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

CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

BOARDS OF DIRECTORS AND CYBERSECURITY: APPLYING LESSONS LEARNED FROM 70 YEARS OF FINANCIAL REPORTING OVERSIGHT

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

Hardly a day goes by in legal and consultant circles when some expert somewhere is not opining on the need for corporate boards to exercise some manner of cybersecurity oversight. While opinions vary, everyone seems to agree that corporate boards need to bring a greater sense of urgency to address the growing business risk of cyber-attacks.

Yet, even the most experienced commentators are underestimating the threat of cyber-attacks, and, even more importantly, are overlooking a glaring history lesson that sits in plain view. As a result, these expert recommendations are unfortunately missing their mark.

What is this conspicuous history lesson? Boards of directors formulating their cybersecurity oversight should look no further than the current board oversight paradigm for financial accounting and reporting. Boards should put in place the same governance procedures to oversee a corporation's cybersecurity wellness that have proven effective and sufficiently flexible to assess and validate financial statement accuracy and reliability.

As cyber-attacks continue to proliferate, more and more corporate boards will come to realize that cybersecurity risks now actually trump financial accounting risks - and not just because technology and networks touch every aspect of an enterprise. The nature, extent and potential adverse impacts of these risks demand a proportionate response.

Consider the history of board oversight of financial accounting: As it became clear that corporate *insiders* were capable of engaging in misconduct, the active oversight and

independent supervision over financial controls and governance structures similarly evolved, reducing the risk of financial fraud, fiscal misstatements and management malfeasance. Along those lines, the efficacy of using independent auditors, audit committees and management certifications to deter and minimize such *insider* misconduct became widely understood and embraced.

But threats to financial accounting transparency and accuracy are primarily insider driven. In contrast, cyber threats can originate from both *inside* and *outside* corporate walls, resulting in a much broader risk profile that requires at least an equivalent if not greater board attention and focus. Indeed, when compared to the risks associated with internal accounting fraud schemes, individual financial malfeasance and other instances of financial reporting deceit or neglect, suffering a cyber-attack can be far more severe in scope, far more cosmic in breadth and far more unpredictable in latitude.

For instance, after suffering a cyber-attack, a corporation must not only bear the substantial regulatory and litigation costs associated with potential privacy violations – that is just the tip of the iceberg. There is so much more damage and destruction. Cyber-attacks involving the theft of intellectual property can result in a company's immediate or even permanent loss of revenue and reputation; cyber-attacks involving denial of services (such as a website being shut down by nefarious hackers) can disrupt or forever diminish consumer or customer confidence; cyber-attacks involving exfiltration of private company emails can have a tumultuous impact upon senior management and create an international uproar; cyber-attacks involving destruction of technological infrastructure or damage to the integrity of a company's data can require massive and costly remediation; cyber-attacks involving the theft of (and future trading upon) confidential information can damage the integrity of a company's stock price and disrupt financial markets; and the list goes on.

Notwithstanding these potentially grave consequences; notwithstanding the fact that most experts now view cyber-attacks to be inevitable; and notwithstanding the pervasive nature of the risk, most corporate boards fail to allocate to cybersecurity the same level of oversight routinely afforded to the area of financial reporting.

We believe this needs to change.

Just as occurred in the financial accounting realm, old and stale governance models must be modified and enhanced to address the very real, difficult to control and ever increasing enterprise threat of cyber-attacks. In practical terms, this means that, just as it does for financial reporting, every corporate board should:

- Create a cybersecurity committee (just like its audit committee);
- Engage an independent cybersecurity firm to conduct an annual cybersecurity audit (just like an independent accounting firm conducts and signs off on an annual financial audit); and

- Add cybersecurity expertise and knowledge to the board (sitting right beside the board's accounting and financial expert).

I. Introductory Roadmap.

To demonstrate the logic of our recommendations, we engage in a three-step analysis.

First, we present a brief history of board oversight of financial reporting. The warning signs and multiple scandals that over time steered boards and regulatory bodies to the now widely-adopted and embraced oversight approach concerning financial reporting provide a powerful analogue for addressing the risks and challenges that corporations routinely face in the emerging area of cybersecurity. In other words, it is déjà vu all over again, and boards should not wait to act until after the world experiences the cyber-era equivalent of the 1929 stock market crash or the 2002 Enron collapse.

Second, we explain how and why cybersecurity has begun to eclipse financial reporting as a top corporate risk. We note that: 1) the sheer magnitude of a cyber-attack exacts a calamitous injury of risk and tumult, far more penetrating than for instance, a financial reporting mishap; and 2) the rising morass of regulatory attention on cyber-attacks has begun to surpass governmental attention on corporate financial reporting. For public corporations in particular, the aftershocks of a financial reporting problem can pale in comparison to the debilitating revenue loss, not to mention the regulatory onslaught and litigation fallout, experienced in the aftermath of a cyber-attack.

Finally, we conclude that corporate boards implementing our recommendations will not only improve the ability of their companies to survive a cyber-attack, but they will also unmistakably demonstrate that board responsibilities are being performed reasonably, diligently and thoughtfully.

II. A Brief History of Boards of Directors Oversight of Financial Accounting and Reporting.

Boards of directors did not always burden themselves with corporate financial accounting and reporting responsibilities. Instead, board involvement with corporate financial statements evolved slowly (over almost a century) with certain unexpected threats providing the impetus for its progression.

The explosive growth of business activity stemming from the Industrial Revolution first ignited the widespread adoption of financial auditing methods and prompted the ingress of financial reporting oversight into the boardroom. Railroads became the pioneers in this area, and their efforts to report and control costs, and to measure production and operating ratios, were major catalysts in the development of the accounting profession in the U.S. Soon all corporations began to recognize and appreciate the need for mechanisms to enable fraud detection and greater financial accountability, while investors increasingly relied upon financial reports as corporations began to participate in the stock market.[2]

But when the stock market crashed in 1929, it became apparent that voluntary financial auditing programs alone were insufficient to protect investors from inaccurate and misleading information that could result in substantial economic loss. The government response was the enactment of the Securities and Exchange Act of 1934, which created the Securities and Exchange Commission (SEC) and made financial reporting obligatory for public corporations. The SEC subsequently mandated that publicly traded U.S. companies submit various periodic reports to the agency in a timely fashion, including an annual financial report. To assist the SEC with ensuring these reports were developed in accordance with generally accepted accounting principles (GAAP), third party public accounting firms were eventually required to provide certain assurances about the financial information contained in a corporation's annual financial report.

