy-2020/93503/ ; http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks ("Cyber Insurance—Mitigating Loss from Cyber Attacks," by Rene L. Siemens, David L. Beck, Pillsbury's Perspectives on Insurance Recovery Newsletter (Summer 2012) ("The market is rapidly growing for insurance that is specifically meant to cover losses arising out of cyber attacks and other privacy and data security breaches. These insurance policies are marketed under names like 'cyber-liability insurance,' 'privacy breach insurance' and 'network security insurance.' Many companies and other institutions that handle legally protected information now view this kind of insurance as an essential part of their coverage programs.").

> security strategy. An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. While it has been suggested that having insurance encourages companies to slack off on security, our research suggests the opposite. Those companies with good security practices are more likely to purchase insurance.[16]

A number of different types of insurance policies have the potential to be implicated in the event of a cyber-attack – or at least to be subject to a request for defense and/or indemnity. Factors depend on the nature of the breach, the relationship of the parties, the type of the information in issue (such as personal information, intellectual property, trade secrets, and emails), the precise form of the operative policy and, if related to third-party liability claims, the allegations asserted and the type of damages sought.

Yet while the market for cyber insurance continues to evolve and grow dramatically,[17] there still has not materialized any form of standardized cyber insurance policy language, and whether standard property casualty provisions even cover losses relating to cyber incidents often remains an open question.[18] Stand-alone cyber insurance policies offer broader coverage and should be

---

[16] "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," available at http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

[17] "Demand for Cyber Insurance Skyrockets," by Corey Bennett (January 15, 2015) at http://thehill.com/policy/cybersecurity/229568-skyrocketing-demand-seen-for-cybersecurity-insurance. See also "Why Cyber-insurance Will be the Next Big Thing" by Mary Thompson (July 1, 2014) available at http://www.cnbc.com/id/101804150#; "Should Your Company Get Cybersecurity Insurance?" by Will Yakowicz, (December 17, 2014) available at http://www.inc.com/will-yakowicz/does-your-company-need-cybersecurity-incurance.html.

[18] Relying on a general property insurance policy for cyber-attack coverage is risky and directors should not rely on a Commercial General Liability policy to cover a data breach, as it most likely will not. For example, in the data breach involving Sony, the breach reportedly exposed the personal information of tens of millions of users, and Zurich American stated in court papers that as a result, Sony was the defendant in over 50 class action lawsuits. Because the Sony policy required the policyholder (Sony) to perpetrate or commit the act of publication of the personal information, the judge stated, "Paragraph E (oral or written publication in any manner of the material that violates a person's right to privacy) requires some kind of act or conduct by the policyholder in order for coverage to present." This decision highlights the hazards of relying on traditional CGL coverage policies for potential data breach coverage. See, *Zurich American Insurance Co. v. Sony Corp. of America, et al* (Supreme Court , State of New York 651982/2011) But see *Hartford Casualty Insurance Company v. Corcino & Associates et al* , where the District Court of the Central District of California ruled that there is coverage under a GCL policy for a data breach involving hospital records of some 2,00 patients. See, also e.g., *Ward General Services, Inc. v. Employers Fire Ins. Co*., 114 Cal.App.4th 548, 556-57 (Cal.App. 4 Dist. 2003); *Southeast Mental Healthcare Center, Inc. v. Pacific Insurance Company*, LTD, 439 F.Supp.2d 831, 838-839 (W.D. Tenn. 2006); America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 93-98 (4th Cir.2003); *State Auto Property & Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1113 (W.D.Okla. 2001). Courts reaching a different conclusion have done so where the data is permanently lost to its owner, not merely improperly accessed. See *Computer Corner, Inc. v. Fireman's Fund Ins. Co*., 46 P.3d 1264 (N.M. 2002) (holding that loss of the pre-existing electronic data was tangible property damage covered by CGL policy where computer store repairing customer's computer permanently lost all the data); *American Guar. & Liab. Ins. Co. v. Ingram Micro*, Inc., 2000 WL 726789, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (holding that computer data permanently lost during a power outage constituted "direct physical loss or damage from any cause" covered by first-party insurance policy); *NMS Services Inc. v. Hartford*, 62 Fed.Appx. 511 (4th Cir. 2003)

explored by every board, along with an evaluation of the sufficiency of the company's Directors and Officers liability insurance program.

