CYBERSECURITY REGULATION AND PRIVATE LITIGATION INVOLVING CORPORATIONS AND THEIR DIRECTORS AND OFFICERS

A Legal Perspective

Written By:

Perry E. Wallace,
Professor of Law and Director,
JD/MBA Dual Degree Program,
Washington College of Law,
American University

Richard J. Schroth, Ph.D,
Executive In Residence and Executive Director,
Kogod Cybersecurity Governance Center,
Kogod School of Business,
American University

William H. Delone, Ph.D,
Kogod Eminent Professor of Information Technology and Executive Director,
Kogod Cybersecurity Governance Center,
Kogod School of Business,
American University

KOGOD SCHOOL of BUSINESS

AMERICAN UNIVERSITY • WASHINGTON, DC

KOGOD CYBERSECURITY GOVERNANCE CENTER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The relentless growth of cybercrimes against corporations reigns as one of the great corporate governance challenges of our times. Our aim in this Legal Research Report is to encourage the largest number of corporate boards and individuals in governance roles to step up and devise and implement proper, effective corporate cybersecurity governance strategies.

Consequently, we analyze the relevant concepts, principles and issues in this area, ultimately laying out a concrete set of best practices, standards and guidelines in establishing and maintaining a high quality cybersecurity governance strategy. Because law and legal principles loom large in this overall story, we accord them a central position.

Here are the questions that we answer in this report:

1. What are the legal and economic risks and impacts for businesses that accompany cybercrime and other cyber threats? What similarities or differences exist, if any, in these risks and impacts as between public companies and private companies? What are the implications of these risks and impacts for private companies that are, or that anticipate being, funded by private equity or venture capital firms? As to both public and private companies, to what extent, and in what ways, should a company's legal counsel participate in the cybersecurity governance process?
2. What are the fundamental elements of the two broad categories of legal duties and standards identified above (those imposed on the corporation and those imposed on the directors and officers), and what are their underlying rationales?
3. How do these legal duties and standards apply to the world of cybersecurity governance, and what practical, useful implications do they carry for directors and officers seeking to fulfill their responsibilities for effective governance?
4. What state-of-the-art, "best practices" approaches and methods for proper cybersecurity governance should boards of directors and officers use to achieve—and even exceed--compliance with those legal duties and standards? What are the implications of this guidance for legal counsel?

Question 1

In Section II of the Paper, concerning "Legal and Economic Implications of Cybercrime and Other Cyber Threats," we delve into the following pertinent topics concerning legal and economic impacts of cybercrime and other cyber threats:

A. Risks and Impacts

In this part, we demonstrate why cybersecurity is important by spelling out the particularities of the risks and impacts of cyber threats, explaining that they are usually quite costly and thus are better managed and governed rather than simply tolerated. We use studies, reports and other materials to provide detailed information on who are the perpetrators, what do they want and how do they operate. In summary, they are as follows:

- **The Violators and Their Objectives**
    - Nation-states, spies who seek to steal our national security secrets or our intellectual property
    - Organized criminals who use sophisticated cyber tools to steal our identity and our money
    - Terrorists who want to attack our infrastructure, or
    - Hacktivists that are trying to make a social statement by stealing information and then publishing it to embarrass organizations

- **Their Methods**
    - Destruction of data or hardware as the world saw with the Saudi Aramco or the banks in South Korea
    - Denial of service of the types that our financial institutions suffered over a period of months
    - Ransomware where files are encrypted until ransom is paid
    - Theft where identity and money is stolen as we saw with the recent retail breaches.

We also discuss certain other risks and impacts that affect companies significantly. Generally speaking, these are consequences of the initial cyberattack:

- **Legal Liability** (government investigations and enforcement actions, as well as private litigation, based on the company's failure to prevent the attack, provide required timely notice of it, or otherwise provide proper cybersecurity governance);
- **Reputational Damage** (harm to the company's "brand," reputation, and good will due to negative perceptions about its competence and standards among the public and in the various relevant markets);
- **Negative Market Effects** (reductions in market share, sales, or stock valuation based on negative perceptions of the company's competence and standards);
- **Intellectual Property Loss** (diminution in value, and perhaps utility, of intellectual property assets because they have been made known to and distributed to improper sources); and
- **Regulatory Risk** (The risk that a change in laws and regulations will materially impact a security, business, sector or market, with accompanying costs and other impacts on competitiveness.)

B. Present and Future Government Compliance and Enforcement; Applicable Laws;

In this part we also elaborate on the subject of government investigation and enforcement about cybersecurity failures, citing numerous authoritative sources who promise that this activity will grow rapidly because of the nature of the threat. Here federal and state agencies and the laws under which they operate are set out and analyzed. Notably, we provide actual case summaries which illustrate much about the present and future regulatory landscape for cybersecurity. These cruelling processes consume time, money and other precious commodities such as employee morale and market standing.

C. Private Litigation;

Private litigation against companies, their directors and officers, or all of them, for failure to manage cyberattacks are prominent, frequent and extremely expensive. These lawsuits are sometimes launched independently of any other events. But very often they are initiated in the wake of some government action, whether or not successful. This "one-two punch" is particularly harmful to companies and, from an evidentiary perspective, poses special challenges.

Suits by external parties (consumers, third party vendors and the like) usually target the company directly and often are "class action" suits whose plaintiffs are "all persons similarly situated." The cost implications are obvious. Suits by internal parties (shareholders) are often "shareholder derivative lawsuits," which means the suit has been filed in behalf of the company. The target defendants are usually the directors or officers and the claims are typically for breach of fiduciary duty or other governance failures.

D. Private Companies, Private Equity and Venture Capital

In this part we deal with private companies, noting that, with certain prominent exceptions, private companies are subject to the same legal duties and "best practices" standards as large public companies. We also provide a picture of the impact that private equity and venture capital financing can have on obliging private companies to step up their standards relative to cybersecurity governance. Finally, we explain why legal, structural and economic constraints have a similar impact on private equity and venture capital firms.

E. A Note on the Role of Legal Counsel

Here we note the central role played in cybersecurity governance by legal counsel. This is a prelude to the presentation of "best practices" for legal counsel in Section V (C) of this Research Report.

Questions 2 and 3

In Section III, concerning "Legal Duties and Liabilities for Cybersecurity Governance Imposed Directly on the Board of Directors and Officers," we elaborate on certain corporate law concepts that govern standards of conduct and liability for officers and directors. We apply these concepts to cybersecurity governance. In corporate law, the fiduciary duty concept derives from the basic legal obligation of directors to manage and direct the business and affairs of the corporation. The concept also applies to officers and anyone else who is delegated authority by the board of directors. It commands to all these fiduciaries to act in this way:

> Carry out your assigned duties properly, in the corporation's and the shareholders' best interests, and if you do not do so, you may be sued by either the shareholders or a corporate representative and held personally liable for economic injuries that come to the corporation or the shareholders because of that failure of duty.

In fact, there are several fiduciary duties that guide the conduct of directors and officers, but the most pertinent ones for cybersecurity governance analysis are the fiduciary duty of care (FDC) and the fiduciary duty of oversight or monitoring (FDOM). Essentially, these duties mean what they say they mean in plain English, and while they would appear to set fairly strict, high standards, in reality they only require minimum good conduct. Only the most egregious conduct will cause liability. Nonetheless, these fiduciary duties are important, because when liability is assigned it is often considerable in the monetary sense. Further, even where directors and officers win in lawsuit, using defenses such as the business judgment rule (BJR), there may be serious reputational damage, employee morale problems and other problems that reduce sales and hurt the company's position in the various markets.

Director/Officer liability may also arise based on the plain language of a statute or rule. In this Research Report, we give the example of Section 11 of the Securities Act of 1933. Section 11 makes directors expressly liable for misrepresentations or omissions of "material" facts in registered public offerings.

In Section IV entitled "Legal Duties and Liabilities for Cybersecurity Governance Imposed Directly on the Corporation," we focus on instances of legal liability imposed directly on the business entity, perhaps a corporation, itself. We emphasize that the corporation is a "separate legal entity." It alone is the business. Hence, when there are violations of law, the business and not the directors and officers (who enjoy "limited liability") is legally liable. On the other hand, there are two well-known exceptions to this limited liability that can render directors, officers and others liable along with the corporation for the violation in question:

- **Direct or Active Participation**, in which a director or officer directly or actively participates in a violation of law (including by way of supervision) and is thus held individually liable along with the corporation; and

- **"Piercing the Corporate Veil,"** in which a court grants a plaintiff's request that the usual protection of limited liability (the corporate "veil" of protection) be ignored or set aside and that therefore individual directors, officers or shareholders be held liable along with the corporation. This is a rarely granted remedy, but it may be imposed when the corporate protections are abused and there has been a basic injustice done to a party outside the corporation (it doesn't apply to injuries to shareholders.)

Question 4

In Section V entitled "'Best Practices' Standards and Guidelines for Cybersecurity Governance," we present examples of the highest quality, gold standard approaches to cybersecurity governance. The examples are taken from the most prominent and respected systems being employed today:

- **National Institute of Standards and Technology (NIST) Voluntary Framework**
- **American Bar Association (ABA) Initiatives**
- **National Association of Corporate Directors (NACD) Principles**
- **FINRA Principles and Effective Practices**
- **U.S. Securities and Exchange Commission SEC Guidance**
- **U.S. Department of Justice Best Practices for Victim Response and Reporting of Cyber Incidents**

These best practices should be key reference points in designing and implementing a high-quality cybersecurity governance program. We also proceed to give some common-sense advice about setting up or improving such a program. Finally we provide advice to legal counsel on how to best represent companies with cybersecurity challenges (which means all of them).

INTRODUCTION

The rapid and constant growth of cybercrimes and other cyber incidents affecting the corporate sector currently reigns as one of the great corporate governance challenges of the times. Accordingly, now that enlightened observers properly view this great menace as much more than simply an IT (information technology) problem, increasing numbers of corporate boards and managements are stepping up to devise and implement appropriate corporate governance strategies to address it. Regretfully, however, too many other directors and managers are content to live in various states of unsupported beliefs that (a) the problem is nonexistent or de minimis in importance, (b) their companies will not be significantly affected or (c) the problem will somehow go away.

In this Research Report, we analyze the relevant concepts, principles and issues in this area, ultimately laying out a concrete set of "best practices" standards and guidelines that should be helpful in establishing and maintaining a high quality cybersecurity governance strategy. Further, because law and legal principles loom large in this overall story, we accord them a central position.

In this Research Report, we answer the following questions relative to the areas of law referred to above:

1. What are the legal and economic risks and impacts for businesses that accompany cybercrime and other cyber threats? What similarities or differences exist, if any, in these risks and impacts between publicly held companies and privately held companies? What are the implications of these risks and impacts for private companies that are, or that anticipate being, funded by private equity or venture capital firms? As to both public and private companies, to what extent, and in what ways, should a company's legal counsel participate in the cybersecurity governance process?
2. What are the fundamental elements of the two broad categories of legal duties and standards identified above (those imposed on the corporation and those imposed on the directors and officers), and what are their underlying rationales?
3. How do these legal duties and standards apply to the world of cybersecurity governance, and what practical, useful implications do they carry for directors and officers seeking to fulfill their responsibilities for effective governance?
4. What state-of-the-art, "best practices" approaches and methods for proper cybersecurity governance should boards of directors and officers use to achieve—and even exceed—compliance with those legal duties and standards? What are the implications of this guidance for legal counsel?

Note that the specific legal context chosen for the Research Report is the matrix of U.S. state and federal laws, which means that this publication is most directly applicable to U.S. and foreign companies that come within the jurisdictional reach of those laws by virtue of their "business presence" in the U.S. At the same time, however, the observations and discussions found in the report certainly have a broad general applicability and thus a global reach. This is case given that (1) this guidance most often concerns itself with the adoption by companies of "best practice" standards that often exceed those imposed by law, and (2) where the guidance exclusively concerns legal standards or legal analysis, we observe that, as a general matter, the U. S. legal system has been a major point of reference, and even a model, for other legal systems around the world.[1]

Finally, we caution that this publication does not purport to be, nor should it be taken as, actual, specific legal advice or counsel. Readers are urged to consult with their own legal counsel when dealing with particular legal issues that might arise in the conduct of their business operations or that they may identify after reviewing this Research Report.

LEGAL AND ECONOMIC IMPLICATIONS OF CYBERCRIME AND OTHER CYBER THREATS

- Risks and Impacts
- Present and Future Government Compliance and Enforcement
- Applicable Laws
- Private Litigation
- Private Companies
- Private Equity and Venture Capital
- A Note on the Role of Legal Counsel

A. Risks and Impacts from Cybercrime and Other Cyber Threats

1. General Picture: Why is Cybersecurity Governance Important? Who are the Violators? What Do They Want? What Methods Do They Use?

Why is Cybersecurity Governance Important?

As noted in the introduction, public awareness and concern about cybercrime and other cyber threats are growing virtually daily as a result of numerous high-profile data security breaches at large retail companies and other cyber incidents. Moreover, concerns that these problems reflect a rapidly expanding trend have been fully and expertly verified in numerous professional reports and studies. For example, the well-known Verizon Risk Team produces an annual *Data Breach Investigations Report*, which contains extensive analyses of relevant cybercrime and other cyber risks and which seeks to encourage greater use of enterprise risk management and to "improve awareness and practice in the field of information security and support critical decisions and operations from the trenches to the boardroom."[2]

Other prominent studies merit our attention. For example, in a 2015 report on the cost of cybercrime by the Ponemon Institute, entitled *2015 Cost of Data Breach Study: United States*[3] (Ponemon Report), in the case of U. S. companies, researchers found that "[t]he average cost for each lost or stolen record containing sensitive and confidential information increased from $201[the previous year] to $217. The total average cost paid by organizations increased from $5.9 million [the previous year] to $6.5 million."[4] Further, the Ponemon Report reached the following critical conclusions:

- Data breach costs are at an all-time high;
- The total average organizational cost of data breach increased in 2015;
- Measures reveal why the cost of data breach increased;
- Certain industries have higher data breach costs;
- Malicious or criminal attacks continue to be the primary cause of data breach;
- Malicious attacks are most costly;
- Certain factors decrease the cost of data breach;
- The more records lost, the higher the cost of data breach;
- The more churn (loss of existing customers), the higher the per capita cost of data breach;

- Certain industries were more vulnerable to churn;
- Detection and escalation costs are at a record high;
- Notification costs increased slightly;
- Post data breach costs increased.[5]

Against this general background, it is no surprise that corporate leaders are now truly concerned about this problem. In a 2014 survey of nearly 500 company directors and general counsel, "data security" was the top area of governance that "keeps [directors] up at night," and it was the second most important area for in-house counsel, after regulatory compliance. Relatedly, corporate law departments ranked cybersecurity as a "high concern," both company-wide and within the law department.[6]

Who are the violators? What do they want? What methods do they use?