As financial reporting statutes, rules and regulations expanded, and their enforcement became more of a state and federal priority, the focus of boards of directors on mitigating the risks associated with the plagues of financial fraud evolved considerably, becoming firmly entrenched at the top of every risk-related board agenda. Boards understood that the best control and protection against internal fraud, accounting misstatements or other insider malfeasance would be independent third-party audit and review coupled with enhanced governance and new management capabilities. Specifically, boards reacted by engaging outside accounting firms to conduct independent financial audits; establishing audit committees; and recruiting accounting professionals to join their ranks.

1. The Role and Need for Audit Committees is Identified.

The first major endorsement for the specific establishment of audit committees came from the New York Stock Exchange (NYSE) in 1939, when, in an annual report, the NYSE blithely recommended that " . . . where practicable, the selection of the auditors by a special committee of the board of directors composed of directors who are not officers of the company appears desirable." Almost 35 years later, in 1973, the NYSE published a far more forceful suggestion in a "white paper," stating that an audit committee "no longer represents a corporate luxury, but has become a necessity."[3]

Next, in 1974, the SEC issued *Accounting Series Release No. 165* which, among other things, added the following provision to Regulation 14A of the proxy rules: "If the issuer has an audit or similar committee of the board of directors, state the names of the members of the committee. If the board of directors has no audit or similar committee, so state."[4]

Finally, at the urging of the SEC, on January 6, 1977, the NYSE adopted a requirement for all listed companies to maintain an audit committee.[5] The NYSE mandated that each domestic company with a listed common stock, as a condition of listing and continued listing, establish no later than June 30, 1978, and maintain thereafter, an audit committee comprised solely of directors independent of management and free from any relationship that, in the opinion of its board of directors, would interfere with the exercise of independent judgment as a committee member. Directors who were affiliates of the

company or officers or employees of the company or its subsidiaries would not be qualified for audit committee membership.[6]

Since this time, the audit committee has played an increasingly leading role in corporate governance. Indeed, as the years have passed, Congress, the SEC, the NASDAQ Stock Market and the Public Company Accounting Oversight Board (PCAOB) have continued to recognize the importance and sanctity of financial audits and audit committees to ensuring the actual and perceived trust of shareholders and the general public. And, not surprising, shareholders and other corporate stakeholders have concomitantly increased their expectations in this same regard.

2. SOX Becomes Law.

In 2001 (almost 70 years after the establishment of the SEC), when Enron, Worldcom and other major financial frauds and corporate governance scandals rocked financial markets, many concluded that more rigorous financial reporting requirement and standards were needed – and on July 30, 2002, the Sarbanes-Oxley Act (SOX) became law.

SOX imposed sweeping changes on publicly-traded companies and the accounting profession. Above all else, SOX firmly established that assurances about internal control practices and operations, as well as the quality and integrity of financial reporting, were the responsibility of both management and independent auditors.

Section 404 of SOX directed the SEC to adopt rules requiring each annual report of a company, other than a registered investment company, to contain (1) a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) management's assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting. Section 404 also required the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the PCAOB.

Under the final SEC rules, management's annual internal control report now had to contain:

- a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;

- a statement identifying the framework used by management to evaluate the effectiveness of this internal control; management's assessment of the effectiveness of this internal control as of the end of the company's most recent fiscal year; and

- a statement that its auditor has issued an attestation report on management's assessment.[7]

SOX also caused the accounting discipline to devote more attention to identifying fraud risks during the course of an audit. For example, *Statement on Auditing Standards No. 99*, *Consideration of Fraud in a Financial Statement Audit*, requires auditors to design audit procedures that provide reasonable assurance of detecting fraud that could have a material effect on the financial statements.[8]

III. Cybersecurity Has Begun to Eclipse Financial Reporting as a Top Corporate Risk.

Though perhaps not manifesting as vividly and abruptly as the 1929 stock market crash or 2001 Enron collapse, cybersecurity concerns have for a variety of reasons begun to eclipse financial reporting fraud and management malfeasance as the most important board concerns and enterprise risks. Why?

- Because cyber-attacks and resulting data breaches have become inevitable for corporations;

- Because business operations have become so dependent on technology that cyber-attacks (aimed at stealing private personal information, valuable intellectual property or other corporate electronic assets) now threaten the lifeblood of corporations; and

- Because cybersecurity regulation has rapidly expanded, imparting upon corporations a far more complex, challenging and unpredictable environment than financial regulation.

1. Cyber-Attacks and Data Breaches Are Now Seen as Inevitable.

When an entire class of kindergartners comes home from school with colds, it is not their fault. No one can protect a child from catching a cold; it is inevitable. The same goes for data breaches. Every company can experience a data breach -- and probably already has.[9] When it comes to cyber-attacks, *there is no security*, essentially rendering "cybersecurity" an oxymoron.[10] In short, data breaches are a real threat, not just media sensationalism.

Even the U.S. government has recognized the harsh reality of the inevitability of data breaches, as evidenced by edicts from a range of law enforcement and regulatory organizations, including the U.S. Department of Justice,[11] the SEC,[12] and the U.S. Department of Homeland Security.[13] As former Federal Bureau of Investigation Robert Mueller stated at the RSA Cybersecurity Summit, back in March of 2012, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[14]

Attacks on the information technology assets of companies are also occurring on a widespread and massive scale, typically crossing national borders. Worldwide, recovery from cyber-attacks and other Internet crimes is costing the private sector more than $400 billion per year, estimates the London-based insurer Lloyds.[15]

Furthermore, in addition to the cost of recovery, there are the costs of prevention: the technology research firm Gartner estimates a total of $77 billion in business cybersecurity having been spent for 2015 alone,[16] while the research firm Market and Markets forecasts $170 billion in cybersecurity spending in 2020, at a compound annual growth rate of 9.8%, with North America expected to be the largest market on the basis of spending and adoption of cybersecurity solutions and services.[17]

Clearly, each board of directors must understand that the entity it oversees and governs will, or already has fallen victim to a cyber-attack of some form at some time. And, more significantly, the board will need to clean up the mess and superintend the fallout.[18]

2. Cyber-Attacks Threaten the Lifeblood of Corporations.

The operations (and profits) of public companies in particular have become increasingly dependent upon the almost infinite interconnectivity and instantaneous access facilitated by technology. From manufacturing to retail, from financial institutions to healthcare providers, from fashion to music, and from legal services to accounting services, whatever the industry, every corporation relies on a broad range of interwoven technologies to conduct business.

To complicate matters further, the devices and resources used by corporate personnel continue to multiply, ushering in a new paradigm of cybersecurity where technological infrastructure has expanded dramatically; where data-points reside on multiple platforms (including employee devices, vendor networks, and the cloud); and where cyber-attacks have become as complex and sophisticated as the networks they infiltrate.