But the question of how to design a stand-alone cyber insurance policy is a difficult one. The actuarial challenges of predicting/gauging both the probability and the impact of a cyber-attack can in turn, make it difficult to match a cyber insurance policy with the unique risk profiles of today's global and technologically sophisticated companies; these are difficulties faced not only by insurance analysts but also by even the most experienced executive teams. Cyber-attack damages are so multifaceted and unique – much more so than fire, flood, health and other more traditional insurance scenarios and models – that there is no normal distribution of cyber-attack outcomes on which to base the probabilities of future effects. As a result, there are now a dizzying array of cyber insurance products in the marketplace, each with its own insurer-drafted terms and conditions, which can vary dramatically from insurer to insurer – some effective and comprehensive and others replete with loopholes, exclusions and other troubling features.[19]

Even the U.S. Department of Homeland Security has officially acknowledged that the cyber insurance market remains confusing for most companies and can be overlooked for all of the wrong reasons:

> Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.[20]

To make matters worse, as opposed to disasters like fires, floods, tornadoes, etc., today's companies who experience a cyber-attack should not expect any assistance or even compassion from the government. In fact, companies should expect quite the opposite for several reasons: 1) the U.S. government is overwhelmed with protecting the nation's own infrastructure and does not have a SWAT team or a rescue team standing-by to assist U.S. companies after a cyber-attack;[21] 2) given the forty-seven or so separate state privacy statutory regimes[22] and a growing

---

(characterizing the erasure of vital computer files and databases as direct physical loss or damage to property for purposes of business income coverage).

[19] "Many 'Loopholes' in Cyber Insurance Policies, L'Oreal CISO Says," By Clint Boulton, Wall Street Journal: CIO Journal (October 3, 2014) available at http://blogs.wsj.com/cio/2014/10/03/many-loopholes-in-cyber-insurance-policies-loreal-ciso-says/; "Cyber Insurance: Worth it, but Beware of the Exclusions," by Taylor Armerding (October 20, 2014) available at http://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html.

[20] http://www.dhs.gov/publication/cybersecurity-insurance.

[21] Testimony of Robert Anderson, Jr., Executive Assistant Director, Criminal, Cyber, Response, and Services Branch Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C., September 10, 2014 at http://www.fbi.gov/news/testimony/cyber-

range of federal agency jurisdiction (each wielding their own unique set of rules, regulations, statutes and enforcement tools), instead of a helping hand, cyber-attack victims should expect subpoenas, enforcement actions and an onslaught of litigation; and 3) the public's (and Congress') view of cyber-attack victims has rapidly become not a view of understanding or empathy but rather a view of suspicion, skepticism and even vilification.[23]

Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown and a range of other risk-related analytics. Boards should, however, make sure management also considers a different approach towards that calculus.

Board members should ask if their senior executives have considered reviewing actual cyber-attacks, analyzing and scrutinizing the typical cyber-incident response workflow and so-called "workstreams" that follow most cyber-attacks. By analyzing and revisiting the realities and economics of these workstreams, a company can then collaborate with their insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workstream costs will trigger coverage; which workstream costs will be outside of coverage; and which workstream costs might be uninsurable.[24]

---

security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

[22] Specifically, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving PII. Security breach notification laws also typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities); definitions of PII (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information). See e.g. https://cybersecuritylawwatch.files.wordpress.com/2014/10/cybersecuity-in-the-golden-state.pdf.

[23] "Fury and Frustration over Target Data Breach," by Anne D'Innocenzio and Bree Fowler, USA Today, available at http://www.usatoday.com/story/money/business/2013/12/20/fury-and-frustration-over-target-data-breach/4145503/; "Companies Slow To Alert About Data Breaches," by Craig Timberg, Andrea Peterson and Ellen Nakashima, Washington Post available at http://www.vnews.com/news/business/13332855-95/companies-slow-to-alert-about-data-breaches; "Rep. Cummings Demands Answers from Background Investigation Contractor on Data Breach," by Jason Miller (January 7, 2015) available at http://www.federalnewsradio.com/520/3775347/Rep-Cummings-demands-answers-from-background-investigation-contractor-on-data-breach; "US Lawmaker Asks Sony for Details on Data Breach, " by Grant Gross (December 23rd, 2014) available at http://www.computerworld.com/article/2863054/us-lawmaker-asks-sony-for-details-on-data-breach.html.