Proper cybersecurity governance requires a full and clear understanding of who is perpetrating acts of cybercrime and other injurious cyber incidents, why they engage in such acts and what methods they use. At a March 26, 2014 roundtable on cybersecurity sponsored by the SEC, one commentator, viewing the challenge globally and including all sectors of society, offered the following answers:

- **The Violators and their Objectives**
    - Nation-states—spies who seek to steal our national security secrets or our intellectual property
    - Organized criminals who use sophisticated cyber tools to steal our identity and our money
    - Terrorists who want to attack our infrastructure, or
    - Hacktivists that are trying to make a social statement by stealing information and then publishing it to embarrass organizations
- **Their Methods**
    - Destruction of data or hardware as the world saw with the Saudi Aramco or the banks in South Korea
    - Denial of service of the types that financial institutions suffered over a period of months
    - Ransomware where files are encrypted until ransom is paid
    - Theft where identity and money is stolen as we saw with the recent retail breaches.[7]

Yet another description of the objectives of the bad acts done in these situations, ones of particular concern to business and described in terms of asset loss, has been cited by the National Association of Corporate Directors (NACD), which has identified the following asset-loss categories:

- Business plans, including merger or acquisition strategies, bids and the like;
- Trading algorithms;
- Contracts with customers, suppliers, distributors, joint venture partners, and the like;
- Employee log-in credentials;
- Information about company facilities, including plant and equipment designs, maps, and future plans;
- Product designs;
- Information about key business processes;
- Source codes;
- Lists of employees, customers, contractors, and suppliers; and
- Client data.[8]

2. Other Risks and Impacts: Legal Liability; Reputational Damage; Negative Financial Market Effects; Intellectual Property Loss, and "Regulatory Risk"

The risks and impacts discussed above have aroused great concern because they carry both legal and economic significance to business operations. SEC Commissioner Luis A. Aguilar has provided a useful guide to many of the specific legal and economic risks that the modern world of cyber risks poses:

> In addition to becoming more frequent, there are reports indicating that cyber-attacks have become increasingly costly to companies that are attacked. According to one 2013 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009. In addition, the aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an attack. Beyond the unacceptable damage to consumers, these secondary effects include reputational harm that significantly affects a company's bottom line. In sum, the capital markets and their critical participants, including public companies, are under a continuous and serious threat of cyber-attack, and this threat cannot be ignored.
>
> As an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors…
>
> The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks…
>
> In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats. Perhaps unsurprisingly, there has recently been a series of derivative lawsuits brought against companies and their officers and directors relating to data breaches resulting from cyber-attacks.[9]

Intellectual property loss or impairment as a result of cyber incidents deserves special mention. Perhaps the most emphatic and insightful expression of its importance comes from the website of the U. S. Department of Justice's Computer Crime and Intellectual Property Section (CCIPS):

> [CCIPS's] enforcement responsibilities against intellectual property crimes are … multi-faceted. Intellectual Property (IP) has become one of the principal U.S. economic engines, and the nation is a target of choice for thieves of material protected by copyright, trademark, or trade-secret designation.[10]

The fact that a major criminal enforcement organ of the federal government places such a high priority on protecting the intellectual property of U.S. companies speaks volumes about the key position of these special assets in the economy and their value to their owners.

A final concern that directors and officers must take into account in managing the corporation is "regulatory risk." This concept has been defined as follows:

> The risk that a change in laws and regulations will materially impact a security, business, sector or market. A change in laws or regulations made by the government or a regulatory body can increase the costs of operating a business, reduce the attractiveness of investment and/or change the competitive landscape … For example,

> utilities face a significant amount of regulation in the way they operate, including the quality of infrastructure and the amount that can be charged to customers. For this reason, these companies face regulatory risk that can arise from events - such as a change in the fees they can charge - that may make operating the business more difficult.[11]

The present period is one where the regulatory risk involving cybersecurity must be characterized as "high." This is because we have a major, growing problem that looms large in society, having the potential to cause great harm to individuals, organizations and the society itself. Nevertheless, there is at present no comprehensive regulatory scheme in place, only piecemeal measures whose effectiveness may be acceptable in the present but certainly will not be in the very near future. Simply stated, this is a time for the exercise of vision by corporate directors and other leaders.

The following section concerns "Government Investigations and Enforcement: Applicable Laws." Note that the top-level government officials cited predict that the government will move to increase regulation and enforcement in the areas of cybercrime and other cyber threats.

B. Government Enforcement Actions; Applicable Laws

A number of federal and state government agencies have been—and will in the future be—conducting cybersecurity-related enforcement investigations of targeted business enterprises. The following observations by a noted expert on government investigations are revealing:

> In another emerging area of white-collar criminal enforcement, U.S. Attorney Bharara has publicly emphasized the Southern District of New York's focus on cybercrime ... In tandem with this increased focus on cybercrime, corporations also can expect increased focus by regulators on cybersecurity. U.S. Attorney Bhara, for instance, has emphasized the importance of prompt disclosure if a corporation has reason to believe customer information has been compromised, and has urged that every company needs to do a better job of creating and fostering a culture of security.[12]

The discussions below highlight prominent examples of the subjects, the legal grounds, and the strategies employed by these governmental, and there is commentary in most instances about their future directions. These discussions also provide insights into what activities, both preventative and responsive, should be the focus of companies that could potentially become subjects of similar governmental action.

1. U.S. Federal Trade Commission

Background

The Federal Trade Commission (FTC) describes its work as follows:

> The FTC is a bipartisan federal agency with a unique dual mission to protect consumers and promote competition. For one hundred years, our collegial and consensus-driven agency has championed the interests of American consumers. As we begin our second century, the FTC is dedicated to advancing consumer interests while encouraging innovation and competition in our dynamic economy.[13]

Cybersecurity: Legal Framework

The FTC is not the only agency with jurisdiction over cybersecurity matters, but its jurisdiction is the broadest. The FTC's cybersecurity activities focus on the areas of "privacy" and "data security," and it has authority under a number of federal laws to conduct investigations and enforcement actions, including:

- The Federal Trade Commission (FTC) Act (prohibits unfair and deceptive trade practices in or affecting commerce);[14]
- The Fair Credit Reporting Act (protects the privacy and accuracy of sensitive consumer report information);[15]

- The Gramm-Leach-Bliley Act (mandates privacy and security requirements for non-bank financial institutions);[16]
- The Children's Online Privacy Protection Act;[17]
- The CAN-SPAM Act;[18] and
- The Telemarketing and Consumer Fraud and Abuse Prevention Act.[19]

Cybersecurity Compliance and Enforcement

Using one or more of these legal authorities, the FTC has vigorously pursued a number of investigations and enforcement actions under three categories: (1) big data, (2) mobile technologies and (3) securing sensitive data. Here are some representative cases:

- Big Data
  - *TeleCheck* and *Certegy* Complaints alleged that these businesses failed to have appropriate procedures in place to maintain the accuracy of consumer data and correct errors, which could result in consumers being denied the ability to use checks to make payments.[20]
  - *TRENDnet* Complaint alleged that the company failed to provide reasonable security for IP cameras used for home security and baby monitoring, resulting in hackers being able to post private video feeds of people's bedrooms and children's rooms on the Internet
- Mobile Technologies
  - *Apple, Amazon*, and *Google* Complaints related to kids' in-app purchases[21]
- Securing Sensitive Data
  - *PaymentsMD* Complaint against a health billing company for allegedly deceptive practices related to its online patient portal. The company offered the portal to consumers as a way for them to view their billing history with various medical providers. Complaint alleged that the company used a deceptive sign-up process—including hidden disclosures and confusing check boxes—to trick consumers into giving their permission to gather sensitive health data from pharmacies, medical testing companies, and insurance companies to create a patient health report.[22]
  - *Microsoft, TJX, Lifelock, CVS, RiteAid, BJ's,* and *Wyndham* Complaints allege that these and other companies failed to implement reasonable security protections, involving not just consumers' financial data, but health information, account IDs and passwords, and other sensitive data.)[23]
  - *Yelp* (mobile app) and *TinyCo* (gaming app) (Complaints filed under the Children's Online Privacy Protection Act, which requires notice and consent to parents before information is collected from kids under 13.[24]

The FTC will continue to focus on these areas in the future, according to "FTC's Privacy and Data Security Priorities for 2015."[25]

2. U.S. Securities and Exchange Commission

Background

The federal securities laws regulate "securities" (financial market instruments such as stocks, bonds, and options) and securities transactions. In passing those laws, Congress and the President determined that there needed to be "full and fair disclosure" of all "material" information regarding securities, in the interests of:

- Investor Protection
- Stock Market Integrity
- Efficient Administration of Stock-Market-Related Transactions[26]

In pursuit of these objectives, Congress enacted, and subsequently amended, several federal

securities laws, and the U. S. Securities and Exchange Commission (SEC) issued an extensive framework of rules and regulations to provide for implementation of those laws. The following non-exclusive list of statutes lies at the core of SEC regulation; they are also pertinent to its regulatory activities in the cybersecurity area:

- Securities Act of 1933[27] (requires that investors receive financial and other significant information concerning securities being offered for public sale; and prohibits deceit, misrepresentations, and other fraud in the sale of securities);
- Securities Exchange Act of 1934[28] (created the Securities and Exchange Commission; empowers the SEC with broad authority over all aspects of the securities industry);
- Trust Indenture Act of 1939[29] (regulates certain aspects of sales of debt securities such as bonds, debentures, and notes that are offered for public sale);
- Investment Company Act of 1940[30] (regulates the organization of companies, including mutual funds, that engage primarily in investing, reinvesting, and trading in securities, and whose own securities are offered to the investing public);
- Investment Advisers Act of 1940[31] (regulates investment advisers).

Cybersecurity: CF Disclosure Guidance and Relevant Regulations

The SEC has been interested in cybersecurity governance for a number of years, but it has substantially increased its compliance and enforcement activities in keeping with the vastly increased need for such a regulatory enhancement. In that regard, the agency has issued several key initiatives in the area. Here are the major ones:

- **CF Disclosure Guidance: Topic No. 2.32 (SEC Guidance)** Although the SEC Guidance does not have the legally binding effect of a statute or a rule or regulation, and it neither creates any new duties nor elevates the level of any existing ones, it is nonetheless very important. This is true because it both (1) signals that the SEC considers cybersecurity to be a priority and (2) identifies relevant areas in documents filed with the SEC that particularly deserve sensitivity to cybersecurity disclosure. The disclosure areas, which appear in most SEC disclosure forms, are listed in the SEC Guidance because disclosure in these areas is highly relevant to the agency's cybersecurity goals.

- **Cybersecurity Examination Initiative.**
  - As a follow-up to the issuance of this guidance, the SEC staff in the Division of Corporation Finance began a review of the level and quality of public company disclosures of cybersecurity practices and risks. This review included "Comment" letters to 50 public companies of various sizes and from a wide variety of industries. Note that the receipt by a company of such a letter from SEC staff providing specific comments about that particular company's disclosure practices is a "high alert" event. Well-informed companies (including those that become informed about the comments) tend to "get the message" that the SEC is seeking high quality disclosure in the areas identified in the letter.
- **Regulation S-P**
  - Regulation S-P[33] contains the privacy rules promulgated by the SEC under Section 504 of the Gramm-Leach-Blilely Act (Act).[34] Section 504 requires the SEC and other federal agencies to adopt rules implementing notice requirements and restrictions on a financial institution's rights to disclose non-public personal information about consumers.[35] While the scope of the regulation is much broader than the world of cyber threats and other incidents, it has been in place longer

that other, more specific, measures, and it has provided a suitable basis for enforcement activity in the cybersecurity area.

- Rule 30(a) of Regulation S-P is known as the "Safeguard Rule." It requires that: "Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." Such policies and procedures must be reasonably designed to: "(a) Insure the security and confidentiality of customer records and information; (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[36]

- **Regulation Systems Compliance and Integrity (Regulation SCI)**

  - The SEC adopted Regulation SCI[37] on November 19, 2014, in order to establish uniform requirements relating to the automated systems of market participants and utilities.

  - The term "SCI entities" refers to certain self-regulatory organizations (SROs); plan processors; clearing agencies; and alternative trading systems (ATSs) that exceed volume thresholds.

  - Regulation SCI requires SCI entities to establish written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and that they operate in a manner that complies with the Securities Exchange Act. It also requires that SCI entities mandate participation by designated members or participants in scheduled testing of their business continuity and disaster recovery plans. SCI entities will have to take corrective action upon the occurrence of "SCI events" (defined to include systems disruptions, systems compliance issues, and systems intrusions), and notify the SEC of such events. With certain exceptions, firms subject to these rules must comply with the requirements by November 3, 2015.[38]

- **Regulation S-ID**

  - Regulation S-ID,[39] the "Identity Theft Red Flag Rules," was jointly issued by the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) to require certain regulated entities to establish programs targeting the risks of identity theft. These rules and guidelines implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which amended section 615(e) of the Fair Credit Reporting Act and mandated that the two agencies adopt rules requiring regulated entities that are subject to the agencies' respective enforcement authorities to address the area of identity theft. For the SEC, the regulated entities covered are essentially brokers or dealers (broker-dealers), investment companies, and investment advisers registered under the Securities Exchange Act.

  - The rules require financial institutions and creditors to develop and implement a written identity theft prevention program designed

to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts. The rules include guidelines to assist entities in the formulation and maintenance of programs that would satisfy the requirements of the rules. The rules also establish special requirements for credit and debit card issuers.

- Notably, the prevention program requires the involvement of the board of directors (or committee thereof) or a designated senior manager in the approval, oversight, development, implementation and administration of the program.

Cybersecurity Compliance and Enforcement

Based on the SEC Guidance and the rules and regulations described above, the SEC has launched various cyber-related enforcement actions. The following are examples of these efforts.