Hence, once identified, cyber-attacks now typically demand a host of costly and detailed responses, including: digital forensic preservation and investigation; notification of a broad range of third parties and other constituencies; malware reverse-engineering; surveillance and remediation; fulfillment of state and federal compliance obligations; exfiltration analysis; endless litigation; engagement with law enforcement; the provision of credit monitoring; consumer notification/monitoring services; crisis management; public relations management; and many other incident response work-streams.[19]

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; loss of productivity; extended management drag; and harm to employee morale and overall business performance.

When a corporation experiences a cyber-attack, it is as quick and as debilitating as an athlete rupturing an Achilles tendon – if possible at all, recovery is long, arduous and the athlete may never perform at the same level again.

3. Cybersecurity Regulation and Litigation Have Rapidly Expanded.

The treatment of cyber-attack victims is less about understanding and sympathy, and more about anger, vilification, suspicion and finger pointing. Sadly, the world of incident response is an upside-down one: rather than being treated like the victim of a crime perpetrated by others, companies experiencing a cyber-attack are often treated like the criminal, becoming defendants in federal and state enforcement actions, class actions and a litany of other costly and crippling proceedings.

A. State Cybersecurity Regulation

As the regulatory protections afforded so-called "personally identifying information" (PII) continue to expand, so do the risks in acquiring, storing and transmitting such information. Privacy laws vary by jurisdiction, are interpreted unpredictably, and are in a constant state of flux,[20] with some based broadly and others based on industry sector, such as, laws covering medical records,[21] financial transactions,[22] credit cards,[23] debt collectors,[24] insurers[25] or even library records.[26]

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, etc.); 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).[27] These laws also often describe the responsibilities the so-called "record holder" has in terms of protecting information from unauthorized access or dissemination, modification and/or destruction and the obligation to report cyber-attacks affecting credit card numbers, social security numbers, dates of birth, medical records and other identifying information. When such devices or the data on them are accessed, targeted, exfiltrated, etc. during a cyber-attack, a company's legal exposure to state regulators can be enormous.

Costs triggered by regulators can include individual notifications, heavy fines, injunctions, credit-monitoring services, government audits and even criminal liability. Inadequate privacy protections are particularly important to regulatory investigators; the investigators for example, will analyze carefully the victim's possible culpability for the cyber-attack, such as having inadequate network security or failing to adopt policies and procedures that are reasonably designed to ensure the security and confidentiality of PII.

In general, the data breach notification statutes of each relevant jurisdiction establish that:

- Residents of the jurisdiction must be notified;
- Notices to affected individuals must contain specific content (or are prohibited from containing certain information, as some states, such as Massachusetts, do not want publication of the methodology of the breach or the type of information at risk, while others require the disclosure of such information);
- State attorneys general and other state agencies must be notified, and if so, whether those notices must contain specific content and be provided before notification of affected individuals; and
- Consumer reporting agencies, such as Experian, TransUnion and Equifax, must be notified.

B. Federal Cybersecurity Regulation

In addition to the labyrinth of state laws and regulations, entities may also be subject to a large and evolving array of federal rules and regulations (enforced by multiple federal regulatory agencies) mandating protection of PII and requiring that certain steps be taken in the event of a cyber-attack.

i. The Federal Trade Commission

Historically, the U.S. Federal Trade Commission (FTC) has been the most active with respect to privacy protections arising from a cyber-attack, and its jurisdiction continues to expand.[28] During August of this past summer, the Third Circuit Court of Appeals affirmed a district court's decision, *FTC v. Wyndham Worldwide Corp,*[29] holding that the FTC has authority to regulate a company's inadequate cybersecurity practices.

From April 2008 to late 2009, Wyndham was the victim of three separate network intrusions where hackers allegedly obtained personal information, including payment-card data, for over 619,000 Wyndham customers. In June 2012, the FTC filed a complaint in federal district court alleging that Wyndham's failure to employ reasonable and appropriate cybersecurity measures, and its failure to disclose its lack of such measures, violated the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[30] The district court denied Wyndham's motion to dismiss the FTC's claims, but certified the unfairness claim for interlocutory appeal.

In a significant victory for the FTC, the Third Circuit unanimously affirmed that the FTC possesses authority to regulate corporate cybersecurity practices, and that Wyndham's failure to employ reasonable and appropriate cybersecurity measures could constitute an "unfair" practice under Section 45(a). With this decision, the potential for FTC lawsuits and enforcement actions resulting from data breaches has increased exponentially.[31]

In addition, the FTC (and other federal agencies that regulate financial institutions, including the Federal Reserve Board, National Credit Union Administration, Office of

the Comptroller of Currency and the SEC) has issued regulations to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[32]

ii. The SEC and Other Financial Regulators

Financial institutions in particular are subject to data privacy related federal regulations (and the term "financial institution" is defined very broadly).[33] The SEC for one, has expanded considerably its efforts relating to cybersecurity, [34] beefing up its regulatory examinations of investment advisers and broker-dealers with targeted sweeps for cybersecurity as well as initiating an active cybersecurity enforcement program.[35] The SEC also requires that public companies may also need to disclose cyber risks and incidents as part of their mandated disclosure of material information to potential investors.[36]

Interestingly, for financial firms, the SEC has gone almost so far as to compel that SEC-regulated entities perform periodic penetration testing and risk and security assessments, by publicly emphasizing the importance of penetration testing at financial institutions such as investment advisers, broker-dealers, exchanges, mutual funds, etc.

Along those lines, in April 2014, the SEC announced its first cybersecurity sweep of brokerage and investment advisory examinations in an SEC Risk Alert, which made the unusual and almost unprecedented move of publishing, as a "resource," the so-called "examination module" (i.e. questionnaire) that SEC staff planned to serve upon targets of the sweep. About a year after the SEC's first sweep, the SEC then published a report containing some strong sentiments about cybersecurity. Next, on September 15, 2015, the SEC announced its second sweep of examinations into brokerage and advisory firms' cybersecurity practices, once again providing the examination module as a resource for regulated entities. In the report and in both modules, the SEC makes clear that their examinations will be probing specifically the results of "risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences."[37]

Not to be outdone, the Financial Industry Regulatory Authority (FINRA) also released in February 2015 its *Report on Cybersecurity Practices*, which provided an in-depth report on cybersecurity at broker-dealers. Therein, FINRA offered its own insights into what it expects from firms' cybersecurity risk management practices, and included its expectation that firms implement "sound technical controls, such as identity and access management, data encryption and penetration testing."[38]

Banking regulators are also following a similar path to the SEC and FINRA. New York State's financial services regulator recently unveiled details about potential new cyber security regulations for banks and insurance companies under its jurisdiction, which includes requiring banks "to conduct annual penetration testing and quarterly vulnerability assessments."[39] Moreover, Standard & Poor's has gone so far as to threaten to downgrade banks with weak cybersecurity, even if they have not been attacked.[40]

iii. Federal Communications Commission

The Federal Communications Commission (FCC) began flexing its regulatory muscle into the regulation of cyber-attacks when, on October 2014, in a 3-2 vote, the FCC assessed a $10 million fine on two telecommunications companies for failing to adequately safeguard customers' personal information.[41] Additionally, on April 8, 2015, the FCC entered into a $25 million settlement with AT&T Services, Inc. (AT&T) resulting from the unauthorized access to personal customer information by employees of foreign-based call centers under contract with AT&T.[42] Next, on November 5, 2015, the FCC entered into a consent decree with cable operator Cox Communications to settle allegations that the company failed to properly protect customer information when the company's electronic data systems were breached in August 2014 by a hacker. The FCC alleged that Cox failed to properly protect the confidentiality of its customers' proprietary network information ("CPNI") and PII, and failed to promptly notify law enforcement authorities of security breaches involving CPNI in violation of the Communications Act of 1934 and the FCC's rules.[43] In total, the FCC brought over a half dozen major cybersecurity-related enforcement actions in 2015 and has stressed that it expects telecommunications companies, which now includes broadband internet access providers, to take "every reasonable precaution" to protect their customers' data.[44]

iv. HIPPA and the HITECH Act

The confidentiality and sensitivity of personal health information (PHI) has evolved into a highly-regulated and increasingly important area of government concern. With respect to health-care related data, the Federal Health Information Technology for Economic and Clinical Health Act (HITECH) increased regulatory oversight, and has more stringent data breach notification obligations related to PHI. Companies storing PHI are scrutinized intensely and their privacy and security protocols must pass muster not only under the HITECH Act but also under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which established for the first time a set of national standards for the protection of certain health information.[45]

v. PCI-DSS

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.[46] 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 work stream involving the PCI-DSS can be extremely costly, cumbersome and disruptive.[47]

vi. The Treasury Department

Cyber-attacks represent a pervasive challenge, which can originate from anywhere in the world. Along these lines, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has gone so far as to issue regulations for the cyber-related sanctions program, which target foreign nations and people who participate in cyber-attacks against U.S. citizens, companies or government agencies.[48] Once Treasury has made designations pursuant to this authority, U.S. persons must ensure that they are not engaging in trade or other transactions with persons named on OFAC's *SDN List*. As a general matter, U.S. persons, including firms that facilitate or engage in online commerce, are also responsible for ensuring that they do not engage in unauthorized transactions or dealings with persons named on any of OFAC's sanctions lists or operate in jurisdictions targeted by comprehensive sanctions programs. Such persons, including technology companies, must maintain a tailored, risk-based compliance program, which may include sanctions list screening or other appropriate measures.[49]

vii. Department of Education

Federal jurisdiction can also be triggered if a cyber-attack involves an educational institution, where the U.S. Department of Education (DOE) has an interest. For instance, any school or institution in the U.S. that provides educational services or instruction and receives funds under any program administered by the DOE is subject to the privacy requirements of the Family Educational Rights and Privacy Act (FERPA). Subject to certain limited exceptions, FERPA gives students (or in some cases their parents) the right to inspect and challenge the accuracy of a student's own education records, while prohibiting schools from disclosing those records, or any personally identifiable information about a student contained in those records, without the student's (or in some cases the parent's) consent.[50]

viii. Recent and Future Federal Regulation

Congress is constantly introducing new legislation to address the growing problem of cyber-attacks. For example, President Barack Obama recently signed into law *The Cybersecurity Information Sharing Act* ("CISA"), a significant cybersecurity regulatory initiative. CISA encourages information sharing regarding "cyber threat indicators" and "defense mechanisms" between and among private entities and the federal government. It provides a safe harbor from liability for private entities when transmitting such information or when monitoring for cyber threats, and will likely be interpreted as yet another critical regulatory consideration during the response of a cyber-attack.[51]
Other recently enacted legislation includes: 1) The Cybersecurity Act of 2015, signed into law December 18, 2015, which promotes and encourages the private sector and the US government to rapidly and responsibly exchange cyber threat information; 2) The Cybersecurity Enhancement Act of 2014, signed into law December 18, 2014, which provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness; 3) The National Cybersecurity

Protection Act of 2014, signed into law December 18, 2014, which codifies an existing operations center for cybersecurity; and 4) The Cybersecurity Workforce Assessment Act, signed into law December 18, 2014, which directs the Secretary of Homeland Security, within 180 days and annually thereafter for three years, to conduct an assessment of the cybersecurity workforce of the Department of Homeland Security (DHS).[52] Experts agree that Congress is extraordinarily active and engaged in the area of cybersecurity, with more than 20 proposed major pieces in the legislative pipeline,[53] even going so far as to propose legislation addressing the need for cybersecurity expertise in the boardroom.[54]

IV. Conclusion.

Some months ago, we authored an article discussing critical topics that every member of a board of directors should know about cybersecurity and data breach response.[55] Today we follow-up that article with a recommendation of three structural and governance changes we believe every corporate board of directors should implement.

Following our recommendation will improve overall enterprise risk identification, and management, of cyber-related challenges and threats, and fulfill the most fundamental duty of care that every director owes to the corporation, its shareholders and other stakeholders. After all, if handled correctly and appropriately, data breaches can actually be the kind of successful failure that not only strengthens a corporation's cybersecurity infrastructure but also reinforces a commitment to customers, partners and other fiduciaries.

Our analysis and recommendations draw from the fundamental practices that corporate boards, regulatory authorities and listing bodies have come to demand and expect in the area of financial reporting and audit processes. Let the past become prologue and, as they did with the oversight of financial reporting, boards should follow a similar course as it relates to the borderless[56] and faceless[57] risks associated with cybersecurity. To accomplish this goal, boards should: create a special cybersecurity committee; engage an independent cybersecurity firm to conduct annual cybersecurity audits; and add a cybersecurity specialist to their ranks.

Historically, when it comes to their CFOs and the financial reporting function, the successful board paradigm has been one of vigorous and independent supervision, requiring the participation of independent third parties. The same should go for CTOs, CIOs and CISOs, and the maxim of *trust but verify* should be equally operative in both contexts.

Board members may soon have little choice but to take these steps, not merely to protect their companies but also *to protect themselves*. Given the current D&O litigation landscape relating to cybersecurity issues, cybersecurity breaches not only create regulatory and other legal liability for corporations but can also create personal liability for directors. For their failure to oversee cybersecurity with the requisite level of care the

growing corporate risk of cyber-attacks, boards may be sued[58] or reported by a whistleblower.[59]

Simply stated, for boards contemplating their cybersecurity oversight, there is no need to reinvent the wheel. History provides an authoritative guide. By leveraging financial accounting governance lessons acquired over the past 70 years, and elevating cybersecurity oversight to the top of the risk food chain, boards can better protect their corporations from cyber-adversaries, better carry out their fiduciary responsibilities – and establish a leadership position in managing the emerging and dynamic risk of cyber-attacks.

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

---

[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 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 R. Fontaine is Chief Executive Officer of Corporate Risk Holdings (and formerly served as its Chief Legal Officer), an enterprise risk management firm that owns Kroll, a global investigations, compliance and data breach response firm with over 50 offices located in 30 countries across the world. Messrs. Fontaine and Stark have been friends and professional colleagues for almost 30 years and have collaborated often on issues of cybersecurity, data breach response and digital compliance.

[2] AICPA: Evolution of Auditing, From the Traditional Approach to the Future Audit, by multiple authors (November 2012) at http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_evolution-of-auditing.pdf.

[3] The Recent History of Corporate Audit Committees by Brenda S. Birkett, *Accounting Historian Journal* (January 2014) available at http://www.accountingin.com/accounting-historians-journal/volume-13-number-2/the-recent-history-of-corporate-audit-committees/.

[4] See, SEC Accounting Release 165 (Adopted, December 20, 1974) available at http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1970/1976_0101_SECAccountingReleases.pdf.

[5] Id.

[6] Id.

[7] "SEC Implements Internal Control Provisions of Sarbanes-Oxley Act" (May 27th, 2003) available at https://www.sec.gov/news/press/2003-66.htm.

[8] See, https://www.sec.gov/interps/account/sab99.htm.

[9] When IANS Research recently surveyed IT professionals and executives at 100 organizations in the United States, every company surveyed (all 100 of them), reported that they had recently experienced a significant attack or breach. The questions were answered by IT pros anonymously, with 90 percent of respondents hailing from organizations with $100 million or more in revenue, and titles including Director of IT, CISO, CTO, Developer and Network Administrator, and Security Engineers. See, "The New Reality: Inevitability of Data Breaches and How to Mitigate Risk," by Jonathan Cogley, Wired Magazine (January 7, 2015) available at http://insights.wired.com/profiles/blogs/the-new-reality-inevitability-of-data-breaches-and-how-to?xg_source=activity#axzz3wg4Dt9Yj.

[10] See e.g. "Marc Benioff: Cybersecurity Has Become an Oxymoron," Interview by Bloomberg News Service at Davos (January 15, 2015) available at http://www.bloomberg.com/news/videos/2015-01-22/has-davos-world-economic-forum-lost-its-authenticity-; Cybersecurity: An Oxymoron?" IT Business Edge by Sue Marquette Miranda (June, 2011) available at http://www.itbusinessedge.com/cm/blogs/poremba/cyber-security-an-oxymoron/?cs=47504.

[11] See, "Best Practices for Victim Response and Reporting of Cyber Incidents Version 1.0" U.S. Department of Justice (April 2015) available at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf ("Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack.").

[12] See, "SEC Division of Investment Management Guidance Update No. 2015-02" (April 2015) available at http://www.sec.gov/investment/im-guidance-2015-02.pdf ("The staff also recognizes that it is not possible for a fund or adviser to anticipate and prevent every cyber attack.").

[13] See, Department of Homeland Security Cybersecurity Overview (September 22, 2015) available at http://www.dhs.gov/cybersecurity-overview ("Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.").

[14] See, Remarks by Robert S. Mueller, III, Director, Federal Bureau of Investigation, RSA Cyber Security Conference, San Francisco, CA (March 01, 2012) available at https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[15] Global Network of Director institutes, Perspectives Paper, "Guiding Principles for Cyber security Oversight (November 27, 2015), citing, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

[16] Id.

[17] Markets and Markets Cybersecurity Spending report available at http://www.marketsandmarkets.com/PressReleases/cyber-security.asp.

[18] This reality raises several critical questions: How best to prepare and respond to the attack? How to maintain uninterrupted business operations? How to minimize the loss of critical business information? How to avoid the inevitable reputational damage? As an aside, what every corporation should work towards is therefore cyber resilience i.e. "the ability of an enterprise to anticipate, withstand, recover from, and evolve to improve capabilities in the face of adverse conditions, stresses or attacks on the supporting resources it needs to function." See, "Building Secure, Resilient Architectures for Cyber Mission Assurance," by Harriet Goldman, Mitre Secure and Resilient Cyber Architectures Conference (October 29, 2010) available at https://register.mitre.org/sr/papers1/Building%20Secure%20Resilient%20Architectures.pdf.

[19] For an expanded and detailed discussion of data breach response workflow, see, "Ten Cybersecurity Concerns For Every Board of Directors," by John Reed Stark and David Fontaine (April 2015) available at http://www.cybersecuritydocket.com/2015/04/30/ten-cybersecurity-concerns-for-every-board-of-directors/.

[20] California recently adopted new legislation implementing small but significant changes to its privacy laws. On September 30, 2014, Governor Jerry Brown signed Assembly Bill 1710, which enhances consumer protections by strengthening the requirements businesses must follow in the event of a breach. Specifically, the new law:

- Requires the source of the breach to offer identity theft prevention mitigation services at no cost to the affected person for no less than 12 months if a Social Security Number or Driver's license number are breached;
- Prohibits the sale of social security numbers, except when part of a legitimate business transaction; and
- Provides that existing personal information data security obligations apply to businesses that maintain personal information, in addition to those who own or license the information.

See, https://cybersecuritylawwatch.files.wordpress.com/2014/10/assembly-bill-no-1710.pdf and https://cybersecuritylawwatch.files.wordpress.com/2014/10/cybersecuity-in-the-golden-state.pdf.

[21] See e.g. Massachusetts Laws About Medical Privacy available at http://www.mass.gov/courts/case-legal-res/law-lib/laws-by-subj/about/privacy.html.

[22] See e.g. State of California Department of Justice, Your Financial Rights available at http://oag.ca.gov/privacy/facts/financial-privacy/rights.

[23] Texas Attorney General's Office Credit Card FAQ, available at https://www.texasattorneygeneral.gov/faq/cpd-credit-card-faq.

[24] See e.g. Privacy Laws Affecting Debt Collection in Washington, available at http://www.avvo.com/legal-guides/ugc/privacy-laws-affecting-debt-collection-in-Washington.

[25] Several state departments of insurance have issued bulletins and regulations requiring insurers doing business in their states to send data breach notifications to the departments of insurance when an insurer has suffered a data breach. For example, Ohio Insurance Bulletin 2009-12 requires insurers to provide notice to the Ohio Department of Insurance of loss of control of policyholder information within 15 calendar days after discovery of the loss of control if it involves more than 250 Ohio residents. And, pursuant to Chapter 11 of Rhode Island Insurance Regulation 107, licensees of the Rhode Island Department of Business Regulation, which includes insurance companies, must notify the department of a data breach in the most expedient time possible and without unreasonable delay. Similarly, the Wisconsin Office of the Commissioner of Insurance, under a bulletin dated December 4, 2006, requires that insurers notify the office no later than 10 days after the insurer has become aware of unauthorized access to the personal information of the insured. The Connecticut Department of Insurance issued Bulletin IC- 25 on August 18, 2010 to require all entities doing business in Connecticut that are licensed by or registered with the Department to notify the Department of any information security incident. Notice must be provided as soon as the incident is identified, but no later than five calendar days after the incident is identified. The Connecticut Bulletin lists numerous facts that must be disclosed in the notification to the Department of Insurance, as they are known at the time, including details about the incident and remedial actions taken. Notice must also contain a draft of the notice the licensee or registrant intends to send to Connecticut residents. The Connecticut Bulletin also imposes a requirement on the licensee or registrant to report incidents involving a vendor or business associate. https://www.acc.com/chapters/ne/loader.cfm?csModule=security/getfile&PageID=1300198 at page 92.

[26] See, State Privacy Laws Regarding Library Records, American Library Association, available at http://www.ala.org/advocacy/privacyconfidentiality/privacy/stateprivacy.

[27] See e.g. https://cybersecuritylawwatch.files.wordpress.com/2014/10/cybersecuity-in-the-golden-state.pdf.

[28] "FTC's Hammer Gets Bigger with Lab MD Case," by Amy Worley, National Law Journal (January 26, 2015) available at http://www.natlawreview.com/article/ftc-s-hammer-gets-bigger-labmd-case-federal-trade-commission.

[29] FTC v. Wyndham Worldwide Corp., No. 14-3514 (3d Cir. Aug. 24, 2015) available at http://www.wlrk.com/docs/FTCvWyndham3dCirOpinion20150824.pdf.

[30] 15 U.S.C. § 45(a).

[31] However, current case law in this area is not all going the way of the FTC. A post from Alston & Bird notes that another recent case, has established some sharp limits. See, "FTC and Wyndham Settle Data Security Allegations," by Kacy Brake, Alston and Bird Privacy and Data Security Blog (December 15, 2015) available at http://www.alstonprivacy.com/ftc-and-wyndham-settle-data-security-allegations/ ("While Wyndham held that the FTC's unfairness authority extends to data security, a recent case suggests that the proof required to establish that a company's act or practice "causes or is likely to cause substantial injury" in the data security context is a high bar. In a November 13, 2015 decision, In re LabMD Inc., the FTC's Chief Administrative Law Judge, D. Michael Chappell, called into question FTC enforcement in the data privacy space. Judge Chappell dismissed the FTC's complaint against LabMD, finding that the FTC failed to carry its burden of demonstrating a "likely substantial injury" resulting from LabMD's allegedly "unfair" data security practices. Judge Chappell ruled that the FTC is required to show that substantial injury to consumers is probable, not merely possible, when there is no evidence of actual consumer injury. Given the ramifications of this decision, the FTC has filed a formal notice seeking an appeal before the full Commission."). But see, "Big Data: A Tool for Inclusion or Exclusion? Understanding The Issues," a January 2016 FTC report, available at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (which has been described as "a concise but essential guide to corporate big data behaviors in the increasingly hawkish view of the FTC.") "FTC Releases Big Data Bible," By Lisa Brownlee Forbes (January 7, 2016) available at http://www.forbes.com/sites/lisabrownlee/2016/01/07/ftc-releases-its-big-data-bible/).

[32] See, Pub. Law 108-59, codified at 15 U.S.C. § 1681 et seq. FACTA is federal legislation directed at protecting consumers against identity theft as well as enhancing the accuracy of consumer report information. It prohibits businesses from printing out more than five digits of a credit card number, and allows consumers to obtain a free credit report every 12 months from each of the nationwide credit reporting agencies. The new regulations, which are commonly referred to as the Red Flags Rules, (16 C.F.R. § 681.) are directed at preventing identity theft by requiring covered entities to develop and implement a written Identity Theft Prevention Program to detect the warning signs – i.e. the "red flags" – of identify theft in order to prevent and mitigate identity theft.

[33] For example, the Gramm-Leach-Bliley Act ("GLBA") was enacted in 1999 to reform the financial services industry and address concerns relating to consumer financial privacy. Title V of the GLBA establishes a minimum federal standard of privacy and applies to financial institutions, including companies that were not traditionally considered to be financial institutions, such as insurance companies. See http://www.ftc.gov/privacy/privacyinitiatives/glbact.html on the applicability of Title V of GLBA to insurance.

[34] Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught by John Reed Stark, Bloomberg BNA Securities Regulation & Law Report (April 2014) at https://www.johnreedstark.com/wp-content/uploads/sites/180/2014/12/Cybersecurity-and-Financial-Firms-Bracing-for-the-Regulatory-Onslaught_BloombergBNA_Stark_April2014.pdf.

[35] For example, on September 22, 2015, the SEC announced that R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, agreed to settle charges that it failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised PII of approximately 100,000 individuals, including thousands of the firm's clients. This was the first SEC enforcement action which specifically addressed its expectations pertaining to the cybersecurity of the entities it regulates, and made a subtle but strong statement concerning the importance of pen testing. According to the SEC, R. T. Jones stored sensitive PII of clients and others on its third party-hosted web server, which was attacked in July 2013 by an unknown hacker who gained access to the data on the server, rendering the PII of more

than 100,000 individuals, including thousands of R.T. Jones's clients, vulnerable to theft. The SEC noted that, among other things, R.T. Jones failed to conduct periodic risk assessments. See *In the Matter of R.T. Jones Equity Capital Management, Inc.* (September 22, 2015) at https://www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[36] Disclosing Cyber-attacks: How to Follow SEC Guidance, by John Reed Stark (November 1, 2011) available at https://www.johnreedstark.com/wp-content/uploads/sites/180/2014/12/2011_Disclosing-Cyberattacks-How-To-Follow-SEC-Guidance-JRS.pdf.