[24] For a detailed discussion of typical workstreams during the aftermath of a cyber-attack see Cyber Insurance,: a Pragmatic Approach to a Growing Necessity by John Reed Stark and David Fontaine available at http://www.cybersecuritydocket.com/2015/04/09/cyber-insurance-a-pragmatic-approach-to-a-growing-necessity/. Akin to when someone with a genetic history of heart disease consults with a cardiologist to help identify the most suitable health insurance or when a new homeowner consults with a local firefighter to help identify the most suitable property insurance, this methodology assesses risk practically. Specifically, this article presents a laundry list of typical workstreams from the perspective of a cyber-attack first responder, who has handled data breaches from both the government side and from the private side for over 20 years, together with a seasoned general counsel, who has both experienced a corporate cyber-attack and successfully insured for its repercussions.

It is also crucial that boards of directors conduct the necessary due diligence to be sure that the cyber insurance carrier their company uses has a good claims paying and claims handling history and has a proven history of rapid and supportive response. When a cyber attack occurs, too often there are doubts as to coverage, which can impact incident response.

Whatever the type of insurance held by a company, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to the workflows enumerated in this article and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility and defensibility, rather than the company itself, the independent digital forensic firm investigating the breach, at the direction of counsel, should lead any briefings with insurance carriers.

As an aside, boards of directors should make sure that during any sort of data breach response, a professional on the incident response team, preferably counsel, will maintain carefully written documentation of all efforts of the response. This will help later on when gathering the "documentation package" to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

4. Third Party Cybersecurity Due Diligence.

Outsourcing of services (such as IT, payroll, accounting, pension and other financial services), which typically involve the transfer of, or allowing access to, PII from a company to its vendor, has become increasingly common for today's corporations.

Given that cyber-attackers will often traverse across a company's network and into the networks of its vendors or vice versa, cyber-attacks can often result in disputes as to the culpability for an attack. As a result, in most data breach scenarios, vendors and companies can end up pointing the finger at one another for their respective cybersecurity failures.

Thus, boards should be concerned if any third party vendor has access to a company's networks, customer data or other sensitive information -- or if there exists any sort of other cybersecurity risk of the outsourced function.[25]

[25] Vendors who become entangled in the cyber-attack of a customer that includes PII of, for example, their customers' employees, can be subject to claims by those whose information is lost, as well as by their client. See, e.g., *Caudle v. Towers, Perrin, Forster & Crosby, Inc*., 580 F. Supp. 2d 273 (S.D.N.Y. 2008). In that case, the court dismissed claims for negligence and breach of fiduciary duty brought by an employee against his employer's pension consultant whose laptop containing PII of employees was stolen; the employee sought on behalf of himself and others credit monitoring costs. The court dismissed the negligence claim in the absence of evidence that the information had been accessed or used. It also dismissed the claim for breach of fiduciary duties, again on the ground that the plaintiff had not shown he had suffered any damages. The court did allow the claim for breach of contract to proceed to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor under the terms of the contract. See also *Ruiz v. Gap*, Inc. 622 F. Supp.2d 908 (N.D. Cal. 2009) (in which sued a company's vendor for losing their Personal Information when a laptop was stolen containing information with job applications; the court dismissed the claims for lack of requisite appreciable harm in light of the fact that the plaintiff had not been a victim of identity theft but rather was claiming increased risk of future identity theft and seeking credit monitoring costs), aff'd, 380 F. App. 689 (9th Cir. 2010) (holding that under California law, a plaintiff must have either prior possession or a vested legal interest in money or property lost in order to claim restitution).

In addition, boards should understand if and how the company incorporates requirements relating to cybersecurity risk into its contracts with vendors, these requirements may trigger notification responsibilities. In the event of a data breach, corporate vendors will want to know all relevant facts relating to the cyber-attack, especially: if their data has potentially been compromised; if services will experience any disruption; the nature of remediation efforts; if there are any official or unofficial findings any investigation; or if there is any other information which can impact their operations, reputation, etc.