- In an action brought under Regulation S-P, *In the Matter of LPL Financial Corporation*[40] (LPL), the SEC targeted a registered broker-dealer and investment adviser, claiming that it "had insufficient security controls to safeguard customer information at its branch offices, LPL failed to implement adequate controls, including some security measures, which left customer information at LPL's branch offices vulnerable to unauthorized access." According to the SEC, the deficiencies allowed hackers to make unauthorized trades in various customer accounts. In fact, LPL had acted promptly in reversing or eliminating the trading positions and had compensated the customers for the trading losses of approximately $98,900. Nonetheless, the SEC still chose to censure the firm, fine it $275,000, and require it to retain and pay for an independent consultant. LPL was required to implement the results of the independent consultant's review, report and recommendations concerning that firm's policies and procedures.[41]
- *In the Matter of Next Financial Group, Inc*.[42] ("NEXT") was a proceeding initiated by the SEC claiming that NEXT, a registered broker and dealer, willfully violated Regulation S-P by "disclosing nonpublic personal information about its customers to nonaffiliated third parties without notice or a reasonable opportunity to opt out of such disclosure; by allowing registered representatives to disseminate customer nonpublic personal information to other brokerage firms when leaving NEXT; and by failing to safeguard customer records and information."[43]
- *In the Matter of Marc A. Ellis*[44] was an SEC administrative proceeding that arose out of violations by GunnAllen Financial, Inc. (GunnAllen), formerly a Tampa, Florida-based broker-dealer, of the Safeguard Rule."). Although GunnAllen maintained written supervisory procedures for safeguarding customer information, they were inadequate and failed to instruct the firm's supervisors and registered representatives how to comply with the Safeguard Rule. Marc A. Ellis, Chief Compliance Officer (CCO) of the firm, a was therefore charged with the responsibility for maintaining and reviewing the adequacy of GunnAllen's procedures for protecting customer information. After the theft of three laptop computers and a registered representative's computer password credentials put customer information collected by GunnAllen at risk of unauthorized access and use, Ellis did not direct the firm to revise nor supplement its policies and procedures for safeguarding customer information. Note that in this case, the SEC not only took enforcement action against the firm itself (GunnAllen), but it also targeted an individual (aiding and abetting), a responsible firm official, for punishment.
- In *In the Matter of Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network*[45] (Commonwealth), the SEC instituted an action claiming violations by Commonwealth, a registered broker-dealer and investment adviser, of the Safeguards Rule. The SEC alleged that at all relevant times, Commonwealth recommended—

but did not require—that its registered representatives maintain antivirus software on their computers, which the registered representatives used to access customer account information on the firm's intranet and trading platform. In addition, Commonwealth did not have procedures in place to adequately monitor and review its registered representatives' computer security measures and their implementation. In November 2008, through the use of a computer virus, an unauthorized party obtained the log-in credentials of a Commonwealth registered representative, accessed Commonwealth's intranet, and entered unauthorized purchase orders from eight customer accounts, all because of the firm's failure to properly protect customer account information. In settlement of the action, Commonwealth paid a penalty of $100,000 and agreed to cease and desist from committing or causing future violations of the Safeguards Rule.[46]

- *Financial Fraud; Insider Trading Based on "Market-Moving" Information.*
    - A cybersecurity firm, FireEye Inc., (FireEye) conducted research, the results of which were reportedly presented to the SEC and the U.S. Secret Service, on what appears to be an extensive program of cyber-related financial fraud. News reports quote credible sources stating that the two agencies have begun major investigations.[47] Such an unusual, new type of enforcement initiative by the SEC, to the extent the news accounts are true, would be insightful about the future directions and the ever-widening scope of that agency's cyber-related activities. According to a report prepared by FireEye on the matter:
    - "FireEye is currently tracking a group that targets the email accounts of individuals privy to the most confidential information of more than 100 companies. The group, which we call FIN4, appears to have a deep familiarity with business deals and corporate communications, and their effects on financial markets. Operating since at least mid-2013, FIN4 distinctly focuses on compromising the accounts of individuals who possess non-public information about merger and acquisition (M&A) deals and major market-moving announcements, particularly in the healthcare and pharmaceutical industries [luring employees into giving up email passwords, known as "spear phishing" or "credential harvesting"].[48]

Finally, as for future directions at the SEC in general, it appears that the agency's efforts will be both intensified and expanded. SEC Chair Mary Jo White herself underscored this at a March 26, 2014 "Cybersecurity Roundtable" wherein she stated that "[t]his is a global threat. Cyber threats are of extraordinary and long-term seriousness."[49]

3. FINRA

Background

The Financial Industry Regulatory Authority, Inc. (FINRA) is a private, non-governmental corporation that assists the SEC in regulating member brokerage firms and exchange markets. By law, specifically under Section 6 of the Securities Exchange Act of 1934, FINRA is classified as a self-regulatory organization (SRO), and the SEC is the government agency with ultimate regulatory authority over it. Thus, it is not a government agency, but it is a regulator. This SRO is the successor to the National Association of Securities Dealers, Inc. (NASD) and the member regulation, enforcement and arbitration operations of the New York Stock Exchange.[50]

Cybersecurity Compliance and Enforcement

FINRA has for some time expressed interest and concern about cybersecurity. Here are some prominent examples:

- **Regulatory and Examination Priorities Letter**

- One example of this engagement has been the regular treatment of the subject in the organization's Regulatory and Examination Priorities Letter since 2007.

- **On-Site Firm Reviews**
    - Also, in 2010 and 2011, FINRA conducted on-site reviews of firms of varying sizes and business models to determine and assess the means by which registered firms control critical information technology and cyber risks.

- **Survey of Firms**
    - Another important activity in this same vein was the June 2001 FINRA survey of 224 firms (Survey), which sought to shed light on relevant industry information technology and cybersecurity practices and issues that may affect investor protection and market integrity.[51]

- **Targeted Examinations**
    - The 2014 "Targeted Examination" (Sweep) focused on the types of threats that firms face, areas of vulnerabilities in their systems and firms' approaches to managing these threats. In this examination, FINRA sent an information request to a crosssection of firms, including large investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers.

- **Report on Cybersecurity Practices**
    - In 2015, FINRA published a "Report on Cybersecurity Practices," (FINRA Report), which drew upon a variety of sources, "including the 2014 sweep, interviews with other organizations involved in cybersecurity, previous FINRA work on cybersecurity and publicly available information." The FINRA Report identified and discussed certain specific topics that should be used by firms in formulating their individualized cybersecurity programs:
        - cybersecurity governance and risk management;
        - cybersecurity risk assessment;
        - technical controls;
        - incident response planning;
        - vendor management;
        - staff training;
        - cyber intelligence and information sharing; and
        - cyber insurance.[52]

These specific topics, it should be noted, are the sub-categories that provided the basis for the development of the FINRA Cybersecurity "Principles and Effective Practices" that are discussed and analyzed in the FINRA Report and summarized in Section V (A) of this Research Report.

Note that, rather than covering all cybersecurity topics or providing exhaustive guidance on each cybersecurity issue discussed, the FINRA Report encourages firms to take a "risk management-based approach" to cybersecurity. The following formulation of the term was developed by the National Institute of Standards and Technology (NIST):

> Risk management is the process of identifying, assessing, and responding to risk. Particularly within critical infrastructure, organizations should understand the likelihood that a risk event will occur and the resulting impact. With this information, organizations determine the acceptable level of risk for IT and ICS assets and systems, expressed as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize systems that require attention. This will enable organizations to optimize cybersecurity expenditures. Furthermore, the implementation of risk management programs offers organizations the ability to quantify and communicate changes to organizational cybersecurity. Risk is also a common language that can be communicated to internal and external stakeholders.[53]

Against this background of investigation, evaluation and assessment, FINRA has proceeded with various enforcement matters. The following cases, presented by FINRA as a "Case Study," are reproduced verbatim from the FINRA Report. They are illustrative of present and likely future enforcement scenarios.

- **Case Study I**
  In one instance where FINRA took enforcement action, an online firm opened four accounts for higher-risk foreign customers who engaged in a pattern of fraudulent trading through the firm's Direct Market Access (DMA) platform. These customers hacked into accounts held at other online broker-dealers where they engaged in a short-sale transaction scheme that facilitated the customers' large profits in their original firm accounts and losses in the outside, compromised accounts at the unsuspecting broker-dealers. This firm violated FINRA Rule 3310(a) and (b) and FINRA Rule 2010 by: a) failing to establish and implement anti-money laundering (AML) policies and procedures adequately tailored to the firm's online business in order to detect and cause the reporting of suspicious activity; and b) failing to establish and implement a reasonably designed customer identification program to adequately verify customer identity.

- **Case Study II**
  In a similar instance FINRA took enforcement action at a firm that opened accounts for a foreign customer from a jurisdiction known for heightened money-laundering risk. In addition to the FINRA case, the SEC, among other entities, later filed a complaint against this customer. The SEC alleged that the customer created an international "pump-and-dump" scheme where shares in thinly traded companies were bought. Then, the customer hacked into accounts at other broker-dealers and liquidated the existing equity positions in those accounts. With the resulting proceeds, the customer bought and sold thousands, and in one case, millions, of shares of the same thinly traded stocks in the original accounts. The unauthorized trading in the hacked accounts pumped up the price of the stocks for the customer, who realized the profits in the accounts at the original firm. The FINRA investigation found this firm failed to establish and implement AML policies and procedures adequately tailored to verify the identity of the firm's higher-risk foreign customer base in order to detect and cause the reporting of suspicious activity.[54]

4. U.S. Department of Justice

Background and Legal Framework

The Department of Justice (DOJ) "Mission Statement" reads as follows:

> To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.[55]

The Judiciary Act of 1789[56] created the Office of the Attorney General as a one-person office, with an Attorney General whose duty was "to prosecute and conduct all suits in the Supreme Court in which the United States shall be concerned, and to give his advice and opinion upon questions of law when required by the President of the United States, or when requested by the heads of any of the departments, touching any matters that may concern their departments."[57] In 1870 Congress passed the Act to Establish the Department of Justice,[58] establishing "an executive department of the government of the United States" with the Attorney General as its head. The Act delegated to DOJ control over all criminal prosecutions and civil suits in which the United States had an interest. Additionally, the 1870 Act gave the Attorney General and the Department control over federal law enforcement.[59] The 1870 Act is the foundation upon which the Department of Justice still rests.

Cybercrime; DOJ Organizational Framework and Mission

The "Computer Crime and Intellectual Property Section" (CCIP S) of the U. S. Department of Justice (DOJ) Criminal Division is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. It is a major objective of CCIPS to *prevent, investigate, and prosecute computer crimes* by working with other government agencies (including the Federal Bureau of Investigation (FBI) and the U.S. Secret Service of the U.S. Department of Homeland Security (DHS)), the private sector, academic institutions, and foreign counterparts.

Cybercrime Legal Framework

CCIPS enforcement activities rely mostly on the following legal authorities as a basis for its prosecutions of cybercrime. They are as follows:

- The Computer Fraud and Abuse Act,[60] which is often referred to as the "hacking statute;"
- Statutes which regulate electronic surveillance and are implicated in all varieties of cybersecurity monitoring and intrusions detection technologies, such as the Electronic Communications Privacy Act,[61] the Wiretap Act[62] and the Pen Trap statute;[63] and
- The evolving constitutional, statutory and jurisprudential framework broadly relating to the collection and use of electronic evidence.

The Justice Department also issued a set of "Best Practices for Victim Response and Reporting of Cyber Incidents." These are summarized and commented on in Section V (A) of this Research Report, which addresses the subject of best practices in cybersecurity governance.

Cybercrime Compliance and Enforcement

The CICPS Section has successfully challenged cybercrime activities in a number of critical cases. The following cases are representative:

- Member of Hacking Group Sentenced to 3 Years in Prison for Intrusions into Corporate and Governmental Computer Systems (April 16, 2015)
- Member of Organized Cybercrime Ring Sentenced to 150 Months in Prison for Selling Stolen and Counterfeit Credit Cards (April 9, 2015)
- Sprint Communications, Inc. Agrees To Pay $15.5 Million To Resolve Allegations Of Overcharging Law Enforcement Agencies For Court-Ordered Wiretaps (April 9, 2015)
- Suspended North Side Pharmacist Pleads Guilty To Trafficking Counterfeit Viagra (April 2, 2015)
- Four Charged in International Uganda-Based Cyber Counterfeiting Scheme (April 2, 2015)
- New Orleans Man Pleads Guilty to Selling Counterfeit Movie DVDs and Music CDs (April 2, 2015)
- Fourth Member of International Computer Hacking Ring Pleads Guilty to Hacking and Intellectual Property Theft Conspiracy (April 1, 2015)
- Counterfeit DVD Trafficker Sentenced (March 31, 2015)
- Computer Analyst Sentenced To Three Years In Prison For Stealing Trade Secrets From Citadel And Previous Employer (January 15, 2015) 64

As to future directions, Assistant Attorney General Leslie R. Caldwell provided insights into what types of initiatives will be the focus of CICPS in a presentation at Georgetown University on May 20, 2015:

> Last summer— under the leadership of the Department of Justice—U.S. law enforcement, foreign partners in more than 10 countries and numerous private-sector partners worked closely to disrupt the Gameover Zeus botnet and Cryptolocker ransomware scheme.
>
> In Gameover Zeus, we faced an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. Unknown to their rightful owners, the infected computers also secretly became part of a global network of compromised computers, known as a botnet...