[37] See, SEC Doubles Down on Cybersecurity, by John Reed Stark, CybersecurityDocket.com (September 16, 2015) available at http://www.cybersecuritydocket.com/2015/09/23/sec-doubles-down-on-cybersecurity/.

[38] Id.

[39] Potential New NYDFS Cyber Security Regulation Requirements (November 9, 2015) available at http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

[40] S&P Credit FAQ, "How Ready Are Banks For The Rapidly Rising Threat Of Cyberattack?,"(September 28, 2015) available at https://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1455510&SctArtId=343857&from=CM&nsl_code=LIME&sourceObjectId=9348447&sourceRevId=2&fee_ind=N&exp_date=20250927-20:56:45.

[41] See, http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches.

[42] See, *In the Matter of AT&T Services, Inc.,* DA 15-399 (Order Adopted April 8, 2015) available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf.

[43] See, *In the Matter of Cox Communications, Inc.,* DA 15-1241 (Order Adopted November 5, 2015) available at https://www.huntonprivacyblog.com/files/2015/11/FCC.pdf.

[44] See, FCC Continues Aggressive Action on Data Breaches, Cooley Client Bulletin (April 2015) available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0ahUKEwiNl46FiZbKAhUI4D4KHfGQDUkQFghCMAY&url=https%3A%2F%2Fwww.cooley.com%2FPdfManager%2Fgetpublicationpdf.aspx%3Ftype%3Dalert%26show%3D71270&usg=AFQjCNGnEGM3xJKZIEKyj02F47p_mlLHjA&sig2=ybQzU7Ir7aeZZItTg3z7GQ.

[45] For example, the U.S. Department of Health and Human Services (HHS) has issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") under HIPAA. The Privacy Rule governs the use and disclosure of an individual's PHI by entities covered under HIPAA. The Privacy Rule also sets standards for an individual's right to understand and control how his or her PHI is used. It applies to health plans, healthcare clearinghouses, and to any healthcare provider who engages in electronic data interchange using one or more of the "standard transactions" as defined by HIPAA (collectively referred to as "covered entities"). The Privacy Rule includes a requirement that a covered entity mitigate, to the extent practicable, any harmful effect that is caused by an improper disclosure of PHI of which it becomes aware. Under the HITECH Act, discussed below, the Privacy Rule also applies directly to business associates of covered entities. 42 U.S.C. § 201 et seq. (HIPAA), 45 C.F.R. Part 160 and Subparts A and E of Part 164 (Privacy Rule). See also FTC Health Breach Notification Rule (16 C.F.R. Part 318) (August 18, 2009) (applying similar rules foreign and domestic vendors of PHR, PHR related entities and third-party service providers that maintain the information of U.S. citizens or residents). http://www.ftc.gov/healthbreach/.

[46] 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.

[47] For example, 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
- Reimbursement for any and all fraudulent activity the card association identifies as being tied to a security data breach.

In addition, when an organization suspects a PCI cyber-attack, the card brands' PCI Data Security Standards require hiring a PCI-approved forensic investigator (also known as a PFI) from a small list of card brand approved vendors. When a breach is suspected, a PFI is required to perform a specified list of investigative work including writing a final report that is issued to both the client and the various credit card companies, which is then used by the card brand companies to calculate potential fines that will be levied against the acquiring banks. These fees are then passed along to the victim company in the form of indemnification. Further, after a breach, a merchant's classification or "tier" may be adjusted upwards, resulting in the imposition of further obligations and potentially even greater fines and penalties should another breach occur. See also "PCI DSS and Incident Handling: What is required before, during and after an incident," SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/compliance/pci-dss-incident-handling-required-before-incident-33119 and "PCI Compliance Under Scrutiny Following Big Data Breaches," by Jen A. Miller at http://www.cio.com/article/2836035/data-breach/pci-compliance-under-scrutiny-following-big-data-breaches.html.

[48] 31 C.F.R. Part 578. These regulations are currently in abbreviated form and are limited to the boilerplate provisions contained in all other targeted sanctions programs. As such, there are currently still no program-specific definitions, interpretive guidance, or general licenses. However, experts expect OFAC to supplement the regulations in the near future, and define "cyber-enabled" activities to include "any act that is primarily accomplished through or facilitated by computers or other electronic devices." Interpretive guidance will likely explain "malicious cyber-enabled activities as "deliberate activities accomplished through unauthorized access to a computer system, including by remote access; circumventing one or more protection measures, including bypassing a firewall; or compromising the security of hardware or software in the supply chain." See "Boilerplate Cyber Sanctions Portend Coming Actions," (January 4, 2016) available at http://www.natlawreview.com/article/boilerplate-cyber-sanctions-regulations-portend-coming-actions#sthash.q858uF6s.dpuf; See also, New EU Data Protection and Cybersecurity Laws Finalized, Morgan Lewis Newsflash (December 23, 2015) available at http://www.morganlewis.com/pubs/new-eu-data-protection-and-cybersecurity-laws-finalised#sthash.uO7QX3nQ.dpuf; See also, *Guiding Principles for Cybersecurity Oversight*, by The Global Network of Director Institute (November 27, 2015) available at https://www.icd.ca/getmedia/4ff9c2d4-6e50-4834-97f1-fdb854e11ff1/GNDI_Cybersecurity_Final.pdf.aspx; See also, "Canadian Financial Regulatory Organization Releases Cybersecurity Guides," by Zach Warren, Legal Tech News (January 4, 2016), available at http://www.legaltechnews.com/id=1202746186200/Canadian-Financial-Regulatory-Organization-Releases-Cybersecurity-Guides?slreturn=20160005141814.

[49] U.S. Treasury OFAC FAQ, Available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx.

[50] 20 U.S.C. § 1232g; 34 CFR Part 99.

[51] Client Update: The Cybersecurity Information Sharing Act, by Debevoise and Plimpton (January 6, 2016) available at http://www.debevoise.com/~/media/files/insights/publications/2016/01/20160106a_the_cybersecurity_information_sharing_act.pdf.

[52] See "Cybersecurity Legislation Watch," ISACA available at http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx.

[53] Id.

[54] See e.g. the "Cybersecurity Disclosure Act of 2015," (available at https://www.congress.gov/bill/114th-congress/senate-bill/2410?q=%7B%22search%22%3A%5B%22transparency+the+oversight+cybersecurity%22%5D%7D&resultIndex=1). In an effort "to improve cybersecurity disclosures for investors and consumers in an age of persistent cybersecurity threats," U.S. Senators Jack Reed (D-RI) and Susan Collins (R-ME), introduced in December, the Cybersecurity Disclosure Act of 2015, which specifically promotes transparency in the oversight of cybersecurity risks at publicly traded companies. The bill is designed to ensure that public companies "provide a basic amount of information about the degree to which a firm is protecting the economic and financial interests of the firm from cyber attacks . . . by encouraging the disclosure of cybersecurity expertise, or lack thereof, on corporate boards at these companies." See, Reed, Collins Seek to Prioritize Cybersecurity at Public Companies Through SEC Disclosures (December 17, 2015) available at http://www.reed.senate.gov/news/releases/reed-collins-seek-to-prioritize-cybersecurity-at-public-companies-through-sec-disclosures. If ever enacted, this legislation would require companies to disclose – in their SEC public filings – whether they have a director who is a "cybersecurity expert" – and if not, why having this expertise on the board isn't necessary because of other cybersecurity steps taken by the company. Just like the early legislative and regulatory directives pertaining to audit committees, the Cybersecurity Disclosure Act of 2015 could be a harbinger to more forceful and imperious legislative and regulatory initiatives in the future. See also, "Republican Plots Course on Data Breach Bills," by Katie Bo Williams, The Hill (January 7, 2016) available at http://thehill.com/policy/cybersecurity/264979-neugebauer-plots-course-forward-on-data-breach-bill; Data Security and Breach Notification Legislation: Selected Legal Issues, by Alissa M. Dolan ,Congressional Research service (December 28, 2015) available at https://www.fas.org/sgp/crs/misc/R44326.pdf.

[55] "Ten Cybersecurity Concerns For Every Board of Directors," by John Reed Stark and David Fontaine (April 2015) available at http://www.cybersecuritydocket.com/2015/04/30/ten-cybersecurity-concerns-for-every-board-of-directors/.

[56] To complicate matters even further, cyber concerns for boards cross borders and are global in nature – mandating additional attention, expertise and oversight, and in addition to the federal and state regulations cited herein, many U.S. companies maintain subsidiaries, affiliates or employees in the European Union (E.U.). Such companies, whether public or private, must comply with relevant E.U. Member State data protection laws and guidelines where "personal data" (as defined by the pertinent law) is collected, processed or transferred by local operations. E.U. Member State data protection laws are based on E.U. Directive 95/46/EC, known as the "Data Protection Directive." And though each *Member State* is required to implement the Data Protection Directive, there is considerable variation across each Member States' interpretation and implementation. See http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm. The European Union is close to enacting a new global cybersecurity "Regulation" which will, among many other things, significantly increase the need for dedicated boardroom oversight of cybersecurity. On December 7, 2015, the European Union Council reached an informal agreement with the Parliament on an important network and information security "Regulation" affecting companies across the EU. The Regulation, together with a new Data Protection Directive that deals with the police and criminal justice sector and a new Network and Information Security Directive (the NIS Directive), would strengthen Europe's foundations on which to build its *Digital Single Market*. European Parliament is due to formally adopt these laws in early 2016. All businesses that offer goods or services in the EU (whether or not for a fee) or that monitor or track individuals within the EU will be subject to the Regulation. The benefit of international regulations rather than a directive is that one data protection law would apply across the EU instead of 28 different data protection laws implementing a directive (as is currently the case). Final

adoption of the regulations will have several important consequences for corporate cybersecurity, including the need for increased focus by boards of directors upon cybersecurity risk. See, "EU Reaches Agreement On New Data Protection Laws," Orrick Alert (December 16, 2015) available at https://www.orrick.com/Events-and-Publications/Pages/EU-Reaches-Agreement-On-New-Data-Protection-Laws.aspx; See also, "New EU Privacy Rules: Top Ten Highlights," by Mason Weiscz (December 17, 2015) available at http://blog.zwillgen.com/2015/12/17/new-eu-privacy-rules-top-10-highlights/#prettyPhoto.

[57] A recent trend in cyber-attacks is a level of anonymity that baffles even the most seasoned investigators, masking not only the identities of the perpetrators but their actual modus operandi as well. For example, so-called APT (Advanced Persistent Threat) 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 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. See e.g. Anatomy of an APT Attack: Step by Step Approach," by Ahiq Ja, InfoSec Institute (May 13, 2015) available at http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/; See also, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers," by Larry Grenemeier, Scientific American (July 11, 2011) available at http://www.scientificamerican.com/article/tracking-cyber-hackers/; See also, "Identifying cyber-criminals is No. 1 Challenge," by Andrew Conte, TribWire, (July 19, 2014) is available at http://triblive.com/news/editorspicks/6449644-74/hackers-bukh-criminals#axzz3wPHcXltG.

[58] "Navigating the Cybersecurity Storm: A Guide for Directors and Officers," by Paul Ferillo (December 1, 2015) available at http://www.weil.com/~/media/files/pdfs/navigatingcybersecuritystormbookfinal.pdf?cid=8590651901. The prospect of litigation is not just an academic consideration. With respect to the Target and Wyndham data breaches, for example, lawsuits were filed against the boards of each corporation for breach of fiduciary duty, and Institutional Shareholder Services Inc. (ISS) openly campaigned against members of Target's audit and corporate responsibility committees. See, "Top 10 Topics for Directors," by Akin Gump Strauss Hauer & Feld LLP, Metropolitan Corporate Counsel (January 27, 2015) available at http://www.metrocorpcounsel.com/articles/31395/top-10-topics-directors.

[59] The whistleblower provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act reward informants who provide actionable information with between 10 and 30 percent of any follow-up SEC recovery over $1,000,000. SEC Office of the Whistleblower FAQs, available at http://www.sec.gov/whistleblower. These provisions provide a particularly powerful incentive for whistle-blowers with information on potential regulatory violations, including lapses in cybersecurity. No financial firm is immune to the disgruntled employees, unhappy investors or portfolio companies, peeved competitors and the like who are now economically incentivized to report even baseless allegations to the SEC (and send them electronically and anonymously if they so choose). Similarly, though not offering any sort of reward, the Financial Industry Regulatory Association (FINRA) has also formed its own Office of the Whistleblower to expedite ''the review of high-risk tips by FINRA senior staff and ensure a rapid response for tips believed to have merit.'' Led by seasoned regulatory expert and FINRA veteran Cameron Funkhouser, FINRA's Office of the Whistleblower enables individuals with evidence of, or material information about, *any* potentially illegal or unethical activity (including cybersecurity breaches) to reach FINRA senior staff, who can quickly assess the level of risk involved and make sure that each tip is properly evaluated (or referred, if outside of their jurisdiction). FINRA, Office of the Whistleblower, https:// www.finra.org/Industry/Whistleblower/.