Vendors may also request images of malware and IOCs or to visit/inspect the company with its own investigation team. Venders may ask for weekly or even daily briefings and may demand attestations in writing with respect to any findings pertaining to their data. Some customers may also have contractual language establishing their rights when a cyber-attack occurs, which can range from notification, to on-site inspections, to the option of an independent risk and security assessment of the victim company (at the victim company's, and not the customer's, expense).

Moreover, if third party vendors conduct remote maintenance of a company's networks and devices, in the event of a cyber-attack, the company may want to confirm it can obtain copies of any relevant logs, as well as access the third party system to scan for IOCs.

Boards of directors should probe the practices and procedures with respect to the cybersecurity of third party vendors. Boards of directors should ask about the company's information security procedures (including training) concerning third party vendors authorized to access a company's network.

5. Physical Security.

Contrary to many popular notions of cyber-attacks, cyber-attacks can sometimes begin with a physical breach. For instance, when an outsider to surreptitiously gather fodder for a social engineering scheme (such as a spearfishing campaign)[26] or when an insider (such as a so-called "bad leaver")[27] gains access to a company's network and wreak havoc, without initially using malware or other clandestine technological means.

---

[26] "Spearphishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by 'random hackers' but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority." http://searchsecurity.techtarget.com/definition/spear-phishing.

[27] "The 21st Century Genesis of the Bad Leaver," by John Reed Stark, the Bloomberg BNA Privacy & Security Law Report, available at http://www.strozfriedberg.com/files/Publication/15ed9779-9ba6-46f8-8e15-02cb04fab267/Presentation/PublicationAttachment/d30ed326-ed0e-47c5-a74b-08eadf0b3b5b/Bad%20Leaver%20Article%20Reprint.pdf.

Hence, boards should also engage in a cursory review of physical security of facilities, including management's plans for reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

6. A Digital Forensics/Data Breach Response Firm on Call.

When a company experiences a cyber-attack, the company will likely need to hire an expert and experienced digital forensics/data breach response firm to investigate for several reasons. First, very few companies employ the kind of personnel who have the technological expertise to understand and remediate today's cyber-attacks. Second, like any company in a crisis, engaging an independent and objective investigator not only insures integrity in the response but also creates a defensible record if challenged later on (e.g. by regulators, class action lawyers, partners, customers, etc.). Finally, if the digital forensics/data breach response firm is engaged by outside counsel, a company can (arguably) maintain and secure the attorney-client privilege for the reports and other investigative documents pertaining to the attack.

Given the scarce number of firms who can truly investigate a cyber-attack, especially those with malware reverse engineering expertise, it makes sense to search for a firm before experiencing a cyber-attack.[28]

A quick side note on malware: board members should realize the term "malware" is often misunderstood. The term "malware" is often defined as software designed to interfere with a computer's normal functioning, such as *viruses* (which can wreak havoc on a system by deleting files or directory information); *spyware* (which can gather data from a user's system without the user knowing it.); *worms* (which can replicate themselves in order to spread to other computers -- unlike a computer virus, a worm does not need to attach itself to an existing program)[29]; or *Trojan horses* (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm).

However, the definition of malware is actually far broader. In the context of a cyber-attack, malware means any sort of program or file that is used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a company's headquarters, legitimate software can actually be malware. For example, during an *"Advanced Persistent Threat"* or *"APT"* attack,[30] attackers will often use "RAR" files as containers for

---

[28] Further, when a cyber-attack hits, the company will require immediate assistance and there will not be time for the usual due diligence and contractual review of the engagement of an incident response firm – so having an agreement, such as a master service agreement, in place makes sense. Also, when negotiating cyber insurance policies, some insurance policies will seek "panel" and "prior consent" provisions that purport to mandate that an insured hire a specific digital forensic/data breach response firm (even if the victim firm already has a prior existing relationship with a particular vendor). Insured should consider such a provision carefully; much like choosing one's own surgeon for a heart procedure, an insured might want the same freedom of choice when it comes to selecting a digital forensics/data breach response firm.

[29] UCSB ScienceLine "What is the difference between a computer virus and a computer worm?" at http://scienceline.ucsb.edu/getkey.php?key=52.