> The Gameover Zeus botnet was a global network of somewhere between 500,000 and one million infected victim computers which were used to steal millions of dollars from businesses and consumers. It was also a common distribution mechanism for Cryptolocker—a form of malicious software that would encrypt the files on victims' computers until they paid a ransom. Security researchers estimate that, as of April 2014, Cryptolocker had infected more than 234,000 computers…
>
> In any event, the sort of collaboration that we achieved in the Gameover Zeus operation was not an aberration. It is the new normal…
>
> But we also want to help you. Last December, at the Legal Symposium on cybercrime on this campus, I announced that the department was taking the fight against cybercrime in a new direction. I announced the Criminal Division's plan to work more closely with the private sector and federal agencies to address cybersecurity challenges. We created a hub for the Division's cybersecurity work, which is the new Cybersecurity Unit in CCIPS … In creating the Unit, we hope to use the lessons that CCIPS has learned and the skills that its prosecutors have gained from investigating and disrupting cybercrime to create actionable guidance and to support public- and private-sector cybersecurity efforts.[65]

5. State Laws and State Attorneys General

State Laws

At the state law level, depending on the particular state, laws have been enacted and enforcement efforts are taking place reflecting that many state government officials have a real understanding of the major problem posed by today's cyber risks. But there is no great national uniformity in the laws or the initiatives of state officials. Therefore, this legal patchwork is a moving target that directors should watch carefully for trends and future developments. In this regard, the following quote on the present status of active state security breach laws from the National Conference of State Legislatures (NCSL) website is directly on point:

> 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 personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, driver's 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). National Conference of State Legislatures list:[66]

After listing the specific laws, the NCSL goes on to note that, at the time of the writing, only Alabama, New Mexico and South Dakota have no security breach laws.[67]

One development in the state privacy law area that deserves comment concerns the California Online Privacy Protection Act.[68] (COPPA) Over the years, California has often led the way" in new policy and program areas.[69] In the instance of COPPA, the "laboratory" state has enacted a landmark statute that, as amended, provides as follows:

> (a) An operator of a commercial Web site or online service, including a mobile app, that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available[70]

This "conspicuously" posted privacy notice must:

- Specify the categories of personally identifiable information that the operator collects through the Web site or online service; about individual

consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information

In addition, the statute states the following:

- If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information, it must provide a description of that process
- Describe the process by which the operator notifies affected consumers of material changes to the operator's privacy policy for that Web site or online service.
- Identify its effective date
- Disclose how the operator responds to Web browser "do not track" signals or other similar mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services.
- Disclose whether the operator is aware that other parties may collect personally identifiable information about an individual consumer's online activities when a consumer uses the operator's Web site or service.[71]

Under this Act, a covered operator that collects personally identifiable information through the Web site or online service from affected individual consumers who reside in California shall be in violation of this section if the operator fails to comply with the Act's operative provisions or with the provisions of its posted privacy policy either (1) "knowingly and willfully" or (2) "negligently and materially."[72]

Other states may well enact similar laws in the near future, especially given the current environment in which the need for such laws becomes increasingly clear.

State-Level Compliance and Enforcement by Attorneys General

Background; Organization and Mission

Most state government enforcement activities involving judicial lawsuits are carried out by the state attorney general, the state's law department. The following example of the New York Attorney General's work is typical:

> As head of the Department of Law, the Attorney General is both the "People's Lawyer" and the State's chief legal officer. As the "People's Lawyer," the Attorney General serves as the guardian of the legal rights of the citizens of New York, its organizations and its natural resources. In his role as the State's chief legal counsel, the Attorney General not only advises the Executive branch of State government, but also defends actions and proceedings on behalf of the State.[73]
>
> The Attorney General serves all New Yorkers in numerous matters affecting their daily lives. The Attorney General's Office is charged with the statutory and common law powers to protect consumers and investors, charitable donors, the public health and environment, civil rights, and the rights of wage-earners and businesses across the State.

Cybercrime and Other Cyber Threats; Compliance and Enforcement

Moving to the topic of state cybersecurity law enforcement, such activities have been significant in certain state attorneys general offices. *Cybercime News*, a publication of the National Association of Attorneys General, National Attorneys General Training & Research Institute, describes current enforcement initiatives, based on various cyber-risk-related laws.[74] The publication provides a helpful picture of how some such offices are rising to meet the challenge of fighting cybercrime. The cases listed relate only to businesses and their managers conducting business normal operations and do not include any of the many types of cases outside that scope, such as child pornography.

- Illinois Attorney General Lisa Madigan filed suit against FileFax Inc., a document storage company, for allegedly exposing thousands of patient medical records containing social security numbers and other personal information. The records were those of patients of Suburban Lung Associates, which contracted with FileFax to maintain and destroy them. The suit alleges FileFax failed to provide safe and secure collection, retention, storage and destruction of the records, citing one instance where FileFax disposed of records in a publicly accessible unlocked garbage dumpster outside its facility.
- Vermont Attorney General William Sorrell filed a settlement with Embassy Suites South San Francisco, resolving allegations the hotel failed to notify consumers of a security breach without unreasonable delay. The hotel had received notification from customers of unauthorized charges on their credit cards, but did not send notice of a breach to residents until six months later.[75]

The publication also reports on the progress of state adoptions of new cyber-related laws, whose enactment will arguably greatly strengthen the capacity of state enforcement officials to protect the public interest in this area.[76]

One potential enforcement matter that illustrates how major cases evolve concerns an investigation by certain state attorneys general of the financial firm J. P. Morgan Chase. Note the investigatory approach and the adroit (and interestingly differing) uses of the media on the part of the attorneys general, as revealed in the following article excerpt from *The Wall Street Journal*. The news report identifies an investigatory scenario in which two state attorneys general may be on the verge of initiating enforcement action in behalf of consumers based on a claim of deficiencies in the firm's cybersecurity governance:

> At least two state attorneys general are investigating J.P. Morgan Chase & Co. for its handling of a cyberattack this summer that compromised customer contact information of about 76 million households and 7 million small businesses, according to people familiar with the matter.
>
> The office of Connecticut Attorney General George Jepsen has been in contact with the bank regarding the cyberattack since the bank's disclosure earlier this year, a spokeswoman for the attorney general said. She declined to provide further detail, saying it was a pending matter.
>
> Illinois Attorney General Lisa Madigan is also looking into the breach. In a statement Friday, Ms. Madigan said that the cyberattack is among the most "troubling" breaches because it shows how vulnerable U.S. institutions and their databases are.
>
> "Millions of Americans trusted Chase to secure their money and personal information, but by failing to be forthcoming, they have lost their confidence in Chase," she said in a statement. She noted the bank's filing this week about the attack "only revealed...limited details."
>
> Ms. Madigan said the cyberattack demands a response from "the highest level of our government" and investigation results should be shared with the public, since consumers' information and financial security is at risk.[77]

In general, a review of the various laws and enforcement activities at the state level make clear that the state law patchwork is obviously beneficial—especially where efforts are vigorous—but the larger national picture of cybersecurity enforcement is not one of uniformity at present.

C. Private Litigation

Legal Theories Used in Lawsuits

One important area of note in the cybersecurity arena is the challenge of private litigation against companies for failure to provide for proper cybersecurity governance. These cases are likely to be based on one or more of the following legal theories:

- Breach of contract;
- Breach of fiduciary duty;

- Waste of corporate assets;
- Unjust enrichment;
- Unfair competition;
- Property (including intellectual property) Misappropriation;
- Tort;
- State or federal statutes that create a "private right of action ," or right of a non-governmental person to sue under that statute seeking relief for cyber-relevant injury inflicted.

Litigation Strategies, Contexts and Scenarios

First, it is crucial to note that many private lawsuits are commenced after a government agency has charged a company with a cybersecurity violation—especially if the government eventually wins, but even if there is merely a settlement. Why? One reason is that where the government has chosen to go forward with charges, there is at least an implicit assumption that there has been a thorough preliminary investigation, by an expert agency, in which substantial incriminating evidence has been uncovered. The impact of such government action can be not only psychological, but also reputational and even legal.

Second, note that where external parties, such as consumers or other contracting parties, sue the corporation for injuries inflicted, they often raise the stakes greatly by bring the suit as a class action. This means that although only a few persons may actually initiate the suit, the suit's ultimate plaintiffs are both those "named" persons and also "all others similarly situated" who may have been harmed by the governance failure. Obviously, in the event of a victory, the monetary damages recovered by the plaintiffs from the corporation must be sufficient to compensate the entire class, which can be catastrophic for some businesses.

Finally, where shareholders sue, the suit is often against the directors and officers for failure to live up to their duties and for thus causing injury to the "corporation and shareholders as a whole." These suits, "shareholder derivative suits," are initiated by the shareholders but the suit is on behalf of the corporation and any relief awarded would go to the corporation.

Illustrative Cases

The following types of litigation are typical. In some of the descriptions the defendant companies provide information on both governmental and private litigation, but this is useful in that it provides an overall picture of the challenge facing a company in the wake of a cyber-breach or other cyber incident. Note that in some instances the litigation descriptions are direct quotes from the corporation's SEC annual disclosure report on Form 10-K. Be aware that the challenge for reporting companies in these instances is to make proper disclosures of the litigation in compliance with SEC rules while (1) avoiding, where possible, making a formal, damaging "admission" or "confession" under relevant court rules of evidence and (2) avoiding, where possible, having to record a "contingent" liability and related expense on its financial statements under relevant accounting rules. The former would negatively affect the corporation's prospects in the lawsuit and the latter would entail an adverse impact on the company's financial status. Finally, note that in some instances the description of the case is a direct quote from a plaintiff's complaint filed with a court. Necessarily, the description of the facts in these instances is one-sided because of the "adversarial" nature of litigation.

Target Corporation

(SEC Form 10-K (MD&A), March 14, 2014)[78]

Description of Event

As previously disclosed, we experienced a data breach in which an intruder stole certain payment card and other guest information from our network (the Data Breach). Based on our investigation to date, we believe that the intruder accessed and stole payment card data from approximately 40 million credit and debit card accounts of guests who shopped at our U.S. stores between November 27 and December 15, 2013, through malware installed on our point-of-sale

system in our U.S. stores. On December 15, we removed the malware from virtually all registers in our U.S. stores. Payment card data used in transactions made by 56 additional guests in the period between December 16 and December 17 was stolen prior to our disabling malware on one additional register that was disconnected from our system when we completed the initial malware removal on December 15. In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals. Our investigation of the matter is ongoing, and we are supporting law enforcement efforts to identify the responsible parties.

Expenses Incurred and Amounts Accrued

In the fourth quarter of 2013, we recorded $61 million of pretax Data Breach-related expenses, and expected insurance proceeds of $44 million, for net expenses of $17 million ($11 million after tax), or $0.02 per diluted share. These expenses were included in our Consolidated Statements of Operations as Selling, General and Administrative Expenses (SG&A), but were not part of our segment results. Expenses include costs to investigate the Data Breach, provide credit-monitoring services to our guests, increase staffing in our call centers, and procure legal and other professional services.

The $61 million of fourth quarter expenses also includes an accrual related to the expected payment card networks' claims by reason of the Data Breach. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks believe they or their issuing banks have incurred. In order for us to have liability for such claims, we believe that a court would have to find among other things that (1) at the time of the Data Breach the portion of our network that handles payment card data was noncompliant with applicable data security standards in a manner that contributed to the Data Breach, and (2) the network operating rules around reimbursement of operating costs and counterfeit fraud losses are enforceable.

Litigation and Governmental Investigations

In addition, more than 80 actions have been filed in courts in many states and other claims have been or may be asserted against us on behalf of guests, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising out of the Data Breach. State and federal agencies, including the State Attorneys General, the Federal Trade Commission and the SEC are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. Although we are cooperating in these investigations, we may be subject to fines or other obligations, which may have an adverse effect on how we operate our business and our results of operations.

The Home Depot, Inc.

(SEC Form 10-K, March 25, 2015)[79]

Data Breach

In the third quarter of fiscal 2014, we confirmed that our payment data systems were breached, which potentially impacted customers who used payment cards at self-checkout systems in our U.S. and Canadian stores. Our investigation to date has determined the intruder used a vendor's user name and password to enter the perimeter of our network. The intruder then acquired elevated rights that allowed it to navigate portions of our systems and to deploy unique, custom-built malware on our self-checkout systems to access payment card information of up to 56 million customers who shopped at our U.S. and Canadian stores between April 2014 and September 2014. On September 18, 2014, we confirmed that the malware used in the Data Breach had been eliminated from our systems. There is no evidence that debit PIN numbers were compromised or that the Data Breach impacted stores in Mexico or customers who shopped online at HomeDepot.com or HomeDepot.ca. In addition, we announced on November 6, 2014 that separate files containing approximately 53 million email addresses were also taken during the Data Breach. These files did not contain passwords, payment card information or other sensitive personal information. The

investigation of the Data Breach is ongoing, and we are supporting law enforcement efforts to identify the responsible parties.

Litigation, Claims and Government Investigations

In addition to the above expenses, we believe it is probable that the payment card networks will make claims against us. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks assert they or their issuing banks have incurred. In addition, at least 57 actions have been filed in courts in the U.S. and Canada, and other claims may be asserted against us on behalf of customers, payment card brands, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising from the Data Breach. Furthermore, several state and federal agencies, including State Attorneys General, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. We are cooperating in the governmental investigations, and we may be subject to fines or other obligations.

Complaint

Aswad Hood, on behalf of himself and all others similarly situated vs. Anthem, Inc., Blue Cross of California and Anthem Blue Cross Life and Health Insurance Company[80]

(United States District Court, Central District of California)

(Class Action Complaint, Case 2:15-cv-00918-CAS-PLA, for Relief Based on: (1) Violation of the California Customer Records Act; (2) Violation of the California Unfair Competition Law; (3) Breach of Contract; and (4) Negligence)

Summary of the Case

1. On February 4, 2015, Anthem, Inc. announced that hackers had breached the company's database warehouse and obtained the personal information of approximately 80 million current and former Anthem health insurance plan members and Anthem employees. The personal information obtained in the breach included plan members' and employees' names, birthdays, medicals IDs, Social Security numbers, addresses, email addresses, and employment information, including income.

2. Plan members' and employees' personal information has been exposed –and their identities put at risk – because Anthem failed to maintain reasonable and adequate security measures. Anthem has statutory obligations to protect the sensitive personal information it maintains, yet failed at numerous opportunities to prevent, detect, or limit the scope the breach. Among other things, Anthem (1) failed to implement security measures designed to prevent this attack even though the health care industry has been repeatedly warned about the risk of cyber-attacks, (2) failed to employ security protocols to detect the unauthorized network activity, and (3) failed to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

3. Plaintiff is a current Anthem Blue Cross plan member who brings this proposed class action lawsuit on behalf of Anthem health plan members and Anthem employees whose personal information has been compromised as a result of the data breach. He seeks injunctive relief requiring Anthem to implement and maintain security practices to comply with regulations designed to prevent and remedy these types of breaches, as well as restitution, damages, and other relief.

Complaint

Dennis Palkon, Derivatively on Behalf of Wyndham Worldwide Corporation v. Stephen P. Holmes, Eric A. Danziger, Scott G. McLester, James E. Buckman, Michael H. Wargotz, George Herrera, Pauline D. E. Richards, Myra J. Biblowit, Brian Mulroney, Steven A. Rudnitsky, and Does 1 – 1081

(United States District Court, District of New Jersey)

(Verified Shareholder Derivative Complaint, Case No. 2:14-cv-01234-SRC-CLW for (1) Breach of Fiduciary Duty, (2) Waste of Corporate Assets and (3) Unjust Enrichment)

Nature and Summary of the Action

1. This is a verified shareholder derivative action on behalf of nominal defendant Wyndham Worldwide Corporation ("WWC" or the "Company") against certain of its officers and members of its Board of Directors (the "Board"). This action seeks to remedy defendants' violations of law, breaches of fiduciary duties, and waste of corporate assets that have caused substantial damages to the Company. Plaintiff has made a litigation demand upon WWC's Board. As set forth below, the Board wrongfully refused plaintiff's demand.

2. WWC is one of the world's largest hospitality companies. As part of their normal business practices, WWC and its subsidiaries routinely collect their customers' personal and financial information, including payment card account numbers, expiration dates, and security codes. WWC and its subsidiaries assure their customers that they will protect this sensitive private information. However, as explained below, WWC failed to live up to this promise.

3. This action arises out of the Individual Defendants' (as defined herein) responsibility for three separate data breaches. In violation of their express promise to do so, and contrary to reasonable customer expectations, WWC and its subsidiaries failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner. As a result of WWC's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from over 619,000 of the Company's customers. For many of these victims, identity thieves have already utilized their personal information to commit fraud and other crimes. For hundreds of thousands of others, constant vigilance of their financial and personal records will be required to protect themselves from the threat of having their identities stolen.

4. **[Redacted language]** Among other things, the Individual Defendants failed to ensure that the Company and its subsidiaries implemented adequate information security policies and procedures (such as by employing firewalls) prior to connecting their local computer networks to other computer networks. Additionally, the Company's property management system server used an operating system so out of date that WWC's vendor stopped providing security updates for the operating system more than *three years* prior to the intrusions. Further, the Individual Defendants allowed the Company's software to be configured inappropriately, resulting in the storage of payment card information in clear readable text. These deficiencies, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.

5. The Individual Defendants aggravated the damage to the Company from the data breaches by failing to timely disclose the breaches in the Company's financial filings. The first time WWC mentioned any of the three data breaches in a financial filing was on July 25, 2012, over *two-and-a-half years* after the third breach had occurred. One week after this untimely disclosure, on August 1, 2012, the U.S. Securities

and Exchange Commission ("SEC") sent a comment letter demanding that WWC timely disclose such incidents in future filings.

6. The defendants' failures to implement appropriate internal controls at WWC designed to detect and prevent repetitive data breaches have severely damaged WWC. The Company is currently a defendant in a lawsuit filed by the Federal Trade Commission ("FTC") alleging unfairness and deception-based violations of section 5 of the Federal Trade Commission Act ("FTC Act") (the "FTC Action") **[Redacted language]** The FTC Action poses the risk of tens of millions of dollars in further damages to the Company. Moreover, WWC's failure to protect its customers' personal and financial information has damaged its reputation with its customer base.

7. Upon learning of these events, plaintiff sent a letter to WWC's Board demanding that the Board "take all necessary steps to investigate, address, and promptly remedy the harm inflicted upon [WWC]." The Board consciously disregarded its duty to conduct a reasonable investigation upon receipt of a shareholder demand and refused to conduct any independent investigation whatsoever of the demand's allegations. The Board refused plaintiff's demand based on the advice of conflicted counsel who could not, and did not, objectively evaluate the demand's allegations. Because the Board failed to act in good faith and with due care (on the basis of a reasonable investigation), its decision to refuse plaintiff's demand was wrongful and is not protected by the business judgment rule.

8. Plaintiff now brings this litigation on behalf of WWC to rectify the conduct of the individuals bearing ultimate responsibility for the Company's misconduct—the directors and senior management.

D. Private Companies, Private Equity and Venture Capital

1. Private vs. Public Companies: Similarities and Differences

While there are technical legal definitions of what makes a company private, closely-held, or public, some simple observations may be more useful. The most salient point on this subject as it relates to cybersecurity, however, is that, for the most part, private companies and public companies (as well as their directors and officers) are bound by the same laws. Perhaps the most the prominent exception to this rule is found in the disclosure-oriented securities laws administered by the SEC.[82] Public companies must make extensive disclosures and financial reports to the SEC about "material" aspects of its business and operations—including aspects involving cybersecurity, related threats and risks and other relevant matters. Additionally, numerous laws provide for exceptions or limited application in the case of small private businesses because of their more limited size and scale by comparison to the large public corporation.

A final observation—and an ironic one—is that a private company, particularly one with an ambitious growth and development agenda, may have to meet most or all the standards applicable to a public company. That is to say, there may be legal, economic or other factors and constraints on "high achiever" private companies that impose disclosure, financial reporting and other standards on them that are the same as those of a public company. Here are some examples of sources of those requirements:

- Government contracts;
- Insurance contracts (including cybersecurity insurance);
- Major subcontracts (public or private);
- Major vendor/vendee relations (either side);
- Private equity, venture capital, or other corporate financing strategies that look toward ambitious growth and development.

Any one of these situations may come with conditions (explicit, implicit, legal, economic or reputational) that may move a private company to a higher level of compliance with legal or other standards.

2. The Impact of Present (and Future) Private Equity or Venture Capital Financing on Private Company Organization and Operation

The following excerpt provides a brief description of the nature and objectives of private equity and venture capital, as well as the main differences between the two forms of financing:

> Private equity is sometimes confused with venture capital because they both refer to firms that invest in companies and exit through selling their investments in equity financing, such as initial public offerings (IPOs). However, there are major differences in the way firms involved in the two types of funding do things. They buy different types and sizes of companies, they invest different amounts of money and they claim different percentages of equity in the companies in which they invest.
>
> Private equity firms mostly buy mature companies that are already established. The companies may be deteriorating or not making the profits they should be due to inefficiency. Private equity firms buy these companies and streamline operations to increase revenues. Venture capital firms, on the other hand, mostly invest in start-ups with high growth potential.
>
> Private equity firms mostly buy 100% ownership of the companies in which they invest. As a result, the companies are in total control of the firm after the buyout. Venture capital firms invest in 50% or less of the equity of the companies. Most venture capital firms prefer to spread out their risk and invest in many different companies. If one start-up fails, the entire fund in the venture capital firm is not affected substantially.[83]

As noted above, private companies whose corporate financing strategies include the use of private equity or venture capital firms should expect to have to meet high-level standards in their organization and operations. These days, of course, this point applies increasingly to cybersecurity governance policies and practices. Three reasons why this is true as a general matter are the facts that:

- Private equity and venture capital firms themselves are seeking especially high returns and are therefore willing to take on significant risks—but not unintelligently or recklessly. Therefore, they impose strict demands on both prospective and present investee companies, and they monitor these companies carefully, including often placing one or more of their own personnel in strategic positions (directors, officers, and the like) in the companies. For example, with respect to information about investee targets of investment:

  > "Information is a prized commodity for [private equity and venture capital] fund managers, who demand high levels of transparency from the companies they invest in"[84];

- The investors in these firms that provide the majority of the capital for investment in private companies include pension funds (public and private), insurance companies, wealthy individuals, and the like. They are not only very astute and discriminating themselves but also are often constrained to protect their own beneficiaries by legal standards such as the "prudent investor" and other fiduciary-duty laws;[85] and
- The overall organization of the financing arrangements set up by these firms often include managing and advisory entities that meet the definition of "investment adviser" under the federal Investment Advisers Act of 1940.86. This Act "requires that firms or sole practitioners compensated for advising others about securities investments must register with the SEC and conform to regulations designed to protect investors."[87] As a result of

> recent legislative and regulatory initiatives, the scope of the Act is now even broader than ever before, imposing its disclosure requirements and other procedures on many organizations that serve as investment advisers to private equity and venture capital firms.[88]

In an era of increasingly stringent cybersecurity consciousness, as well as government enforcement and private litigation, any private company—and any such company's directors and managers—must be prepared to set properly high levels of cybersecurity governance. Similarly, private equity and venture capital firms clearly must follow this same advice. These points are underscored by the following predictions of a prominent legal practitioner in the area:

> As we look ahead to 2015 and 2016, there are three major issues impacting the private equity market: (1) increased regulatory oversight regarding the activities of private equity funds… (2) a "flight to quality" on the part of the limited partner investors that invest … and (3) a rebalance of negotiating leverage between the general partners that manage the fund and the limited partners.[89]

E. A Note on the Role of Legal Counsel

Given the pervasive role of law, regulation and litigation in the cybersecurity area, it should come as no surprise that the role of legal counsel is critical to companies faced with cyber threats and other cyber incidents. The following quote from an experienced attorney not only underscores this point but also summarizes the essential duties that a company's in-house counsel should assume in corporate cybersecurity governance:

> A big part of the GC's role is risk identification, analysis and management in an ever-increasing number of ways. An organization's Compliance group, as well as its Privacy function, may report up through the Law Department. GCs, particularly those in consumer-facing companies, in public companies, those that contract with the government, and in companies with highly valued and protected public images, are increasingly called upon to help manage crises that arise from cyber-attacks. As a public company director, I know that boards expect their GCs to provide real-time analysis and guidance on all components of risk mitigation, including cybersecurity. In the digital age, news of these attacks (particularly those involving the theft of customers' credit card, healthcare information, and other highly sensitive data) can go viral around the world within minutes, having an immediate effect on a brand's reputation and standing in the marketplace. With regard to their organizations' own intellectual property, GCs also sit squarely on the front lines in helping to ensure important business assets remain secure and that their risks—legal and otherwise—are kept at a minimum.[90]

In Section V(C) of this White Paper, we set out "best practices" standards and guidelines for attorneys charged with counseling companies through the maze of issues and considerations that must be mastered to accomplish high levels of corporate governance.

LEGAL DUTIES AND LIABILITIES FOR CYBERSECURITY GOVERNANCE IMPOSED DIRECTLY ON THE BOARD OF DIRECTORS AND OFFICERS

A. State Law Duties and Liabilities Imposed on Directors and Officers to Promote Corporate Governance; The Fiduciary Duty Concept

1. Some Basic Concepts of Corporate Law

The corporation is a "separate legal entity" under the law, but it cannot act for itself. It must act through people, and these people take on roles such as directors, officers, legal counsel, investment bankers and others (both inside and outside the corporation). Moreover, the board of directors plays a primary, indeed a central, role in the governance of the corporation. For example, Delaware General Corporation Law (DGCL) § 141 (a) provides as follows:

> The business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors ....[91]

The fiduciary duty concept grows out of this "corporate statutory norm" by introducing into corporate law certain standards of conduct and liability for how directors manage the corporation. Officers and others working for the corporation are also fiduciaries because their delegations of power and authority from the directors include certain duties. Note that in general, these fiduciary duties are owed to the corporation and the shareholders[92]. This means that usually only the corporation (including through a representative) or the shareholders may sue the directors and officers in court based on violations (breaches) of these duties.[93] Simply stated, the fiduciary duty concept sends the following message:

> Carry out your assigned duties properly, in the corporation's and the shareholders' best interests, and if you do not do so, you may be sued and held personally liable for economic injuries that come to the corporation or the shareholders because of that failure of duty.

In pursuit of this basic command, fiduciary duty law has generally been structured into two major duties, the fiduciary duties of care and loyalty, as well as certain additional duties, notably for our purposes, the fiduciary duties of oversight (monitoring).[94]

2. The Fiduciary Duty of Care and the Business Judgment Rule

Purpose of the Duty

The fiduciary duty of care (FDC) is one a fundamental requirement and guide in corporate law whose rationale is clearly self-evident. More particularly, to provide a specific example, *American Law Institute (ALI) Principles of Corporate Governance,* Section 4.01(a) requires that directors carry out their work for the corporation:

> in good faith, in a manner that he or she reasonably believes to be in the best interests of the corporation, and with the care that an ordinarily prudent person would reasonably be expected to exercise in a like position and under similar circumstances. [95]

Furthermore, directors must meet this standard at a minimum, meaning that they have no legal

obligation to achieve higher-level "best practices" standards.[96] At the same time, if they have special skills (such as those in accounting, finance or technology) they must apply those skills in satisfaction of their duties. The plain language of this well-known statement of the FDC suggests its great relevance to cybersecurity governance. Moreover, this relevance grows literally daily with the rapidly increasing number, variety and virulence of cyber risks and threats today.

The Business Judgment Rule

The "business judgment rule" (BJR) helps set limits on directors' and officers' liabilities when they are sued for breaches of fiduciary duty. It only applies when they are sued about a specific decision that they have made. So, if the FDC requires that directors' decisions be made "carefully," the BJR assures that they don't have to be perfect. One court has described the nature and effect of this court-made rule of "judicial self-restraint":

> Absent bad faith or some other corrupt motive, directors are normally not liable to the corporation for mistakes of judgment.[97]

Under Delaware law, the liability standard is set at "gross negligence," which means that the "legal presumption" of the BJR is not powerful enough to protect against fiduciary conduct reaching this level.[98] In a lawsuit, the directors and officers will assert their protections under the BJR as an "affirmative defense." If the plaintiff cannot rebut the legal presumption, then he or she will lose the lawsuit. This is the result in most cases.[99]

3. The Fiduciary Duty of Loyalty

The fiduciary duty of loyalty (FDL) has generally been defined in "broad and unyielding terms."[100] For example, as observed in the famous case of *Guth v. Loft*:

> Corporate … directors are not permitted to use their position of trust and confidence to further their private interests … [The FDL] demands of a corporate … director … the most scrupulous observance of his duty, not only affirmatively to protect the interests of the corporation … but also to refrain from doing anything that would work injury to the corporation, or to deprive it of profit.[101]

The types of FDL cases we are describing here are classic "conflict-of-interest" cases. They are a major part of corporate law. But for our purposes, conflict of interest FDL cases are not a major focus in discussions about cybersecurity governance.

4. Other Fiduciary Duties: the Duty of Oversight and Monitoring

A particularly pertinent fiduciary duty for directors and officers of corporations concerned with cybersecurity is the fiduciary duty of oversight, or monitoring. This duty relates to director duties to oversee and monitor corporate activities properly. It comes into play when directors are sued for losses caused by the corporation arising:

> from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss.[102]

Under Delaware corporate law, the leading case law guidance for how directors and officers should proceed to prevent liability in cases of this nature comes from *In re Caremark Intern. Inc. Derivative Litigation*[103] and *Stone v. Ritter*.[104] *Stone* affirms that "*Caremark* articulates the necessary conditions predicate for director oversight liability." Together, those two cases identify the two alternative factual scenarios that, if proven, will give rise to director liability:

- The "directors utterly failed to implement any reporting or information system or controls," or
- The directors, "having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.[105]

The "bottom line" on this duty is that, although it is real and actual, it is not as stringent as one might imagine. Indeed, both the *Caremark* and

Stone courts characterized a plaintiff's chances of winning in a lawsuit like this against the directors as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[106] Nevertheless, directors are sometimes held liable, and for this reason directors must have in place—and implement—appropriate measures and protocols in order to comply properly with their duties and avoid personal liability.