[30] So-called APT attacks are typically stealthy, sophisticated, targeted and relentless state-sponsored attacks that employ carefully crafted and evolving reconnaissance, low-and-slow approaches that are typically difficult to detect, and are not flagged by antivirus technologies and other traditional cybersecurity tools. In

transporting exfiltrated information, yet RAR files have a broad range of legitimate uses and can be used in the context of general corporate activities.[31]

Thus, reverse engineering malware, which can be hiding in plain sight, is both an art and a science. Forensic investigators, incident responders, security engineers, and IT administrators employ a broad range of practical skills to examine malicious programs that target, access and infect corporate computer systems. Understanding the capabilities of malware is not only critical for responding to information security incidents, but it is also critical to an organization's ability to derive threat intelligence and to fortify defenses.

Yet, malware reverse engineering is costly, with hourly rates more akin to a law firm partner's rather than information technology specialists. Even finding a specialist with reverse malware engineering skills can quickly become a challenge -- educational institutions are only just beginning to graduate individuals with malware skills and most malware specialists are self-taught or are "home-grown" within digital forensic firms. Thus, Boards should bear in mind that without a competent digital forensics firm, staffed with digital forensic examiners who are skilled at malware reverse-engineering, its executives may end up feeling like a homeowner with a rapidly flooding basement -- yet no plumber to help find the leak and plug it up.

7. Outside Legal Counsel on Call.

Just about all incident response workflow requires careful legal navigation because, among other things, the legal ramifications of any failure can be calamitous or even fatal for any public or private company. Clearly, outside counsel or inside counsel should lead investigative workflow, quarterbacking the investigation and remediation for the c-suite and sharing with senior management the ultimate responsibility for key decisions. Just like any other independent and thorough investigation, the work relating to a cyber-attack will involve a team of lawyers with different skillsets and expertise (e.g. regulatory; ediscovery; data breach response; privacy; white collar defense; litigation; law enforcement liaison; and the list goes on).

In addition to the governmental investigations and litigation, the list of civil liabilities after a cyber-attack is almost endless, including shareholder lawsuits for cyber security failures; declines in a company's stock price; and management negligence. There may also be consumer/customer driven class action lawsuits against companies falling victim to cyber-attacks, alleging a failure to adhere to cyber security "best practices."[32]

---

fact, most malware used APT attackers is undetectable by off-the-shelf antivirus products. The term APT has been coined to describe specific types of adversaries, exploits, and targets used for explicit strategic intelligence gathering goals. Victims of APT attacks include global financial institutions like Citigroup; large U.S. hospital groups like Community Health Systems; worldwide U.S. defense contractors like Northrup Grumman and SAIC; international defense contractors like Israeli defense firms Elisra Group, Israel Aerospace Industries and Rafael Advanced Defense Systems; well-known data security agencies like RSA and even large government agencies like OPM.

[31] Specifically, RAR is the native format of WinRAR archiver. Like other archives, RAR files are data containers, they store one or several files in the compressed form. After you downloaded RAR file from the Internet, you need to unpack its contents in order to use it. http://www.rarlab.com/rar_file.htm.

[32] See e.g. "Sony Hit With Fourth and Fifth Class-Action Lawsuits Over Stolen Data," by Austin Siegemund-Broka, (December 19, 2014) available at http://www.hollywoodreporter.com/thr-esq/sony-hit-fourth-fifth-class-759563 (see complaint at http://www.scribd.com/doc/250633150/Shapiro-v-Sony); "Supervalu Hit

Even more importantly, with respect to cyber-attack investigations, attorney-client privilege will arguably apply to the work product from the digital forensic investigators hired by outside counsel. Protecting communications with the attorney client privilege is not done to hide information. Rather, the privilege helps protect against inaccurate information getting released in an uncontrolled fashion and allows for more careful contemplation and preparation for litigation or government investigation/prosecution, two scenarios more and more likely to occur.[33]

Board members should query management and insure that within the legion of law firms on its contact list, a law firm with cybersecurity expertise is also on speed dial.

8. Logging Capabilities.

After a data breach, in addition to user systems (like laptop and desktop computers), servers, etc., the logs of other systems such as firewalls and intrusion detection systems will also require analysis. Exactly what logs are available relating to a cyber-attack depends on a company's overall cybersecurity policies and practices. Logging retention can differ dramatically among companies – and some companies may not have any log management system that aggregates logging information, which means that its logging information will be scattered and disorganized. Also, some companies may only preserve logs for a short period, such as thirty days, before "rolling over them" and thereby deleting the logs permanently. [34]

Logging information can include logs relating to events occurring with firewalls, operating systems, applications, anti-virus software, LANDesk,[35] web servers, web proxies, VPNs,[36] change auditors, DHCPs[37] and a broad range of other audit files.[38]

With Lawsuit After Breach," available at http://www.bankinfosecurity.com/supervalu-hit-lawsuit-after-breach-a-7214; "Community Health Systems Faces Lawsuit," available at http://www.databreachtoday.com/community-health-systems-faces-lawsuit-a-7238.

[33] See also, "Law Firms Tout Cybersecurity Cred," By Christopher M. Mathews, (March 31, 2013) Wall Street Journal available at (http://www.wsj.com/articles/SB10001424127887324883604578394593108673994; "Law Firms Offer Cybersecurity Advice and Attorney Client Privilege to Firms," by Debra Cassens Weiss (April 22, 2013) available at http://www.abajournal.com/news/article/law_firms_offer_cybersecurity_advice_and_attorney-client_privilege_to_hacke.

[34] "Deficiencies in security logging and analysis can allow attackers to hide their location, malware, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records, victims can remain blind to the details of the attack and to subsequent actions taken by the attackers. Sometimes logging records are the only evidence of a successful attack and without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Many organizations keep useful logs for compliance purposes, but attackers rely on the fact that such organizations might only rarely review their logs, and never discover that that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files." https://www.sans.org/critical-security-controls/control/14.

[35] "LANDesk is an asset management software system used to remotely inventory and manage desktop

Most free and commercial operating systems, network services and firewall technologies offer logging capabilities and can contain a treasure trove of relevant evidence requiring investigative analysis and resources (such as a SIM/SEM) as well as human resources in the form of specially qualified digital forensic examiners.[39]

Logging information can be of critical use during a cyber-attack response, and it is too often something management overlooks as a priority; thus, boards should ask management at least a few questions as to their logging practices and procedures.

9. Penetration Testing/Risk and Security Assessments/NIST Framework.

Just like an annual physical check-up by a physician, a company should undergo a risk and security assessment of their inner cybersecurity workings. Implementing cybersecurity solutions requires a comprehensive risk assessment to determine defense capabilities and weaknesses and ensure the wise application of resources. What works best is a disciplined yet flexible methodology that incorporates a company's organizational culture, operational requirements and tolerance for risk, and then balances that against current technological threats and risk. In the end, a proper risk and security assessment quantifies risk, develops meaningful risk metrics and conveys the effectiveness of risk mitigation options in clear and concise terms.

Board members should ask to review any risk and security assessment reports, penetration testing results,[40] etc. One caveat though – companies should avoid engaging consultants

---

computers. It has the ability to report on installed software and hardware, allow remote assistance, and install operating system security patches." American University Office of Information Technology Frequently Asked Questions About LANDesk http://www.american.edu/oit/software/LANDesk-FAQ.cfm.

[36] A virtual private networks ("VPN") is a network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network.

[37] Dynamic Host Configuration Protocol ("DHCP") is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

[38] For the best results, such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled in order to ensure that each managed item actively connected to the network is periodically generating logs.

[39] Analytical programs such as SIM/SEM ("Security Incident Management" or "Security Event Management") solutions for reviewing logs can only provide value, when the right expert is conducting the analysis. Actual correlation tools can make audit logs far more useful for subsequent manual inspection and can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand what is gleaned from log files.

[40] There exist no standardization about penetration testing (like some sort of emissions or DNA test) and some commentators have very strong opinions about the utility and value of penetration testing. See e.g.

who present deliverables that provide a written laundry list of problems in need of solutions or a so-called "heat map," which identifies the most serious potential weaknesses. The reason? Because the reality is that most companies will not be able to cure all weaknesses (because for example, of cost concerns, logistical impossibilities, practical barriers, etc.). Thus, though intended for a company's benefit, the heat maps and laundry lists can also provide regulators, law enforcement, class action lawyers and other disgruntled parties with a fast and easy roadmap for liability.

Relatedly, a board can begin to assess a company's possible cybersecurity measures by reviewing the *Framework for Improving Critical Infrastructure Cybersecurity*, released by the National Institute of Standards and Technology ("NIST") in February 2014. The NIST Cybersecurity Framework (the "Framework") is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks.[41] The Framework is a user-friendly text, which does not require a computer science degree in order to understand its basic notions. NIST even provides a "Roadmap for Improving Critical Infrastructure Cybersecurity," which is a nine-page outline that should be required reading for all corporate board members.[42]

Though the Framework is voluntary guidance for any company, its so-called Core Functions dominate discussion at cybersecurity symposia and the government is strongly encouraging consideration of NIST standards by boards of directors. For instance, recently, at a New York Stock Exchange conference, SEC Commissioner Luis Aguilar noted in a speech concerning cybersecurity and boards of directors that "[a] t a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed.[43]",

---

"Penetration Testing Should Not be a Waste of time," by Jim Bird (October 4, 2014) available at http://architects.dzone.com/articles/penetration-testing-shouldnt. Thus, careful consideration should be given to how to, and who should, conduct a company's penetration testing and how the results should be interpreted. "Penetration testing "Conducting a Penetration Test on an Organization," Sans Institute InfoSec Reading Room, available at http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67.

[41] The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (the "NIST Cybersecurity Framework"), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, was released in response to President Obama's issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecurity," dated February 12, 2013. The NIST Cybersecurity Framework sets out five core functions and categories of activities for companies to implement that relate generally to cyber-risk management and oversight, which the NIST strips down to five framework *Core Functions*: Identify, Protect, Detect, Respond and Recover. This core fundamentally means the following: companies should (i) identify known cybersecurity risks to their infrastructure; (ii) develop safeguards to protect the delivery and maintenance of infrastructure services; (iii) implement methods to detect the occurrence of a cybersecurity event; (iv) develop methods to respond to a detected cybersecurity event; and (v) develop plans to recover and restore the companies' capabilities that were impaired as a result of a cybersecurity event. See http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf at p. 8.

[42] NIST Roadmap for Improving Critical Infrastructure Cybersecurity (February 12, 2015) http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[43] "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," Speech by SEC

Moreover, though it is probably too early to tell for sure, the NIST standards seem destined to become a baseline for best practices by companies, including in assessing legal or regulatory liability.

10. Lessons Learned from Prior Attacks.

When a company experiences a cyber-attack, aside from the cyber-attack's investigation, remediation, etc., a company should also engage in a bona fide review after the fact – and organize and document the lessons learned.

For example, DOS (Denial of Service) or DDOS (Distributed Denial of Service) attacks continue to pose a serious threat to most companies, especially those with an active online commerce component to their operations – and should always be an important Board concern.[44] Boards should have an understanding of how many DOS/DDOS attacks the company has experienced; the specific actions a company is taking to deter DOS/DDOS attacks; and how the company has learned form prior DOS/DDOS attempts.

Moreover, remediation of a data breach can require more than installing new hardware and software both for fortification and detection – and more than even constructing an entirely new network security suite. Remediation may also require deployment of a new solution within the category of "endpoint detection and response." End point detection and response offer state-of-the-art software/hardware solutions, which can detect possible future breaches and gather relevant data in an easily and quickly searchable database.

Some examples of endpoint detection and response state-of-the-art software and hardware designed to identify attacker behavior and their tools, tactics and procedures are Carbon Black,[45] Palo Alto firewalls[46] or FireEye MIR.[47] These kinds of solutions are installed within the entire attack vector including domain controllers, database servers and user work stations.

Commissioner Luis Aguilar available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VPxpsEJtlRF (June 10, 2013).

[44] "DDOS attacks in 2014: Smarter, Bigger, Faster, Stronger," by Gur Shatz, (April 20, 2014) available at http://venturebeat.com/2014/04/20/ddos-attacks-in-2014-smarter-bigger-faster-stronger/.

[45] "Carbon Black, within the Bit9 + Carbon Black Solution, delivers the first true continuous response solution. Carbon Black's primary goal is to reduce the cost and complexity of incident response by providing continuous endpoint visibility and signature-less detection capabilities to deliver full context, attack classification and situational awareness of the threats attacking your enterprise. Carbon Black can automate the tedious and time-consuming data acquisition process by continuously recording and understanding the relationships of the critical data necessary to unravel the full lifecycle and kill chain of an attack." See https://www.bit9.com/solutions/security-incident-response/.

[46] "Palo Alto firewalls are part of the large suite of Palo Alto cybersecurity appliances designed to manage, implement and optimize new age firewall systems to safely allow applications, and tackle the threat of modern day malware." See https://www.paloaltonetworks.com/network-infrastructure/cyber-security-appliances.

[47] Among other things, MIR, owned by Fire Eye, is designed to detect malware and other signs of compromise on endpoints across the enterprise and: 1) sweep thousands of endpoints for evidence of compromise, including malware and irregular activities; 2) enable remote investigate securely over any network, without requiring access authorization; and 3) collect targeted forensic data, with intelligent filtering to return only the data needed. See https://www.fireeye.com/products/mir-endpoint-forensics.html.

Conclusion

Cybersecurity has quickly emerged as a key corporate risk area and therefore one that a board of directors should address. For instance, in a recent speech on boards and cybersecurity, SEC Commissioner Luis Aguilar warned an audience of corporate board members:

> Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.[48]

Yet unfortunately, the public's view of cyber-attack victims is less about understanding and sympathy, and more about anger, suspicion and finger-pointing. The world of incident response is an upside-down one: rather than being treated like *criminal victims*, companies experiencing data breaches are often treated like *criminals*, becoming defendants in federal and state enforcement actions, class actions and other proceedings. And given in particular the 47 or so separate state privacy regimes, together with a growing range of federal agency jurisdiction, instead of accepting a helping hand, cyber-attack victims are instead accepting service of process of multiple subpoenas.

These harsh realities together with the spate of large scale and headline grabbing cyber-attacks experienced in the past year (and that most experts believe that this is just the beginning of a new era of cybersecurity defense),[49] mean that members of corporate boards will become much more actively involved in ensuring the organizations they oversee are adequately addressing cybersecurity. For corporations, this is the dawning of a new era of data breach and incident response, where trying to avert a cyber-attack is like trying to prevent a kindergartener from catching a cold during the school year.

Formerly looked upon as the problem of the IT director, cybersecurity has quickly evolved into a board issue and responsibility, which the board has a fiduciary duty to understand and oversee. In the aftermath of a corporate cyber-attack, boards and the companies they govern are subjected

---

[48] "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," Speech by SEC Commissioner Luis Aguilar available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VPxpsEJtlRF (June 10, 2013).

[49] "Executives in Davos Express Worries Over More Disruptive Cyber attacks," by David Gilles, New York Times (January 22, 2015) ("You will get a data breach, period . . . If you think you haven't been attacked, you're lying to yourself.") available at http://dealbook.nytimes.com/2015/01/22/in-davos-executives-express-worries-over-more-disruptive-cyberattacks/?_r=0.

to immediate public scrutiny and, in many cases, unwarranted criticism. This new cyber-reality has essentially removed the distinction between board member and IT executive.[50]

But cybersecurity engagement for members of the board of directors does not mean that members should obtain computer science degrees or personally supervise firewall implementation and intrusion detection system rollouts. Boards of directors can accomplish oversight of cybersecurity in two ways. First, by using the concerns outlined in this article to become actively involved in ensuring the organizations they oversee are adequately addressing cybersecurity. Second, and most importantly, by approaching the subject in much the same way as an audit committee probes a company's financial statements and reports: with a vigorous, skeptical, intelligent and methodical inquiry.

[50] "Corporate Boards Race to Shore-up Cybersecurity: Directors Grapple With Issues Once Consigned to Tech Experts, by Danny Hadron, Wall Street Journal (June 29, 2014) available at http://www.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146. See also, "Homeland Security Wants Corporate Board of Directors More Involved in Cyber-security," by Ellen Messmer, NetworkWorld.com (July 29, 2014) available at http://www.networkworld.com/article/2458975/security0/homeland-security-wants-corporate-board-of-directors-more-involved-in-cyber-security.html ("Setting corporate cyber-security policy and taking actions around it must be a top concern for the board of directors at any company, not just the information-technology division, the Department of Homeland Security (DHS) indicated as a high-level official there backed a private-sector effort to raise awareness at the board level.").