5. The Takeaways About Fiduciary Duty Law: How Should Directors and Officers Proceed in the Face of Modern Cybersecurity Risks and Threats?

The Duties and the Built-in Protections Against them; the BJR and Beyond

As one can see, the legal architecture in and around the FDC starts off looking rather demanding and strict on directors and officers in their management of the corporation. That is, until one encounters the BJR, which, as can be seen, typically provides significant director and officer protection. Moreover, as regards all of the fiduciary duties, the legal architecture in and around it provides for certain additional protections, and while these protections are not unlimited, they often play a significant role in shareholder litigation against directors. Here are some prominent examples:

- Statutory provisions giving the directors a right to rely upon corporate records or the information, opinions, reports, and the like, of corporate officers, directors, employees and consultants;[107]
- Exculpation provisions, which, when approved and inserted in the corporate documents, provide for the limitation—or even elimination—of liability for monetary damages in the event a demonstrated violation of the FDC;[108]
- Provisions containing a process by which directors may narrow the scope of their FDL "conflict-of-interest" liability in "interested transactions," so long as the transactions are "fair" and not in "bad faith." For example, pursuant to these authorizations, directors and officers may enter into profitable contractual agreements with their corporation, again subject to the fairness and good faith limitations.[109]
- Corporate indemnification provisions, which provide reimbursement for certain expenditures incurred by directors and officers in the course of litigation or similar actions under specified circumstances;[110]
- Director and Officer (D&O) Liability Insurance, which provides insurance; coverage for certain losses incurred by directors and officers.[111]

These protections should be considered together in understanding the total exposure picture for directors in any given setting.

Nevertheless, the Harm from Litigation Can Be Actual and Serious

On balance, although one could easily conclude that fiduciaries' protections make them invincible, this would be a mistake. None of these protective measures will help in instances of egregious behavior. Further, even unsuccessful FDC claims may cause substantial losses to the corporation, such as reputational damage, business sales or market share losses and share price de-valuations in the stock market.

We believe it would be helpful at this point to review the structures and procedures put in place in the Stone case, a case in which the court held that the directors had clearly met and exceeded their fiduciary duties—in large part because of the extensive information and reporting system that they had set up and maintained. Arguably, this system would be protective under any scenario in which directors and officers are faced with cybersecurity risks and threats. Note that corporations of more modest means and resources will likely search for innovative ways to streamline this more elaborate system.

Stone v. Ritter

In *Stone*, plaintiffs (shareholders) brought suit against the directors in connection with a $50 million payment by AmSouth Bancorporation in fines and civil penalties "to resolve government and regulatory investigations pertaining principally to the failure by bank employees to file 'Suspicious Activity Reports' ('SARs'), as required by the Federal Bank Secrecy Act ('BSA') and various anti-money-laundering ('AML') regulations." The court dismissed the case, and in doing so had great praise for the compliance program and practices—put in place before receiving notice of the government investigations. The following features were the highlights of those preventative steps. Remember that the program and practices failed to capture the violations themselves, but legally they were sufficient to exonerate the directors of all claims.

- A BSA Officer had been appointed who was responsible for all BSA/AML-related matters, including employee training, general communications and reporting, and presenting AML policy and program and changes to them to directors, officers and other relevant personnel.
- A BSA/AML Compliance Department had been established, headed by the BSA Officer and comprised of nineteen professionals, including a BSA/AML Compliance Manager and a Compliance Reporting Manager.
- A Corporate Security Department had been established, which was responsible at all times for the detection and reporting of suspicious activity as it relates to fraudulent activity, and was headed in a former U.S. Secret Service officer.
- A Suspicious Activity Oversight Committee, made up of board members, had been established to "oversee the policy, procedure, and process issues affecting the Corporate Security and BSA/AML Compliance Programs, to ensure that an effective program exists at AmSouth to deter, detect, and report money laundering, suspicious activity and other fraudulent activity."[112]

B. Other Legal Duties and Liabilities Imposed on Directors and Officers in State or Federal Law; "Statutory" Law and the Example of the Federal Securities Laws

Often a federal, or Congressional, act will impose legal duties not only on the corporation but also on its directors and officers. The discussion below will illustrate this point in the context of the federal securities laws.

Public Offerings and Director Duties and Liabilities

Although the securities laws impose numerous express duties and liabilities on directors, certain provisions are especially noteworthy and appropriate to the cybersecurity governance context. One prominent example can be found in Section 11 of the Securities Act of 1933, which imposes liability on certain persons, including directors, in connection with misstatements or omissions during the public offering of securities. Specifically, that section imposes liability on:

> every person who was a director of (or person performing similar functions) … [who participated in the preparation of a] registration statement" (disclosure document) in a registered public offering containing] an untrue statement of a material fact or omitted to state a material fact required … to make the statements therein not misleading."[113]

The obvious Congressional intention in including directors on the list of potentially culpable persons was to provide a special incentive for directors to apply themselves with a high degree of professionalism to the public offering process, which is a critical part of the American financial architecture.

Again, we have yet another instance in which a corporate governance process was of such great overall significance to the American economy and society that Congress deemed it necessary to require an especially high level of quality in director performance through the device of express individual duties and liabilities.

LEGAL DUTIES AND LIABILITIES FOR CYBERSECURITY GOVERNANCE IMPOSED DIRECTLY ON THE CORPORATION; SOME BASIC CONCEPTS OF CORPORATE LAW

A. The Corporation is a Separate Legal Entity, or "Person." Therefore it is the "Business" That has the Duty and Suffers the Liability for Violations (Not the Directors, Officers and Others).

In understanding the roles and status of the board of directors (as well as the officers and others), one must first understand that the corporation itself is the "business." This is true because by law, the corporation is deemed to have its own, separate "legal personality." Perhaps the most important implication of this "entity" status of the corporation is that, with two major exceptions, the corporation alone (and not the people who work for it) is legally responsible for its business acts that violate applicable law, such as torts and violations of contractual or regulatory requirements. Another direct implication of this separate legal status (and primary responsibility) is that the natural persons who physically carry out the [invisible, incorporeal] corporation's business activities have certain legal protections ("limited liability"), since they are not the actual, responsible business. Note that while the term "limited liability," strictly speaking, applies to corporate shareholders (whose liability is "limited" to only their investment in the corporation), it also applies to directors, officers and others working for the corporation.

Nevertheless, as the discussions below demonstrate, limited liability is not absolute. Corporate law includes certain "exceptions" to the general rule of limited liability, and in this sense there are exceptions, or limitations, to the legal protections of limited liability.

B. Exceptions to Limited Liability: Piercing The Corporate Veil

A director, officer or other person working for a corporation who is ordinarily entitled to the protection of limited liability can lose that protection of a court decides to "pierce the corporate veil." While the elements of analysis for this illusive and rarely granted judicial remedy vary virtually from state to state, piercing typically will occur when:

- Corporate business activities have caused a true injustice to someone that also amounts to an actual violation of some law, and
- The corporation itself hasn't sufficient assets to compensate that injured person.

When this happens and a lawsuit is brought against the corporation, a court may also allow some blameworthy person working for the corporation to be included as a defendant. In such a case, the court will be said to "pierce," "lift," or ignore the otherwise protective corporate "veil," thus also imposing liability on the blameworthy person and requiring him or her to pay compensation for the claims made by the plaintiff.

C. Exceptions to Limited Liability: "Direct" or "Active" Participation in the Corporate Violation

Another exception to, or limitation on, limited liability is that of "direct" or "active" participation. This legal concept is completely separate and apart from piercing the corporate veil. In effect, the concept says the following:

> Just because you work for a corporation, you don't have limited liability in every situation. If you participate directly or actively in an illegal act (including supervising others in the commission of one), you will be held liable along with the corporation. Neither the existence of the corporation nor your relationship with it will protect you from liability.

The cases are generally uniform in their acceptance of this theory. For example, in *People ex rel. Madigan v. Tang,*[114] the court conducted an exhaustive analysis of U.S. case law on the subject. The following quote from that case both underscores this point and also provides more particular guidance as to the specific actions and approaches to management and governance that might create liability for directors or officers:

> From our analysis of ... the other cases cited by the parties, and the Act itself ... we conclude that in order to state a claim 'for personal liability against a corporate officer under the Act, a plaintiff must do more than allege corporate wrongdoing. Similarly, the plaintiff must allege more than that the corporate officer held a management' position, had general corporate authority, or served in a supervisory capacity in order to establish individual liability under the Act. The plaintiff must allege facts establishing that the corporate officer had personal involvement or active participation in the acts resulting in liability, not just that he had personal involvement or active participation in the management of the corporation.[115]

D. The Takeaway for Cybersecurity Governance: Violations of Laws Directed at the Corporation Could Result in Both Corporate and Individual Liability

The fundamental point of this section is that directors and officers should never simply assume that they will enjoy the protections of limited liability automatically and inevitably. Understanding these exceptions is crucial to their body of knowledge and comprehension about serving successfully and effectively as directors of a corporation.

"BEST PRACTICES" STANDARDS AND GUIDELINES FOR CYBERSECURITY GOVERNANCE

Over the years, "best practices" standards and guidelines for cybersecurity governance have been issued by various organizations. The following discussion identifies some of the more prominent ones. Perhaps more important, the discussion distills these various guidelines and standards into a useful set of considerations in establishing a tailored approach to cybersecurity governance.

A. Best Practices Standards and Guidelines on Cybersecurity Governance

1. National Institute of Standards and Technology (NIST) Voluntary Framework

Reflecting the need to enhance critical national infrastructure security, President Obama issued Executive Order (EO) 13636 *Improving Critical Infrastructure Cybersecurity,* in February 2013. The EO directed the National Institute of Standards and Technology (NIST) to coordinate an effort with stakeholders to develop an appropriate voluntary framework. The framework was to be based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure.

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). To protect critical infrastructure from cyber threats, the NIST Framework is recommended for organizations of all sizes, regardless of threat exposure or the sophistication of cybersecurity systems, in recognizing, assessing, and managing risk. Critical infrastructure is defined as "[s]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets could have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters."

The NIST Framework provides a common roadmap for organizations to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state; and,
- Communicate among internal and external stakeholders about cybersecurity risk.

While the NIST Framework is not a law, regulation or official standard of care, some have expressed the view that it could well become a "de facto standard of care" through the evolution of case law and public opinion.[116] Most realistically, it will become influential, but not dispositive, as a standard.

2. American Bar Association (ABA) Initiatives

The American Bar Association (ABA) has taken seriously the need for effective cybersecurity governance. To that end, it has organized an ABA Legal Task Force on Cybersecurity and provides numerous resources on the subject for the benefit of its members and other professionals.[117] In addition, the ABA has adopted the following policy initiatives:

- **Report and Resolution 109, Adopted at the 2014 Annual Meeting in Boston**

  August 2014

  This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and to the data and systems to be protected.

- **Report and Resolution 118, Adopted at the 2013 Annual Meeting in San Francisco**

  August 2013

  This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms and urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions.

- **Cybersecurity Legal Task Force: Resolution and Report to the ABA Board of Governors**

  November 2012

  The ABA's Board of Governors approved a policy in November comprised of five cybersecurity principles developed by the Cybersecurity Legal Task Force. The Resolution reads as follows:

  > RESOLVED, That the American Bar Association urges the Executive and Legislative branches to consider the following guiding principles throughout the decision-making process when making U.S. policy determinations to improve cybersecurity for the U.S. public and private sectors:
  >
  > - **Principle 1**: Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.
  > - **Principle 2**: Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.
  > - **Principle 3**: Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.
  > - **Principle 4**: Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.
  > - **Principle 5**: Training, education, and workforce development of government and 18 corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.[118]

- **House of Delegates: Resolution 105A, Adopted at the 2012 Annual Meeting in Chicago**

  August 2012

  The ABA House of Delegates amends the black letter and Comments to Model Rules 1.0, 1.6, and 4.4, and the Comments to Model Rules 1.1 and 1.4 of the ABA Model Rules of Professional Conduct dated August 2012.119

The ABA resources are extremely helpful. Even though the policy statements and resolutions are very broad and do not provide practical advice, they do much to encourage and influence the development of concrete cybersecurity standards. Also, the ABA offers a number of practical materials that have been useful in the development of actual professional products such as this Research Report.[120]

3. National Association of Corporate Directors (NACD) Principles

As part of its general mission of "advancing exemplary board leadership and establishing leading boardroom practices," the National

Association of Corporate Directors (NACD) has produced a guidance document entitled *Cyber Security: Boardroom Implications.*[121] Although it is brief, the document distills the essentials of good cybersecurity governance. Particularly useful is the section entitled "Key Considerations for Board-Management Dialogue." The essential points of the section are the following:

- Identifying High-Value Information Targets
- Formulating Cyber Threat Detection and Response Plans
- The Human Factor[122]

These are, in fact, fundamental parameters in the development of a cybersecurity governance program. NACD also sets out a more extensive formulation in its publication entitled *Cyber-Risk Oversight Handbook*[123]. In that document, NACD presents five major principles of oversight:

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;
- Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances;
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda;
- Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
- Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[124]

These principles are discussed and explained thoroughly in the CyberRisk Oversight *Handbook*. Moreover, they are augmented by several quite useful appendices:

- APPENDIX A—Questions Directors Can Ask Management Once a Cyber Breach Is Found
- APPENDIX B—Questions Directors Can Ask to Assess the Board's "Cyber Literacy"
- APPENDIX C—Sample Cyber-Risk Dashboards

Altogether, these initiatives by the NACD provide truly complete guidance on cybersecurity governance. Indeed, they played a role in the development of this Research Report.

4. FINRA Principles and Effective Practices

In the FINRA Report discussed earlier, we noted its "Summary of Principles and Effective Practices" for cybersecurity governance. Presented below are the main governance areas and the Principles related to them; the "Effective Practices" are omitted because their length makes reproduction here impractical. Obviously, any use of this document for serious planning purposes would require resort to both the principles and effective practices in each governance area.

- **Governance and Risk Management for Cybersecurity**

  Principle: Firms should establish and implement a cybersecurity governance framework that supports informed decision making and escalation within the organization to identify and manage cybersecurity risks. The framework should include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available.

- **Cybersecurity Risk Assessment**

  Principle: Firms should conduct regular assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation.

- **Technical Controls**

  Principle: Firms should implement technical controls to protect firm software and hardware that stores and processes data, as well as the data itself.

- **Incident Response Planning**

  Principle: Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents.

- **Vendor Management**

  Principle: Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management.

- **Staff Training**

  Principle: Firms should provide cybersecurity training that is tailored to staff needs.

- **Cyber Intelligence and Information Sharing**

  Principle: Firms should use cyber threat intelligence to improve their ability to identify, detect and respond to cybersecurity threats.

- **Cyber Insurance**

  Principle: Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes.

5. U. S. Securities and Exchange Commission SEC Guidance

In deciding to issue its "CF Disclosure Guidance: Topic No. 2"[125] (SEC Guidance), the SEC determined that "it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances."[126] Moreover, the SEC appreciated the delicate balance to strike in deciding exactly what and how companies should make disclosures:

> We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security—and we emphasize that disclosures of that nature are not required under the federal securities laws.[127]

In pursuit of these objectives, the agency set out the following disclosure areas, providing in each instance a substantive and illustrative discussion of what should be the nature of disclosure in each area:

- Risk Factors;
- Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A);
- Description of Business;
- Legal Proceedings;
- Financial Statement Disclosures; and
- Disclosure Controls and Procedures[128]

As indicated in our earlier discussion of SEC activity in this area, this SEC Guidance and other agency initiatives have provided the basis for what is now a robust cybersecurity compliance and enforcement program. Further, the future promises only more of the same conscientiousness and intensity.

6. U.S. Department of Justice Best Practices for Victim Response and Reporting of Cyber Incidents

The Justice Department's "Best Practices for Victim Response and Reporting of Cyber Incidents"[129] has come to be respected as one of the important guides to cybersecurity governance. The following are the essential points of the guidance:

- Steps to Take *Before* a Cyber Intrusion or Attack Occurs

- Identify Your "Crown Jewels"
- Have an Actionable Plan in Place Before an Intrusion Occurs
- Have Appropriate Technology and Services in Place Before An Intrusion Occurs
- Have Appropriate Authorization in Place to Permit Network Monitoring
- Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident
- Ensure Organization Policies Align with Your Cyber Incident Response Plan
- Engage with Law Enforcement Before an Incident
- Establish Relationships with Cyber Information Sharing Organizations

- Responding to a Computer Intrusion: Executing Your Incident Response Plan
  - Step 1: Make an Initial Assessment
  - Step 2: Implement Measures to Minimize Continuing Damage
  - Step 3: Record and Collect Information
  - Step 4: Notify
- What Not to Do Following a Cyber Incident
  - Do Not Use the Compromised System to Communicate
  - Do Not Hack Into or Damage Another Network

This very thorough set of guidelines concludes with a "Cyber Incident Preparedness Checklist"[130] that is extremely helpful in and of itself.

B. Practical Advice on Cybersecurity Governance

The practical advice contained in this section is the product of many of the sources used in this Research Paper. The advice is not exhaustive, but it is meant to be comprehensive by serving as the core of a cybersecurity corporate governance program under the supervision of the corporation's board of directors:

- First, review all the best practices standards and guidelines discussed above and compare your own company's program to them, both at a distance and in detail;
- Consider retaining a consultant on cybersecurity governance (remember the difference between this type of professional and an IT expert). For most companies, this is a cost-effective measure, and the cost certainly compares favorably to the direct and secondary costs of a cyberattack;
- The process of designing or improving a cybersecurity governance program should include at least the most affected stakeholders (board of directors and relevant board committees, officers, IT personnel, legal counsel and perhaps the most substantial shareholders);
- Obtaining buy-in for acceptance requires open endorsement at the highest levels of the company, with those persons participating in presentations, training sessions and other means of clarifying that the program is an integral part of the company's corporate governance framework;
- Remember that constant evaluation and monitoring of the program's effectiveness is a fundamental requirement, which is a universal best practice.

C. The Role of Legal Counsel; Best Practices

As emphasized in Section II (E) of this Research Report, the role of legal counsel is crucial in cybersecurity governance. Essentially, they play a special, exclusive role in guiding the board of directors, the officers and the staff through the entire governance process, while bringing to bear a thorough knowledge of the law and the legal implications of every significant decision and choice

in that process. The following guidance is the product of a 10-point agenda developed by Harriet Pearson (IBM's first global privacy officer) and a study conducted by the Maurer School of Law at Indiana University. It should be borne in mind by legal counsel in performing these duties.

1. **Fulfill Fiduciary Duty of Board and Management.** Prove the company's directors and management met their duty to safeguard the company's stock price and assets. (32% of respondent counsel said they were involved in this activity)
2. **Address Disclosure Obligations and Appropriate Communications.** Conduct training for effective internal and external communication during cybersecurity incidents. (48%)
3. **Guide Participation in Public-Private Partnerships and Law Enforcement Interactions.** Manage information sharing to reduce risk and avoid conflicts with clients or government authorities. (10%)
4. **Achieve Regulatory Compliance.** But avoid "check- the-box" compliance efforts that may hinder effective cybersecurity measures. (46%)
5. **Provide Counsel to Cybersecurity Program.** Bring policy issues or potential legal risks to senior management or the board. (13%)
6. **Prepare to Handle Incidents and Crisis.** Identify internal and external resources and consider in advance what legal issues may arise during an incident. (53%)
7. **Manage Cybersecurity-Related Transactional Risk.** Whether M&A, vendor management or customer contracts, create a due diligence checklist and approach to cybersecurity issues. (43%)
8. **Effectively Use Insurance.** Use insurance (it's better than it used to be) but check the exclusions and conditions. (28%)
9. **Monitor and Strategically Engage in Public Policy.** Stay informed and engage in advocacy to build awareness of company positions and concerns. (22%)
10. **Discharge Professional Duty of Care.** Protect client and related information, particularly if it involves electronic communications and social media.[131]

Finally, projecting into the future, one experienced practitioner has made the following prediction about the need for general counsel to focus on cybersecurity:

> Legal departments should be prepared to address the intersection of cybersecurity and compliance within their organizations. The start of a federal cybersecurity compliance program could result in new government regulated disclosures and duty of care obligations. The Executive Order has prompted Congressional action, both through Framework adoption incentive proposals and efforts to codify the Executive Order. However, even without increased attention from the federal government, corporations need to be proactive in ensuring compliance with existing federal and state regulations, establishing the necessary controls, understanding the risks and having a plan in the event of a cyber-threat.[132]

CONCLUSION

Good cybersecurity governance is no longer an option. It is now a mandate. This Research Report has attempted to provide, from a legal perspective, some guidance that will assist boards of directors in carrying out their mandate to manage and direct the business and affairs of the corporation (and their legal counsel as well), as to cybersecurity matters, in a manner that is both productive for the corporation and the shareholders and protective for the directors.

END NOTES

[1] *See, e.g.* Pedro J. Martinez-Fraga, *The American Influence on International Commercial Arbitration: Doctrinal Developments and Discovery Methods* (Cambridge University Press 2014), tracing the contours of US doctrinal developments concerning international commercial arbitration.

[2] *See, e.g.* "2014 Data Breach Investigations Report," Verizon Risk Team, available at https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf.

[3] "2015 Cost of Data Breach Study: United States," p.1-, *Ponemon Institute Research Report*, May 2015, available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF.

[4] *Id.*

[5] *Id.* at 1-3.

[6] *Id.* at 1-3.

[7] *See*, "The Emergence of Cybersecurity Law," p. 4, February 2015, Indiana University Maurer School of Law/Hanover Research, available at http://info.law.indiana.edu/faculty-publications/The-Emergence-of-Cybersecurity-Law.pdf.

[8] Mary E. Galligan, Director, Cyber Risk Services, Deloitte & Touche, Transcript, "SEC Roundtable on Cybersecurity," March 26, 2014, Securities and Exchange Commission, available at http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

[9] "Cyber-Risk Oversight," Director's Handbook Series, 2014, NACD, page 6.

[10] Luis A. Aguilar, SEC Commissioner, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," June 10, 2014, Cyber Risks and the Boardroom" Conference, New York Stock Exchange, available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[11] "About the Computer Crime and Intellectual Property Section," U. S. Department of Justice, Criminal Division, available at http://www.justice.gov/criminal-ccips.

[12] "Regulatory Risk," Investopedia, available at http://www.investopedia.com/terms/r/regulatory_risk.asp.

[13] Daniel J. Fetterman and Mark P. Goodman, "White-Collar Landscape: Regulators, Targets and Priorities," in *Defending Corporations and Individuals in Government Investigations 31 (2014-2015 ed. D. J. Fetterman & Mark P. Goodman, Eds.)*.

[14] "What We Do," United States Federal Trade Commission, available at https://www.ftc.gov/about-ftc/what-we-do.

[15] 15 U.S.C. § 45(a).

[16] 15 U.S.C. §§ 1681–1681x.

[17] *See* 16 C.F.R. Parts 313 & 314, implementing 15 U.S.C. § 6801(b).

[18] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.

[19] 15 U.S.C. §§ 7701-7713; *see also* 16 C.F.R. Part 316.

[20] 15 U.S.C. §§ 6101-6108.

[21] *U.S. v. Telecheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), available at https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc.; *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3184/certegy-check-services-inc.

[22] *Apple, Inc.*, No. C-4444 (Mar. 25, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc.; *FTC v. Amazon.com*, No. 2:14-cv-01038 (W.D. Wash. filed July 10, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3238/amazoncom-inc.; *Google, Inc.*, No. C-4499 (Dec. 2, 2014) (F.T.C. consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3237/google-inc.

[23] *PaymentsMD, LLC*, No. C-4505 (Jan. 27, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.

[24] *See generally Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[25] *U.S. v. Yelp Inc.*, No. 3:14-cv-04163 (N.D. Cal. filed Sept. 17, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3066/yelp-inc.; *U.S. v. TinyCo, Inc.*, No. 3:14-cv-04164 (N.D. Cal. filed Sept. 17, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3209/tinyco-inc.

[26] Jessica Rich, Director, Bureau of Consumer Protection, FTC "FTC's Privacy and Data Security Priorities for 2015," March 3, 2015, Privacy and Cybersecurity Roundtable, Sidley Austin LLP, March 3, 2015, available at https://www.ftc.gov/system/files/documents/public_statements/671241/150303sidleyaustin.pdf.

[27] *See generally*, John c. Coffee, Jr. & Hillary A. Sale, *Securities Regulation* 1-9 (12th ed. 2012) ("The Goals of Securities Regulation").

[28] 15 U.S.C. § 77a et seq.

[29] 15 U.S.C. § 78a et seq.

[30] 15 U.S.C. §§ 77aaa –77bbbb.

[31] 15 U.S.C. §§ 80a-1–80a-64.

[32] 15 U.S.C. §§ 80b-1- 80b-2.1.

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

[34] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 17 CFR Part 248, Subpart A., available at https://www.law.cornell.edu/cfr/text/17/part-248/subpart-A.

[35] Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, available at http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[36] *Id.*

[37] 17 CFR § 248.30, available at https://www.law.cornell.edu/cfr/text/17/part-248/subpart-A.

[38] Regulation Systems Compliance and Integrity, Release No. 34-73639; File No. S7-01-13, November 19, 2014, 17 CFR Parts 240, 242, and 249, available at http://www.sec.gov/rules/final/2014/34-73639.pdf.

[39] SEC Release No. 34-73639; File No. S7-01-13, "Regulation Systems Compliance and Integrity," November 19, 2014, 17 CFR Parts 240, 242, and 249, available at http://www.sec.gov/rules/final/2014/34-73639.pdf.

[40] Regulation S-ID, 17 CFR § 248, Subpart C, available at http://www.sec.gov/rules/final/2013/34-69359.pdf.

[41] In the Matter of LPL Financial Corporation ("LPL"), formerly known as Linsco/Private Ledger Corp., SEC Action against LPL alleging a failure to adopt policies and procedures to safeguard customers' personal information, Administrative Proceeding, File No. 3-13181, Awptember 11, 2008, available at www.sec.gov/litigation/admin/2008/34-58515.pdf.

[42] *Id.*

[43] *In the Matter of Next Financial Group, Inc.* ("NEXT"), SEC Action against NEXT alleging willful violations of Regulation S-P by disclosing nonpublic personal information about customers to nonaffiliated third parties, Initial Decision, , Administrative Proceeding, File No. 3-13631, June 18, 2008, available at www.sec.gov/litigation/admin/2007/34-56316.pdf.

[44] *Id.*

[45] *In the Matter of Marc A. Ellis*, Administrative Proceeding, File No. 3-14328, April 7, 20011, available at http://www.sec.gov/litigation/admin/2011/34-64220.pdf.

[46] *In the Matter of Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network, Administrative Proceeding*, File No. 3-13631, September 29, 2009, available at https://www.sec.gov/litigation/admin/2009/34-60733.pdf.

[47] *Id.*

[48] Sarah N. Lynch and Joseph Lynn, "SEC hunts hackers who stole emails to trade corporate stocks," Jun 23, 2015, Reuters, available at http://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623.
Barry Vengerik, Kristen Dennesen, Jordan Berry and Jonathan Wrolstad, "Hacking the Street? Fin4 Likely Playing the Market," p. 3, 2014, FireEye. Inc., available at https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-fin4.pdf.

[49] Mary Jo White, "Opening Statement at SEC Roundtable on Cybersecurity," March 26, 2014, Securities and Exchange Commission, available at http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.
"About FINRA," FINRA website, available at http://www.finra.org/about.

[50] *See*, "Report on Cybersecurity Practices," (FINRA Report), page 3, available at https://mailhost.wcl.american.edu/exchange/wallace/Inbox/FINRA%20Guidelines.EML/1_multipart_xF8FF_2_FINRA_Report%20on%20Cybersecurity%20Practices.pdf/C58EA28C-18C0-4a97-9AF2-036E93DDAFB3/FINRA_Report%20on%20Cybersecurity%20Practices.pdf?attach=1.

[51] *Id.*

[52] "Improving Critical Infrastructure Cybersecurity, Executive Order 13636, Preliminary Cybersecurity Framework," National Institute of Standards and Technology (NIST), available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[53] FINRA Report, page 5.

[54] "About DOJ," United States Department of Justice website, available at http://www.justice.gov/about.

[55] Judiciary Act of 1789, ch. 20, sec. 35, 1 Stat. 73, 92-93 (1789).

[56] *Id.*

[57] Act to Establish the Department of Justice, ch. 150, 16 Stat. 162 (1870).

[58] *Id.*

[59] 18 U.S. Code § 1030.

[60] 18 U.S. Code Chapter 119.

[61] 18 U.S.C. §§ 2510-2522.

[62] 18 U.S. C. Chapter 206.

[63] *See*, CCIPS Press Releases—2015, available at http://www.justice.gov/criminal-ccips/ccips-press-releases-2015.

[64] Press Release, "Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Georgetown Cybersecurity Law Institute," May 20, 2015, available at http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-georgetown-cybersecurity.

[65] National Conference of State Legislators, available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[66] *See, e.g.*, California Governor Edmond G. Brown, Jr., "State of the State Address," Jan. 24, 2013, available at http://gov.ca.gov/news.php?id=17906. In his speech, Governor Brown refers specifically to the areas of climate change, health care, jobs, education and transportation, asserting that "The rest of the country looks to California." *Id.*

[67] California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), available at http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=.

[68] *See, e.g.,*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] "Our Office," New York State Office, Attorney General, available at http://www.ag.ny.gov/our-office.

[73] "CYBERCRIME NEWS," May – June 2015 Issue, National Association of Attorneys General Training & Research Arm, available at http://www.naag.org/assets/redesign/files/nagtri-PDF/cybercrime/Cybercrime-May-June-2015-Issue.pdf.

[74] *Id.*

[75] *Id.*

[76] Emily Glazer, "State Attorneys General Investigating J.P. Morgan Summer Cyber Breach," WSJ, Oct. 3, 2014, available at http://www.wsj.com/articles/state-attorneys-general-investigating-j-p-morgan-summer-cyber-breach-1412363262.

[77] Target Corporation, SEC Form 10-K, March 14, 2014, pages 16-17, available at http://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm#sE677C3BE093238F09058B8F76DDE1AA1.

[78] The Home Depot, Inc., SEC Form 10-K, pages 18-19, March 25, 2015, available at http://www.sec.gov/Archives/edgar/

data/354950/000035495015000008/hd-212015x10xk.htm#s301FBDE93E5897A646E64F74E64E6BC1.

[79] *Aswad Hood, on behalf of himself and all others similarly situated vs. Anthem, Inc., Blue Cross of California and Anthem Blue Cross Life and Health Insurance Company*, page 2, Class Action Complaint, Case 2:15-cv-00918-CAS-PLA, U.S. District Court, Central District of California, Filed 02/09/15, available at http://www.girardgibbs.com/blog/wp-content/uploads/Anthem-Data-Breach-Class-Action-Lawsuit-Girard-Gibbs-LLP.pdf.

[80] *Dennis Palkon et al. v. Stephen P. Holmes et al.*, pages 1-3, Case number 2:14-cv-01234, U.S. District Court, District of New Jersey, Filed 05/02/14, available at http://www2.bloomberglaw.com/public/desktop/document/PALKON_v_HOLMES_et_al_Docket_No_214cv01234_DNJ_Feb_27_2014_Court_.

[81] Securities Exchange Act Sections 12 (a) and (g)(1)(A) and 15 (d) (1), available at http://www.sec.gov/about/laws/sea34.pdf.

[82] "What is the difference between private equity and venture capital?" Investopedia, available at http://www.investopedia.com/ask/answers/020415/what-difference-between-private-equity-and-venture-capital.asp.

[83] Madison Marriage, "Gender diversity: a hidden problem," July 15, 2015, Financial Times, p. 6.

[84] *See, e.g.*, "Meeting your fiduciary responsibilities," U. S. Department of Labor (ERISA), available at http://www.dol.gov/ebsa/publications/fiduciaryresponsibility.html.

[85] Investment Advisers Act of 1940, codified at 15 U.S.C. §§ 80b-1- 20, available at http://www.sec.gov/about/laws/iaa40.pdf.

[86] "The Laws that Govern the Securities Industry," SEC, available at http://www.sec.gov/about/laws.shtml#invadvact1940.

[85] *See, e.g.*, Speech by SEC Chairman: Opening Statement at SEC Open Meeting: Dodd-Frank Act Amendments to the Investment Advisers Act, June 22, 2011, available at http://www.sec.gov/news/speech/2011/spch062211mls-items-1-2.htm.

[86] E. Eric Rytter, "New Trends and Challenges Facing Private Equity and Venture Capital Investors," in *Understanding Legal Trends in the Private Equity and Venture Capital Market* 56 (2015 ed.).

[87] Rich Steeves, "Cybersecurity a top concern for general counsel," quoting Paul Williams, office managing partner at Major, Lindsey & Africa, September 10, 2013, Inside Counsel, available at http://www.insidecounsel.com/2013/09/10/cybersecurity-a-top-concern-for-general-counsel.

[88] Delaware General Corporation Law, Section 141 (a). See also, Model Business Corporation Act (MBCA) (2006), Section 8.01 (b), providing that "All corporate powers shall be exercised by or under the authority of, and the business and affairs of the corporation managed by or under the direction of, its board of directors …."

[89] *See, e.g., Stanziale v. Nachtome (In re Tower Air, Inc.)*, 416 F.3d 229, 238 n. 12 (3d Cir. 2005).

[90] While the question of who has "standing" to sue directors and officers based on breaches of fiduciary has been somewhat complicated in recent years, the two categories with clear, historic entitlement are shareholders and the corporation (including through corporate representatives). *See, e.g.*, Marc J. Carmel, G. Alexander Bongartz & Mark Poerio , "Advice for directors and officers of distressed corporations: Fiduciary duties," Inside Counsel, June 26, 2015, available at http://www.insidecounsel.com/2015/06/26/advice-for-directors-and-officers-of-distressed-co?page=3.

[91] In the non-profit organizational area, courts and commentators often include a fiduciary duty of "obedience." *See, e.g.*,

[92] American Law Institute (ALI) *Principles of Corporate Governance, Section 4.01(a)*.

[93] *See, e.g.*, Brehm v. Eisner, 746 A.2d 244, 256 (Del. 2000).

[94] *Cramer v. General Telephone & Electronics Corp.*, 582 F.2d 259, 274 (3d Cir. 1978).

[95] *See, e.g., Smith v. Van Gorkom*, 488 A. 2d 858 (Del. 1985).

[96] *See, e.g., Cramer v. General Telephone & Electronics Corp.*, 582 F.2d 259, 274 (3d Cir. 1978).

[97] *Cede & Co. v. Technicolor, Inc.*, 634 A.2d 345, 361 (Del. 1993), modified, 636 A.2d 956 (Del. 1994).

[98] *Guft v. Loft*, 5 A.2d 503, 510 (Del. 1939).

[99] *In re Caremark Intern. Inc. Derivative Litigation*, 698 A.2d 959, ____ (Del. Ch. 1996).

[100] *Id.*

[101] *Stone v. Ritter*, 911 A. 2d 362 (Del. 2006). *Stone*, 911 A.2d at 370.

[102] *Caremark*, 698 A.2d at 967, quoted in Stone, 911 A.2d at 372.
[103] Delaware General Corporation Law (DGCL), Title 8, § 141 (e.,

[104] *See, e.g.*, Del. Gen. Corp. Law Sec. 102(b) (7); Virginia Corporations Code Sec. 13.1-690.

[105] *See, e.g.*, Marciano v. Nakash, 535 A.2d 400, 1987 Del. LEXIS 1312 (Del. 1987).

[106] *See, e.g.*, Del. Gen. Corp. Law Sec 145; Model Bus. Corp. Act Secs. 8.50-8.59; Cal. Corp. Code Sec. 317.

[107] *See, e.g.*, Melvin Aron Eisenberg & James D. Cox, Corporations and Other Business Organizations 490-92 (2011).

[108] *Stone*, 911 A.2d at 371

[109] Securities Act of 1933, Section 11.

[110] People ex rel. Madigan v. Tang, 346 Ill. App. 3d 277 (2004).

[111] *Id.* at 289.

[112] IU/Hanover article

[113] *See*, ABA Legal Task Force website, available at http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html.

[114] "Cybersecurity Legal Task Force: Resolution and Report to the ABA Board of Governors," November 2012, available at http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf.

[115] *Id.*

[116] *Id.*

[117] *Cybersecurity: Boardroom Implications*, 2014, NACD, available at https://www.nacdonline.org/applications/secure/?FileID=88578.

[118] *Id.* at 6-7.

[119] *Cyber-Risk Oversight Handbook*, NACDJune 10, 2014, available at https://www.nacdonline.org/Cyber.

[120] *Id.* at 3.

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

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] "Best Practices for Victim Response and Reporting of Cyber Incidents" U.S. Department of Justice, April, 2015, available at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

[126] *Id.*

[127] *See*, "The Law of Cybersecurity & In-House Counsel," March 3, 2015, describing "Pearson's Cybersecurity Agenda for Corporate Counsel & Survey Responses," available at http://michaelpower.ca/2015/03/the-law-of-cybersecurity-in-house-counsel/.

[128] Rich Steeves, "Cybersecurity a top concern for general counsel," quoting Sherrie Farrell, office managing partner, Detroit and Diversity Committee Chair, Dykema,, September 10, 2013, Inside Counsel, available at http://www.insidecounsel.com/2013/09/10/cybersecurity-a-top-concern-for-general-counsel.

ABOUT THE AUTHORS

PERRY E. WALLACE

Professor Perry E. Wallace received his undergraduate degree in electrical engineering and engineering mathematics from the Vanderbilt University School of Engineering. He received his law degree from Columbia University, where he was awarded the Charles Evans Hughes Fellowship. He is a tenured Professor of Law at the Washington College of Law of the American University, where he teaches corporate, environmental and international law.

Professor Wallace was for several years a senior trial attorney at the United States Department of Justice, handling cases involving environmental and natural resources law. He has also served as a securities and commercial arbitrator. Professor Wallace has served on numerous boards, commissions and councils over the years, including the U.S. Environmental Protection Agency's National Advisory Council for Environmental Policy and Technology, the Environmental Working Group and the Academic Council of the Institute for Transnational Arbitration.

RICHARD SCHROTH

Dr. Richard Schroth is a trusted private advisor and thought leader to business around the globe. He is Executive Director of The Kogod Cybersecurity Governance Center at American University and an Executive in Residence. Honored as one of the Top 25 Consultants in the World by Consulting Magazine and his peers, Richard is the Managing Director of the Newport Board Group's Global Technology Strategy, Innovation and Cyber Practice and the Axon Global Cyber Alliance, where he actively leads world-class teams of cyber professionals and board level advisors seeking to minimize the serious nature of cyber risk.

Dr. Schroth is energetically engaged in the cutting-edge of global private sector cyber initiatives including areas of M&A cyber diligence, board policies for cyber risk and advanced cyber business strategy. He is a private confidant to Fortune 500 boards, executives, private equity firms, national professional associations and Economic and Trade Consular Offices. Richard is a full board member of the National Association of Corporate Directors, an NACD Board Leadership Fellow and member of the NACD Board Advisory Services where he leads strategy sessions with Boards on cyber and related risk issues around the world.

Former Senior United States Fulbright Scholar, Dr. Schroth was nominated as a Fellow in the American Academy of Arts and Sciences for his distinguished career and contributions to the US as a leading international consultant – thought leader in business, technology, and Cyber-Counter Intelligence. Dr. Richard Schroth received his Doctorate from Indiana University, a M.S. from the University of Illinois, post-bachelors work at Texas A&M and holds a B.S. from Western Illinois University. Dr. Schroth has been honored as The Distinguished Alumnus of all the universities where he has graduated.

WILLIAM DELONE

William DeLone is an Eminent Professor of Information Technology at the Kogod School of Business at American University and Executive Director of the Kogod Cybersecurity Governance Center. Professor DeLone earned a B.S. in mathematics from Villanova University; an M.S. in industrial administration from Carnegie-Mellon University; and a Ph.D. in Computers and Information Systems from the University of California, Los Angeles. His dissertation studied the successful use of computers and information systems by small businesses. He has served as Acting Dean, Senior Associate Dean, and Chair of the Department of Information Technology. He also served as Chair of American University's Strategic Planning Steering Committee.

Professor DeLone's primary areas of research include the assessment of information systems' effectiveness, risk and value, e-government and public value and the management of global software development Professor DeLone has been published in the top information systems journals. Professor DeLone has lectured and consulted on information systems at universities in London, Paris, Rome, Venice, Warsaw, Galway, Singapore, Kuwait, Leipzig & Saarbrucken in Germany, and Guatemala.

ACKNOWLEDGEMENTS

The Kogod Cybersecurity Center would like to recognize our sponsor FINRA, whose financial support made this report possible.

The authors would like to acknowledge the contributions of Israel Martinez, National Practice Partner of The Newport Board Group's Cyber Practice and CEO of Axon Global along with Patrick Von Bargen, co-founder of 38 North Solutions, who reviewed and commented on earlier versions of the report.

ADVISORY COMMITTEE

Ben Beeson,
Lockton

John Brady,
FINRA

Dr. Erran Carmel,
Dean

Steve Cooper,
US Department
of Commerce

Jim Dinegar,
Greater Washington
Board of Trade

Donna Dodson (liaison),
NIST

Tracie Grella,
AIG

Bruce Hoffmeister,
Marriott International

John Honeycutt,
Discovery
Communications

Gary LaBranche,
Association of Capital
Growth

Scott Laliberte,
Protiviti

Israel Martinez,
Axon Global Services

Jim Messina,
The Messina Group

Hitesh Sheth,
Vectra Networks

Stuart Tryon,
U.S. Secret Service

Dr. David Swartz,
American University

Ralph Szygenda,
Senior Fellow

Leif Ulstrup,
Executive in
Residence

David S. Wajsgras,
Raytheon

KCGC LEADERSHIP

Dr. William DeLone,
Executive Director

Dr. Richard Schroth,
Executive Director

Dr. Gwanhoo Lee,
Director of Center Operations

Dr. Parthiban David,
Faculty Research Director

THIS PUBLICATION IS SPONSORED BY

FINRA

KOGOD SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC