DLA Piper Global Women's Leadership Summit
September 19-20, 2016
CLE Written Materials

Moderator
Stefanie Fogel, Co-Chair Boston Litigation, Chair Data Security Litigation Sub-Group and Information Governance, Co-Chair of the Food & Beverage Sector, DLA Piper LLP

Panelists
Clarissa Cerda, General Counsel, Pindrop Security, Inc.

Suzanne Rich Folsom, General Counsel, Chief Compliance Officer and Senior Vice President - Government Affairs, United States Steel Corporation

Sarah E. Morgenthau, Deputy Assistant Secretary for the Private Sector, US Department of Homeland Security

Kellye L. Walker, Executive Vice President and General Counsel, Huntington Ingalls Industries, Inc.

Panel Topic
Cyberattacks and Cyber Security: What Should a General Counsel Do?

I. COURSE OVERVIEW

Cyberthreats and cyber security have become key areas of focus for all companies and even government organizations. Protecting organizations from ever increasingly sophisticated hackers is essential to preserving a company's reputation and value. As a result, effective and pre-emptive collaboration between the legal department and those that have direct responsibility for managing and protecting an organization's information and technology systems have become a priority for in-house counsel.

This panel will discuss the role of the legal department in mitigating the risks of cyberattacks in an increasingly complex and global business environment. The panel will also discuss strategies and best practices in leading an organization through the various legal, business and regulatory issues in the aftermath of a cyberattack.

II. COURSE DISCUSSION

A. Evolving Risk Landscape

Cybercrimes are an ever evolving landscape. Cyberattackers are shifting from one-hit attacks to more

sophisticated, long-term operations. Staying current with the cybercrime trends is not a straight-forward endeavor

in today's global interconnected world. Now with new and increased use of technologies such as mobile devices, social media, and cloud computing and advancement of attackers' techniques, often evidencing skillful social engineering entwined with sophisticated long-term technical exploits, virtually all organizations and companies are potential targets. Indeed, even governments are not immune from such attacks. We know that cyberattacks can be extremely damaging to businesses, particularly if security is breached and confidential business and personal data compromised. Such attacks cost companies and taxpayers billions of dollars each year. With all of this in mind, company executives, including in-house counsel, face increasing pressure from boards of directors, shareholders and the general population to stay current and take all necessary precautions to prevent cyber security threats. Thus, managing cyber security risk has become a top priority for most global organizations and in-house counsel in particular. The panelists will discuss:

(1) The current cybercrime landscape and global legal trends in the development of laws and regulations.

(2) How the legal department can help companies effectively stay current with trending cyberthreats and at the same time implement repeatable and practical policies and procedures.

(3) Evolving trends in imposing liability and responsibility on individual employees, officers and directors, and board members as a result of cybercrime, as well as changes in reporting and disclosure obligations.

B. Cyber security Preparedness and Effective Cyber Compliance

Companies and government organizations should invest in data security controls and procedures to deter or prevent cyberattacks, but there is no single definition for what constitutes "reasonable" cyber security measures. This panel will discuss current benchmarks, standards and guidelines that companies can use as a framework to assess effective cyber security protection. This panel will explore the concept of "good" security programs versus "defensible" security programs.

C. Mitigating Risk and Exposure

In addition to an effective cyber security program focused on the prevention of intrusion, there are additional steps companies can take to further limit exposure and risk and to respond quickly and seamlessly in the event of a breach. This panel will address discuss best practices for the development, implementation and testing of customized and current incident response plans. Panelists will explore the importance of the following items to

mitigation risk and exposure:

- employee training and implementation of employee training programs;
- third-party vendor audits – how much is enough?;

- cyber security insurance policies and considerations for the selection of providers; and
- recovery and follow-up items after an attack

III. CONCLUSION/COURSE SUMMARY

Staying abreast of trends in the law and the schemes and targets of cyber criminals is not only recommended but is a necessity for all organizations. This risk is not unique to any particular industry, geography, business size, or public v. private company structures. The General Counsel is a critical strategist in identifying potential vulnerabilities and risks, developing and maintaining defensible cyber security programs, ensuring appropriate corporate governance and education, and meeting legal obligations in response and reporting. This panel will provide varied perspectives from industry and government as to how the General Counsel can and should provide the most effective support, guidance and recommendations to limit the risks raised by cybercrime.

CRR Supplemental Resource Guide

Volume 9

Training and Awareness

Version 1.1

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0003284

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Supplemental Resource Guide series! This document was developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP). It is the ninth of 10 resource guides intended to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).[1] The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *operational resilience* for IT operations. Operational resilience indicates the organization's ability to adapt to risk that affects its core operational capacities.[2] It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations as well as times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but are useful to any organization interested in implementing or maturing operational resilience capabilities for critical IT services.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. **Training and Awareness** ⇦***This guide***
10. Situational Awareness

The objective of the CRR is to allow organizations to measure the performance of fundamental cyber security practices. DHS introduced the CRR in 2011. In 2014 DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state

5. communicate among internal and external stakeholders about cybersecurity risk

The CRR Self-Assessment Package includes a correlation of the practices measured in the CRR to criteria of the NIST CSF. An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

Each resource guide in this series has the same basic structure but can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one resource guide will be able to make use of complementary materials and suggestions to optimize their adoption approach. Stakeholders identified in the implementation of other domains may also be stakeholders in training and awareness. Training and awareness can be used to support and reinforce the implementation of the other nine domains. For example, in incident management, training provides the incident response team with the understanding of how the team works together to respond to incidents; in controls management, awareness activities inform staff of newly deployed controls such as new password requirements.

Each guide derives its information from best practices described in a number of sources, but primarily from the CERT®-Resilience Management Model (CERT®-RMM).[3] The CERT-RMM is a maturity model for managing and improving operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute (SEI). This model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational risk management activities
- define maturity through capability levels
- enable maturity measurement against the model
- improve an organization's confidence in its response to operational stress and crisis

The CERT-RMM provides the framework from which the CRR is derived—in other words, the CRR method bases its goals and practices on the CERT-RMM process areas.

This guide is intended for organizations seeking help in establishing a training and awareness process. To outline this process, this document will use an approach common to many organizations. The process phases described include

- create a training and awareness plan
- assess training and awareness needs
- conduct training and awareness activities
- improve training and awareness capability

More specifically this guide

- educates and informs readers about the training and awareness process
- promotes a common understanding of the need for a training and awareness process
- identifies and describes key practices for training and awareness
- provides examples and guidance to organizations wishing to implement these practices

® CERT® is a registered mark owned by Carnegie Mellon University.

Additionally, Appendix B provides a mapping between the practices that constitute the Training and Awareness domain in the CRR and the appropriate Function, Category, and Subcategory in the NIST CSF.

The guide is structured as follows:

I. Introduction—Introduces the *CRR Resource Guide* series and describes the content and structure of these documents.

II. Training and Awareness—Presents an overview of the training and awareness process and establishes some basic terminology.

III. Plan for Training and Awareness—Highlights the elements necessary for an effective training and awareness plan.

IV. Assess Training and Awareness Needs—Presents an approach for identifying cybersecurity-related skills needed for specific roles (administrators, technicians, etc.) and cybersecurity awareness needs for staff throughout the organization.

V. Conduct Training and Awareness Activities—Outlines a process that defines the steps necessary to manage, develop, schedule, and conduct training and awareness activities.

VI. Improve Training and Awareness Capability—Provides an approach for evaluating and improving training and awareness capability.

VII. Conclusion—Highlights the key points from this guide and provides contacts and references for further information.

Appendices

A. Training and Awareness Resources
B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Audience

The principal audience for this guide includes individuals responsible for designing, managing, or conducting training and awareness. Executives who establish policies and priorities for training and awareness, managers and planners who are responsible for converting executive decisions into plans, and staff responsible for implementing the plans and conducting training and awareness activities can also benefit from this guide.

To learn more about the source documents for this guide and for other documents of interest, see Appendix A.

II. Training and Awareness

Overview

Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization's operational cyber resilience requirements and goals are known and used. The process depicted in Figure 1 helps the organization ensure that the training and awareness process supports the organization's cyber resilience objectives. This guide focuses on the training and awareness activities that make staff members aware of their role in the organization's cyber resilience concerns and policies. Staff members also receive specific training to enable them to perform their roles in managing organizational cyber resilience. Though this guide focuses on training and awareness for cyber resilience activities, these activities should integrate with and support the organization's overall training and awareness program. If the organization already has training or awareness programs, it is important that they include cyber resilience. Existing programs can use their established information gathering processes, building capabilities, evaluation methods, record keeping, and improvement activities to support cyber resilience training and awareness.

The training and awareness domain focuses on general awareness, skill building, and ongoing training.[4]

Figure 1: The Training and Awareness Process

In this guide, *training* refers to a set of activities that focuses on staff members learning the skills and gaining the knowledge needed to perform their roles and responsibilities in support of their organization's resilience program. Awareness activities focus on staff members developing an understanding of resilience issues, concerns, policies, plans, and practices. The high-level outline below highlights the main areas of this domain and points the reader to the corresponding details in this guide.

The following sections detail each of the steps in the training and awareness process.

Training and Awareness Process

Plan for Training and Awareness

Training and awareness is a support process that ensures staff members have the knowledge and skills to perform their work, including work in other processes such as incident management, controls management, and risk management. Training and awareness typically takes place at various levels of an organization. Enterprise training and awareness addresses organization-wide needs. Specific training and awareness activities are typically developed and implemented at the organizational level (e.g., business unit or team) where they are needed. For training and awareness at any level of the organization, management support is essential. With management support, processes are defined to identify, implement, and assess training and awareness on an ongoing basis to ensure skilled employees can provide resilient services.

Planning for training and awareness is essential for a successful program. The plan documents the program objectives, strategy for achieving those objectives, and the infrastructure and resources needed to execute the plan.

Important activities while planning for training and awareness include the following:

- Obtain support for training and awareness planning.
- Establish a training and awareness program strategy.
- Establish an approach to building a training capability.
- Establish an approach to building an awareness capability.

Assess Training and Awareness Needs

The identification of training and awareness needs provides critical information for the development of a training and awareness program. If the organization has an established training and awareness program, there may already be a needs analysis process in place. Still, the organization should review the previously identified needs to ensure they include those specific to cyber resilience and, periodically, to see if any of the needs have changed.

Training and awareness needs specific to cyber resilience can be derived from other domain plans (e.g., controls management and risk management). Those plans include a list of critical skills needed to perform the planned work. Job descriptions also provide information on skills and knowledge needed to perform a particular job. As the organization assigns roles to staff, it should identify any gaps in skills and knowledge as training needs. It should also review domain plans to identify the activities needed to educate staff members about the organization's cyber resilience concerns, which inform the organization's awareness needs. Once training and awareness needs are identified, an organization must analyze those needs to determine what actions it will take to resolve the gaps.

Important activities for identifying training and awareness needs include the following:

- Obtain support for training and awareness needs assessment.
- Establish a strategy for identifying training needs.
- Establish a strategy for identifying awareness needs.
- Establish a process for training and awareness needs analysis.

Training needs are the documented gaps between current skills of people assigned to roles and the skills they need to effectively perform the role's work. Awareness needs are the communications capabilities that an organization needs to inform staff of cyber resilience concerns.

Conduct Training and Awareness Activities

Building capability and conducting training and awareness activities usually involve engaging multiple levels of the organization as well as third-party providers. Cyber resilience efforts should be incorporated into any existing training and awareness program and evaluated for effectiveness. Establishing capability for cyber resilience training and awareness includes identifying and developing the program's educational vehicles (courses, presentations, etc.). Each organization will have unique needs for cyber resilience training and awareness that must be addressed with activities developed specifically for the organization, as well as common needs that can be met by third-party providers.

Important activities for building capability and conducting training and awareness include the following:

- Establish and maintain support functions for training and awareness (e.g., library for storing materials and a record tracking system).
- Develop training and awareness materials.
- Procure third-party provider services.
- Conduct training and awareness activities.

Improve Training and Awareness Capability

In the evaluation and improvement phase of the training and awareness process, the organization should evaluate existing training and awareness activities against the organization's objectives. If the activities are not meeting their objectives, then the organization must initiate improvement actions. Improvements to the training and awareness activities, based on the analysis of the collected data, should support the achievement of organizational objectives.

To be effective, training and awareness activities must be meaningful to both the employee and the organization. Evaluators must plan ahead to collect sufficient data to examine the effectiveness of the activities and recommend improvements to be incorporated in the next cycle. The data collected should allow the analysis of the programs against four desired outcomes:

- Employees are better able to perform their jobs.
- Supervisors are better able to assess changes to their employees' on-the-job performance.
- The organization feels confident that the employees are performing activities in a way that demonstrates a resilient organization (e.g., meets the goals and objectives).
- The training and awareness activities can be improved.

Evaluation requires the collection of data and observations throughout the organization's training cycle. Evaluation and analysis of training and awareness programs should occur at an organizationally defined

frequency to support the incorporation of updated material and synchronization with the execution of the training and awareness plan.

Important activities in the training and awareness assessment process include the following:

- Establish a plan to evaluate the training and awareness program.
- Evaluate the training and awareness program and analyze results.
- Improve the process.
- Update training and awareness materials.

Summary of Steps

The following sections of this guide lay out the discrete steps for developing a plan to implement the training and awareness process as described above:

Plan for Training and Awareness

1. Obtain support for training and awareness planning.
2. Establish a training and awareness program strategy.
3. Establish an approach to building a training capability.
4. Establish an approach to building an awareness capability.

Assess Training and Awareness Needs

1. Obtain support for training and awareness needs assessment.
2. Establish a strategy for identifying training needs.
3. Establish a strategy for identifying awareness needs.
4. Establish a process for training and awareness needs analysis.

Conduct Training and Awareness Activities

1. Establish and maintain support functions for training and awareness.
2. Develop training and awareness materials.
3. Procure third-party provider services.
4. Conduct training and awareness activities.

Improve Training and Awareness Capability

1. Establish a plan to evaluate the training and awareness program.
2. Evaluate the training and awareness program and analyze results.
3. Improve the process.
4. Update training and awareness materials.

Organizations that already have a training and awareness program can assess and improve it by using the guidance in this resource guide.

III. Plan for Training and Awareness

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin developing a training and awareness program.

	Input	Guidance
✓	Scoping statement	This statement defines what the training and awareness program and plan need to address. Training and awareness should cover, at a minimum, all critical organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their mission. This approach may allow an organization to address the areas of greatest risk first and mitigate their impact while training and awareness objectives are being defined for noncritical areas. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix B for a cross-reference between the CRR and this guide.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • legal • human resources • third-party providers (e.g., training vendors) • training and awareness program staff • compliance personnel
✓	Management support	Sponsorship by senior management is necessary for establishing a training and awareness program and implementing processes. This should include the appropriate funding and resources to implement the activities described in this guide as well as support and oversight to ensure that these activities are aligned with the other activities in the organization.
✓	An understanding and acknowledgement of an acceptable approach to training and awareness	Acknowledgement from management for the intended approach to training and awareness, including stakeholder expectations about acceptable risk tolerance for the identified critical assets and services, is required.
✓	Externally imposed requirements for training and awareness	Regulatory requirements define mandatory training and awareness, certifications, qualifications, and other needs (this includes service-level agreement requirements).
✓	List of critical services	To properly develop a training and awareness program, the critical services in the organization need to be identified.
✓	Risks	Obtain the list of categorized and prioritized risks. Risks change over time, so it is important that the updated list is provided when risks change.
✓	Assignment of responsibility for training and awareness	Job descriptions for roles that have responsibilities for training and awareness should reflect those responsibilities (for example, executive ownership, planning, development of training and awareness capability, and delivery of training and awareness).

	Input	Guidance
✓	Budget for training and awareness	Identify the available funds to perform training and awareness planning and execution, including • staffing resources • tools (applications and associated hardware) • third-party support

Step 1. Obtain support for training and awareness planning.

Obtaining support from management is essential to ensuring the training and awareness plan is effectively implemented. A top-down approach is often helpful in ensuring the training and awareness program meets the resilience objectives of the organization.

The level of management support required depends on the scope of the training and awareness program being implemented. Senior-executive-level support is necessary for a training and awareness plan that addresses the entire organization. Smaller implementations, such as those at the service level, may require sponsorship only from management responsible for that particular service. To illustrate, consider an electric utility company that has four main services: generation, transmission, distribution, and business support. A training and awareness program could be implemented for these services individually. When the scope is limited to a single service or component of an organization, the involvement and support of the organization's senior management may be limited, and more involvement might be required from management within the individual service or component.

Initially, training and awareness planning is usually iterative. As the other phases of the training and awareness process are completed (needs assessment, conducting training and awareness, and improvement), the plan will need to be reviewed and revised. Eventually, training and awareness planning might be done more periodically.

Step 2. Establish a training and awareness program strategy.

A training and awareness program should be developed to reflect priorities at the enterprise and operating-unit levels as well as for specific critical services. The following steps illustrate an approach for establishing objectives for a training and awareness program:

A. **Identify management directives and organizational priorities.** Organizational priorities can be articulated in many forms and help identify the strategic objectives. Strategic objectives are derived from strategic planning activities, which usually forecast two to five years out.[5] The following sources can provide insight into management directives and organizational guidelines:
   - strategic plan—The document in which an organization defines its plans for achieving its mission, where the organization wants to go, and how it plans on getting there.[6] Large enterprises may have strategic plans at multiple levels within the organization, such as the enterprise and operating-unit levels.
   - critical success factors (CSFs)—A small number of areas in which an organization must consistently perform well to meet its goals and mission.[7] CSFs illustrate what the organization considers its top priorities in achieving its goals.

- legal and regulatory obligations—Obligations that often give insight into requirements placed on the organization by external entities.[8]
- internal policies and standards—Policies and procedures developed by the organization to promote acceptable behaviors and practices.[9]

B. Define and document training and awareness program objectives. Training and awareness program objectives are derived from the management directives and organizational priorities identified above.

C. Prioritize training and awareness program objectives. Training and awareness program objectives should be prioritized based on their potential to affect operational resilience.[10] This will help the organization determine the allocation of resources, such as the number of staff members requiring training and types of training and awareness activities (e.g., in-house or vendor-supplied).

The resources available to an organization for training and awareness will influence the strategy selection. The training and awareness program strategy should

- focus on increasing the cyber resilience of critical services
- align with the organization's strategic objectives

The purpose of a training and awareness program is to identify specific activities that can implement and support the training and awareness objectives.

The following steps illustrate an approach for integrating training and awareness objectives specific to cyber resilience in an existing training and awareness program:

A. Review the existing activities before implementing new training and awareness program activities. This will ensure new training and awareness activities are not redundant.

B. Review existing training and awareness program activities to determine if they are still effective. This review is often completed as a by-product of auditing or feedback and measurement activities. A training and awareness program activities assessment should provide sufficient evidence to determine the effectiveness of the implemented training and awareness program activities.

C. Establish new training and awareness program activities to fill the gaps between existing activities and needed ones. (See Section VI, Steps 2 and 3 for more information on identifying training and awareness needs.)

D. Confirm existing and updated training and awareness program activities are still relevant, and assign responsibility for implementation of new activities. Responsibility for ensuring that training and awareness program activities are implemented typically rests with the operating-unit managers.

To put training and awareness program activities into perspective, consider a large enterprise with multiple operating units consolidated onto one campus. The activities will likely be controlled by one operating unit responsible for the training and awareness program activities affecting the critical services. Because the other operating units share the facility, they can participate and benefit from the same training and awareness program activities.

Step 3. Establish an approach to building a training capability.

When establishing its approach to building a training capability, the organization needs to consider the types of training needed and how that training will be sourced. Will it be developed in-house or procured from a third-party provider? Most training programs use a combination of training options based on what best meets their training needs and are guided by the training strategy and objectives.

"Capabilities for implementing the training plan must be established and maintained, including the selection of appropriate training approaches, sourcing or developing training materials, obtaining appropriate instructors, announcing the training schedule, and revising the awareness capability as needed." CERT-RMM, p. 666

There are many different training approaches, including the following examples:

- classroom training
- guided self-study
- on-the-job training
- mentoring programs
- online training
- webinars and podcasts

Determining which approach to use depends on factors such as needed skills and knowledge, budget, audience, availability, and work environment. Classroom training provides a rich learning environment, but it is also expensive, and attendees must be available for the duration of the class. In contrast, on-the-job training provides hands-on skill development in the learner's work environment, though with the potential drawback of incomplete or inconsistent training opportunities. All of the approaches require attention to learning objectives and the training materials that support them.

Step 4. Establish an approach to building an awareness capability.

The overlap between building a training capability and an awareness capability is often minimal, so it is important to define the approaches separately.

"Establishing a capability for implementing the awareness plan requires the selection of appropriate awareness approaches, sourcing or developing awareness materials, obtaining appropriate awareness facilitators or instructors (if needed), delivering internal communications about awareness activities, and revising the awareness capability as needed." CERT-RMM, p. 658

Below is a list of example approaches:

- poster campaigns
- newsletters
- email messages
- presentations at organization-wide or team meetings
- trainer-facilitated sessions
- informal sessions (e.g., brown bag lunches, webinars, conferences)

As the training and awareness plan documentation matures, the organization needs to address a few questions about building an internal organizational infrastructure to support the implementation of the plan, presented in Table 1.

Table 1: Training and Awareness Planning Questions

Can you answer YES?	Questions
	Do we know what roles/positions we need filled now?
	Do we know what roles/positions we would like to have?
	Do we have a good account of the team's capabilities (skills, training)?
	Do we have actual job descriptions for every role we need to grow?
	Do we have training events/resources in our budget and on our calendar?
When you answer all of these as YES!—then you can feel comfortable that you have a plan.	

Once your organization has documented its training and awareness plan, standards, and guidelines, it should review and update them periodically (at least annually or as required by other guidelines) and as driven by events (e.g., critical service change, significant organizational changes) to ensure they are achieving the desired results.

Output of Section III

	Output	Guidance
✓	Management directives and guidelines	Management directives and guidelines should be clearly identified.
✓	Training and awareness program objectives	Using the management directives and guidelines, training and awareness program objectives should be defined.
✓	Training and awareness program activities strategy	Organizations should identify the appropriate mix of training and awareness program activities to achieve the program objectives.
✓	Approach to building a training capacity	Training capability that meets the training objectives is identified.
✓	Approach to building an awareness capability	Awareness capability that meets the awareness objectives is identified.
✓	Training and awareness plan	Training and awareness strategy and objectives are documented with the initial approach for implementation and identified resources needed.

IV. Assess Training and Awareness Needs

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin assessing training and awareness needs.

	Input	Guidance
✓	Scoping statement	This statement defines the boundaries of the training and awareness needs assessment. The assessment should cover critical organizational services. Organizations that are not sure where to start should focus on the most essential services and the areas that directly affect their mission. If your organization has participated in a CRR, it may be beneficial to begin with the critical service addressed during the CRR. See Appendix B for a cross-reference between the CRR and this guide.
✓	List of stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • human resources • managers of resilience management activities (e.g., incident management, controls, situation awareness, service continuity) • managers of the critical services
✓	Management support	Senior management should provide an endorsement for conducting a training and awareness needs assessment.
✓	Assignment of responsibility for training and awareness needs assessment	Job descriptions for roles that have responsibilities for training and awareness (for example, executive ownership, human resources, training and awareness program personnel) should clearly state those responsibilities. Also, the training and awareness responsibilities of managers of critical services and managers of cyber resilience activities should be clearly defined.
✓	Budget for training and awareness needs assessment	Identify available funds to perform a training and awareness needs assessment, including • staffing resources • tools (applications and associated hardware) • third-party support, if needed

Step 1. Obtain support for training and awareness needs assessment.

Obtaining support from management is essential to ensuring that the training and awareness needs assessment is effectively conducted. The level of management support required depends on the scope of the needs assessment being conducted. When the scope is limited to a single service or component of an organization, the involvement and support of the organization's senior management may be limited, and more involvement might be required from officials within the individual service or component.

Step 2. Establish a strategy for identifying training needs.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Cyber security awareness and training programs are established.	
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	**PR.AT-1: All users are informed and trained**
3. Are skills gaps present in personnel responsible for cyber security identified? [OTA: SG3.SP1]	**PR.AT-1: All users are informed and trained**

Training needs are derived by identifying the skills and knowledge required to perform the necessary work and comparing them to the current skills and knowledge capabilities of the assigned personnel. Any gaps that prevent personnel from effectively performing their work are identified as training needs. If the organization has an established training program, there may already be a needs analysis process in place. Still, the organization should review the previously identified needs to ensure they include those specific to cyber resilience.

If the organization does not have a training program, then it should develop an approach for data collection and analysis. There are many ways to collect the necessary data, for example, document review (e.g., domain-related plans), surveys, interviews, questionnaires, user observation, workshops, exercises, brain storming, use cases, prototypes, and role playing. Using a variety of elicitation techniques may facilitate initial needs assessments. Once the needs are established, a simple review by key stakeholders will ensure that this is still an accurate picture of the needs.

One approach to identifying training needs specific to cyber resilience is to use domain-related plans (e.g., controls management plan, risk management plan). Those plans should include a list of critical skills and knowledge needed to perform the planned work. Job descriptions also provide information on skills and knowledge needed to perform a particular job. As the organization assigns roles to staff, it should identify any gaps in skills and knowledge as training needs. If plans or skills and knowledge information are not available, it may be necessary to gather training needs through interviews with managers responsible for the different aspects of the organization's cyber resilience efforts or from employee training and development plans.

Training needs are documented and accumulated across the organization, providing an overall picture of the number of people who need training in different skill and knowledge categories. This information is used in the analysis step (Section IV, Step 4).

Step 3. Establish a strategy for identifying awareness needs.

Unlike skills training, awareness efforts communicate a message to a broad group of employees with different skills and experience. The awareness message often conveys information about organizational goals, objectives, and critical success factors. The message can also provide employees with information that improves operational resilience (e.g., security and confidentiality guidelines, vulnerability and incident notices). Awareness needs are identified through multiple sources, such as

- resilience requirements
- organizational policies
- vulnerabilities under watch
- laws and regulations

- service continuity plans

In addition, plans for domain processes can be reviewed for awareness activities needed to provide staff members with an understanding of the organization's cyber resilience concerns. Another way to gather awareness needs information is to interview managers responsible for the different aspects of the organization's cyber resilience efforts.

It is also useful to identify different groups of people by the types of awareness information they need. For example, the general population of an organization may need information about organizational goals and objectives, and those responsible for responding to a service disruption will need information on changes to service continuity plans.

Documenting and accumulating awareness needs across the organization provides an overall picture of the extent of awareness activities to be conducted, as well as the different awareness categories (such as personnel groups or need for urgency). This information is used in the analysis step (Section IV, Step 4).

Step 4. Establish a process for training and awareness needs analysis.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Cyber security awareness and training programs are established.	
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	**PR.AT-1: All users are informed and trained**
4. Have training needs been identified? [OTA: SG3.SP1]	**PR.AT-1: All users are informed and trained**

The organization must analyze its training and awareness needs to determine how it will resolve the gaps and meet organizational goals. Table 2 and Table 3 outline an approach to analyzing training and awareness needs.

Table 2: Training Needs Analysis

Activity	Details
Compare required skills and knowledge and current skills and knowledge to identify gaps (training needs).	Review the identified training needs to determine if the program can meet them.
Categorize the training needs.	Example categories include • technical skills • process knowledge and skills • resilience knowledge
Create a table showing training needs by category and number of people needing the training.	Gain a better understanding of the extent of the training need across categories and the actual number of people needing the training.
Determine if the training activity is the responsibility of a specific group or is organization-wide.	There are times when a training need may be specific to a group or even just one team. In those cases, the group or team will have the responsibility to meet that need.
Determine the priority of the identified training needs.	Criteria for prioritizing could include • criticality of the skill or knowledge for delivering the service(s) • number of people who already have the skill or knowledge vs. those who need it (depth of skill or knowledge in the organization) • total number of people who need the skill or knowledge
Create a list of prioritized training needs.	

Table 3: Awareness Needs Analysis

Activity	Details
Review identified awareness needs.	Review the identified awareness needs to determine if the program can meet them.
Categorize the awareness needs.	Example categories include • resilience requirements • organizational policies • vulnerabilities under watch • laws and regulations • service continuity plans
Create a table showing awareness needs by category and personnel groups.	Gain a better understanding of the extent of the awareness need across personnel groups as well as categories of awareness needs of the different personnel groups.
Determine if the awareness activity is the responsibility of a specific group or is organization-wide.	There are times when an awareness need may be specific to a group of personnel or even just one team. In those cases, the group or team will have the responsibility to meet that need.
Determine the priority of the identified awareness needs.	Criteria for prioritizing could include • criticality of the awareness information for delivering the service(s) • risks associated with personnel not being aware of the needed information • total number of people who need to be exposed to the awareness information
Create a list of prioritized awareness needs.	

Output of Section IV

	Output	Guidance
✓	Identified training needs	• Table of training needs showing categories and number of personnel needing the training • List of training needs ordered by priority
✓	Identified awareness needs	• Table of awareness needs showing categories and personnel grouping • List of awareness needs ordered by priority
✓	Recommended training and awareness actions	• List of recommended training and awareness actions

V. Conduct Training and Awareness Activities

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin conducting training and awareness activities.

	Input	Guidance
✓	Training and awareness plan	• What were the goals and objectives of the plan, and what is the expected timeline?
✓	Identified training needs	• Table of training needs showing categories and number of personnel needing the training • List of training needs ordered by priority
✓	Identified awareness needs	• Table of awareness needs showing categories and personnel grouping • List of awareness needs ordered by priority
✓	Recommended training and awareness actions	• List of recommended training and awareness actions

Step 1. Establish and maintain support functions for training and awareness.

If the organization has an established training program, there may already be training and awareness support functions in place. If not, then the organization needs to establish certain support functions. First, a library structure needs to be created for storing training and awareness materials. The structure should allow for versioning of materials such as presentations and internally developed course materials (course modules, handouts, exercises, etc.).

Also, the organization should establish a tracking and record-keeping system. Training and awareness records could include

- course or training activity with date conducted
- course or training activity attendees
- course instructors
- awareness activities with date conducted, completed, or disseminated
- personnel attending awareness activity (if a presentation)
- employee training records

In addition, a tracking mechanism for tracking progress against the planned training and awareness activities needs to be in place.

Other support functions include

- logistical functions, such as email distribution lists, classroom scheduling, and instructor scheduling systems
- measurement and evaluation activities (see Section VI)

Step 2. Develop training and awareness materials.

The organization can use the lists of prioritized training and awareness needs to plan how those needs will be met. Training can be accomplished through several different approaches, such as

- classroom training
- guided self-study
- on-the-job training
- mentoring programs

In addition to determining the approach to use, the organization needs to decide whether it will acquire the training through a third-party provider or develop the training itself. Although many training needs can be met through third-party providers, certain organization-specific training (such as process-related training) should be developed internally.

Similarly, awareness activities can be accomplished through several different approaches, such as

- poster campaigns
- newsletters
- email messages
- presentations for organization-wide or team meetings
- trainer-facilitated sessions

Again, the organization needs to decide whether it will acquire third-party services to support the awareness activities or do the work in-house. If the organization decides to develop training and awareness materials in-house, it is recommended that the organization follow a development approach. Table 4 shows an example development approach.

Table 4: Example Training and Awareness Materials Development Approach

Development Item	Purpose
Product Plan	Documents the need for the training or awareness material, intended audience, materials needed, resources needed, and development and delivery constraints
Product Design	Documents a high-level design and a list of the elements that need to be developed (e.g., for a course, presentation materials, exercises, handouts)
Training or Awareness Materials	Specifies materials developed to conduct the training or awareness activity
Verification & Validation of Materials	Defines tests, pilots, prototypes, or other activities to make sure the materials are ready for full-scale production and deployment
Disposal/Sustainment	Explains the removal of items once they have been updated or are no longer useful to your organization

Initial planning for the development of training and awareness materials can reduce the amount of rework caused by uncertain requirements early in the development cycle.

Step 3. Procure third-party provider services.

When an organization decides to use third-party providers to develop or deliver training or awareness activities, it should ensure that the training or awareness activities delivered address the needs of the organization and are of the quality expected. Also, the organization needs to establish an agreement with that supplier. This may be as simple as a license fee or a registration fee for attending a course, or it may be more complex and require a more formal contract agreement.

Step 4. Conduct training and awareness activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2:SP1]	**PR.AT-1: All users are informed and trained**
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	**PR.AT-1: All users are informed and trained**

Training and awareness activities need to be scheduled. For a class, it is best if the schedule provides at least a three-month lead time before an actual activity is conducted. This allows time to prepare materials, prepare instructors, arrange logistics, and settle attendee availability. Other activities also need to be scheduled to ensure that the activity developer is available and that materials production is completed. When scheduling activities, consider other scheduled organizational activities, holidays, and potential vacations or other staff absences. Training activities and awareness activities can be conducted through significantly different approaches (from classroom training to email messages), which can allow for some flexibility in scheduling to meet situational needs.

The conduct of training and awareness activities should be tracked against the plan and scheduled to ensure the training and awareness objectives are met. Evaluation of training and awareness activities provides feedback on their effectiveness. See Section VI, Improve Training and Awareness Capability, for a discussion on evaluation techniques and analysis.

Outputs of Section V

	Output	Guidance
✓	Tracking records and material	• Materials used, personnel trained, and initial feedback
✓	Product development artifacts	• Materials used to develop the training and awareness products
✓	Training and awareness activity materials	• Materials that are used to conduct the training and awareness activities
✓	Training and awareness activities schedule	• Schedule of when training and awareness activities are conducted

VI. Improve Training and Awareness Capability

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin assessing training and awareness.

	Input	Guidance
✓	Training and awareness plan	What were the goals and objectives of the plan?
✓	Tracking records and material	What materials were used, who was trained, and what was the initial feedback?
✓	Interviews with employees and supervisors	What observations can the employee provide about the effectiveness of the training and awareness activity after the employee has performed the job?

Step 1. Establish a plan to evaluate the training and awareness program.

Evaluation of the training and awareness program should be planned for while the training and awareness program is being developed and its materials are being planned and designed.

Key personnel performing the evaluation should have the following responsibilities:

- developing the evaluation process and scope
- analyzing and assessing the training and awareness activities
- managing internal/external entities during the evaluation process
- summarizing the evaluation results

Stakeholders include

- owners of enterprise-level cybersecurity policies and procedures
- service or asset owners
- supervisors of employees with cybersecurity responsibilities
- external entities such as trainers and those developing training and awareness materials
- staff performing the work

Depending on the scope of the assessment, personnel performing the evaluation or stakeholders supporting it may require specialized training.

Artifacts and materials produced in the planning of training and awareness activities will support the evaluation of the overall program's effectiveness. The organization can also require data to be collected before and during these activities.

When evaluating the effectiveness of training and awareness activities, plan to collect measures that allow the examination of four specific aspects:

- the appropriateness of the learning conditions (in the employee's opinion)
- what, specifically, an employee was expected to learn from each training or awareness activity
- how the performance or behavior of the employee changed following specific training and awareness activities
- the effectiveness of a specific training and awareness activity compared to other options

Collection of this data will require access to those who plan and administer the training and awareness activities, the employees who will participate in those activities, and the supervisors who will select and evaluate the employees who will participate.

The data collected should enable the organization to analyze the program against four desired outcomes:

- Employees are better able to perform their jobs.
- Supervisors are better able to assess changes to their employees' on-the-job performance.
- The organization feels confident that the employees are performing activities in a way that demonstrates a resilient organization (e.g., meet the goals and objectives).
- The training and awareness activities can be improved.

Step 2. Evaluate training and awareness program and analyze results.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	PR.IP-7: Protection processes are continuously improved

Once the organization has developed a plan to collect the data needed to evaluate the training and awareness program, it should implement the plan. Data may be collected continuously or after discrete events, such as at the end of a class or presentation. But those evaluating the training and awareness plan should establish a schedule that supports the collection, consolidation, and analysis of data and enables Step 3 (Improve the Process).

Collect data.

Using the objectives that define training and awareness activities, those evaluating these activities organize the data to support a regular evaluation cycle. Recall that the previous step outlined the measures that support the analysis of the program. Data collected to support this analysis comes from four sources:

- the employees being trained
- the supervisors who identified the training shortfalls and can observe changes in employee behavior
- corporate leadership that establishes performance objectives to accomplish the organization's mission
- those who actually conduct the training and awareness activities

Table 5 lists the types of data that might be collected, describes the data, and suggests what the data might be used to determine.

Table 5: Evaluation Measures

Type of Data	Data Description	Data Determines…
Employee Satisfaction Survey (administered immediately after activity, responses on a scale of poor to excellent)	• Adequacy of learning environment • Adequacy of instructor/learning activity • Extent to which the employee was prepared	• Fulfillment of the conditions • Relevancy of training to employee • Adequacy of articulation of prerequisites for this training
Learning and Teaching Effectiveness (performance test just prior to successful completion of the course)	• Results of performance testing based on activity just completed	• Fulfillment of the training objectives • Appropriateness of the activity to the performance desired • Comparison to similar activities
Employee Performance Effectiveness (60-90 days after training and awareness activity)	• Structured questionnaire to evaluate before-and-after performance of tasks relevant to activity being evaluated • Measure of quantitative improvement • Measure of qualitative improvement	• Effectiveness of training and awareness activity • Efficiency gains toward meeting corporate objectives • Comparison to similar activities
Training and awareness program effectiveness	• Value of improvement due to training and awareness activities • Cost of training and awareness activities	• Improvements achieved by the organization • Allocation of resources for training and awareness activities

The organization must recognize that the evaluation process is an information-gathering process. The evaluations allow the organization to measure the effectiveness of training and awareness activities and will ultimately work to achieve organizational performance and efficiency objectives.

Identify weaknesses.

Evaluators should be looking for and documenting the weaknesses such as the following (for illustration only; these may not represent weaknesses in all organizations):

- conditions—Example: training was conducted using equipment that was no longer in the organization's active inventory.
- ineffective training activity—Example: employees are consistently unable to demonstrate skills by the end of the block of instruction.
- insufficient impact on employee behavior—Example: despite mandatory phishing awareness training, a significant percentage of employees falls victim to a simulated phishing email.

Leverage existing assessment results.

Evaluations should leverage existing documentation from other domains, such as the results of service continuity exercises, incident handling responses, and risk assessments. Looking back on existing documentation from these areas could give the organization useful insight on how training and awareness objectives have or have not been satisfied.

See the Service Continuity Resource Guide, Volume 6 of this series. Also see the Service Continuity (SC) process area in the CERT-RMM for additional information on conducting service continuity exercises.

See the Incident Management Resource Guide, Volume 5 of this series. Also see the Incident Management and Control process area in the CERT-RMM for additional information on handling incidents.

See the Risk Management Resource Guide, Volume 7 of this series. Also see the Risk Management process area in the CERT-RMM for additional information on managing risks.

Step 3. Improve the process.

Training and awareness capabilities must be kept current and up to date; the manner in which the training and awareness material is delivered must be effective in the eyes of those who are being trained.

The results of a completed evaluation will enable the organization to make informed decisions about improving the training and awareness plans and strategies. Once the organization has identified the problem areas, it can begin to identify updates to existing training and awareness activities and propose new activities.

Use the feedback loop.

As depicted in Figure 1 (page 4), an organization's evaluation of its training and awareness activities is an ongoing process. As technology and processes change, so must the training and awareness program. The organization must always assess these changes so it can properly manage decisions related to operational resilience.

The organization should leverage other domains during the feedback loop. Lessons learned from the deployment of other processes may yield training and awareness needs that will enable the organization to increase its operational resilience. Domains to consider include the following:

- incident management—As incidents are investigated, gaps in the training and awareness program will become known. These gaps should be discussed during the post-incident brief, and recommendations to improve the training and awareness program should be made.
- risk management—The organization's normal risk review sessions will reveal new risks. The revealed risks that can be mitigated by training should be fed into the training and awareness plan.
- service continuity—As disaster recovery and business continuity plans are developed and exercised, failures should be documented, and recommendations for new training and awareness objectives and activities should be fed into the training and awareness program.

The list above provides examples for the organization to consider. Domains not listed, however, can provide inputs to the training and awareness plan.

KEY TAKEAWAY: *The organization should always look to improve its operational cyber resilience by leveraging other domains and their outputs.*

Step 4. Update training and awareness materials.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – Awareness and training activities are conducted.	
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3, OTA:SG3.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	PR.IP-7: Protection processes are continuously improved

The final step in the evaluation process enables the organization to implement the updates and new training and awareness activities. The process outlined above provides the due diligence an organization needs in order to confidently assess the training and awareness program and make changes based on the evaluation.

As updates are made, it is important for the organization to schedule follow-on reevaluations to ensure that the updates and new activities are effectively achieving training and awareness objectives.

Output of Section VI

	Output	Guidance
✓	Evaluation report	• Outlines the areas below
✓	Evaluation of changes to on-the-job performance	• Contains changes reported by both employees and their supervisors
✓	Data	• Improves both learning and teaching
✓	Return on investment	• Supports resource allocation to the most effective training and awareness activities
✓	Review of material	• Maintains currency
✓	Remediation plans	• Ensures training and awareness objectives are satisfactorily addressed

VII. Conclusion

Establishing and supporting an ongoing training and awareness program enables your organization to meet its goals and objectives. The training and awareness program helps to ensure that your organization can sustain its critical services and meet its responsibility to its stakeholders and its contribution to national critical infrastructure.

The variety of documentation, standards, and guidelines developed to address training and awareness is extensive, but there are just a few straightforward foundational activities that these items share, such as establishing a training and awareness program, planning, identifying training and awareness needs, conducting training and awareness activities, and improving the program. This document is organized around those common foundational activities. The approach taken is to provide an outline of *what* should be done to establish and maintain a training and awareness program, rather than *how* to do it.

The following documents provide broad program guidance:

- *NIST Special Publication 800-16 Revision 1 (2nd Draft Version 2), A Role-Based Model For Federal Information Technology/Cyber Security Training* provides information on a training methodology for the development of training for personnel with cybersecurity responsibilities.
- The *CERT-RMM* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing practices. The Operational Training and Awareness process area provides a detailed description of practices and goals associated with training and awareness.

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov, or visit the website of the Office of Cybersecurity and Communications at http://www.dhs.gov/office-cybersecurity-and-communications.

Appendix A. Training and Awareness Resources

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
    - NIST Special Publication 800-16 Revision 1 (2nd Draft Version 2), A Role-Based Model For Federal Information Technology/Cyber Security Training

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

CERT-RMM
http://www.cert.org/resilience/products-services/cert-rmm/index.cfm

Appendix B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 6 cross-references CRR Training and Awareness Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at https://www.us-cert.gov/ccubedvp for more information on interpreting practice questions. The NIST CSF available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf provides informative references for interpreting Category and Subcategory statements.

Table 6: Cross-Reference of CRR Goals/Practices and NIST CSF Categories/Subcategories Reference and the Training and Awareness Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Training and Awareness Resource Guide Reference
Goal 1 – Cyber security awareness and training programs are established.		—
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 4
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	**PR.AT-1:** All users are informed and trained	Section IV, Step 2
3. Are skills gaps present in personnel responsible for cyber security identified? [OTA: SG3.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 2
4. Have training needs been identified? [OTA: SG3.SP1]	**PR.AT-1:** All users are informed and trained	Section IV, Step 4
Goal 2 – Awareness and training activities are conducted.		—
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2:SP1]	**PR.AT-1:** All users are informed and trained	Section V, Step 4
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	**PR.AT-1:** All users are informed and trained	Section V, Step 4
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. **PR.IP-7:** Protection processes are continuously improved	Section VI, Step 2
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3, OTA:SG3.SP3]	**PR.AT:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. **PR.IP-7:** Protection processes are continuously improved	Section VI, Step 4

Endnotes

1. For more information on the *Cyber Resilience Review*, please contact the Cyber Security Evaluation Program at CSE@hq.dhs.gov.
2. *CERT-RMM*. "Glossary of Terms" [Caralli 2010].
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT®-RMM: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1).* Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit http://www.cert.org/resilience/rmm.html.
4. "Operational Training and Awareness Process Area." *CERT-RMM* [Caralli 2010].
5. The *CERT-RMM* (EF:SG1) [Caralli 2010] discusses the need for resilience activities to meet strategic objectives.
6. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
7. Gates, L. P., *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework* [CERT 2010] discusses strategic planning.
8. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
9. The *CERT-RMM* (OTA:SG1and SG3) [Caralli 2010] discusses how to identify management directives and organizational guidelines.
10. The *CERT-RMM* (OTA:SG1:SP1and SG3:SP1) [Caralli 2010] discusses prioritizing objectives.

CYBERSECURITY: SHOULD THE SEC BE STICKING ITS NOSE UNDER THIS TENT?

Loren F. Selznick and Carolyn LaMacchia†

TABLE OF CONTENTS

I. INTRODUCTION

On January 29, 2015, Anthem, Inc. learned of a cyberattack that occurred over the course of several weeks.[1] Anthem, the country's second-largest health insurer, reported unauthorized access to a database containing 80 million customer and employee records.[2] Critical information accessed included Social Security numbers, birthdays, street and email addresses, and income data.[3] Working closely with the Federal Bureau of Investigation, the company has taken corrective measures, but the attackers have not been identified.[4] According to media reports, Anthem will soon deplete its $100 million cyber-

† Dr. Selznick (J.D. Cornell University) is an Assistant Professor of Business Law at Bloomsburg University of Pennsylvania and Dr. LaMacchia (Ph.D. Nova Southeastern University) is an Assistant Professor of Information and Technology Management, also at Bloomsburg University of Pennsylvania.

1. *How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services*, ANTHEM FACTS, https://www.anthemfacts.com (last visited Mar. 6, 2016).
2. *Id.*
3. *Id.*
4. *Id.*

insurance coverage just to notify the victims and provide free identity-theft protection and credit monitoring in the wake of this breach.[5] Anthem's predicament is commonplace—managing a loss that is not readily apparent, unpredictable, and costly. With more business operations dependent upon technology, cybersecurity breaches occur on a daily basis and impact entities of all sizes.

Investors envision similar cybersecurity breaches at their own companies. What if hackers obtained the debit and credit card information of retail customers? What if the cloud storage the company maintained for clients were breached? What if medical information were left unprotected? What if trade secrets were revealed? For businesses, investors need information to evaluate the likelihood of a cybersecurity breach and its potential effect on overall company health.

Similarly, cybersecurity breaches could affect the operation of the securities markets themselves. What if a broker-dealer network were breached? Would investor funds and identity information be protected? Could hackers manipulate stock prices, post phantom transactions, or shut down exchanges?

Enter the Securities and Exchange Commission (SEC), whose role is to protect investors by requiring companies to disclose material risks to the bottom line and by addressing risks to overall market function.[6] Serious cybersecurity breaches have the potential to affect the stability and even viability of publicly-traded companies, traders, and exchanges. The SEC has, therefore, considered this emerging risk a priority. On the one hand, the SEC wants sufficient disclosure to ensure that investors are not blindsided by a major cybersecurity breach. On the other hand, required disclosures or remedial steps should not make such a breach more likely.

The SEC has issued a guidance statement for disclosures about cybersecurity risks to publicly-traded companies.[7] It has also required individual companies to provide additional information about cybersecurity risks.[8] The SEC response appears to have been both too much and too little at once. The agency has companies disclosing the kinds of minor cybersecurity breaches that everyone experiences, which are annoying, but not life-threatening.[9] Listing them camouflages the major risks that concern investors. When a major breach occurs, however, the disclosures required are ineffective.

The SEC has also conducted cybersecurity examinations of broker-dealers and transfer agents. Pursuant to these examinations, it collected information about the approaches reporting companies use to protect

5. Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/.

6. *About the SEC*, SEC, http://www.sec.gov/about/whatwedo.shtml (last visited Feb. 29, 2016).

7. SEC, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (Oct. 13, 2011) [hereinafter TOPIC NO. 2], http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

8. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, RISK ALERT: OCIE CYBERSECURITY INITIATIVE (Apr. 15, 2014) [hereinafter RISK ALERT], https://www.sec.gov/ocie/announcement/ Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

9. TOPIC NO. 2, *supra* note 7.

themselves against security breaches. The agency then studied the efforts of the industry as a whole.[10] Recent criticism of the cybersecurity measures at the SEC itself, however, brings into question whether collecting the sensitive information actually increases the risk to investors.[11] The SEC required regulated entities to hand over information that may have been too sensitive in light of its own cybersecurity weaknesses.

This article, an interdisciplinary study, examines first, cybersecurity risks to the investing public, second, whether the SEC is the appropriate agency to address these risks, third, what the SEC is doing about them and the flaws in its response, and, fourth, whether its response can be improved.

II. CYBERSECURITY BREACHES

Cybersecurity breaches come in many forms and are used to steal data assets, disrupt company operations, extort information, or damage reputations.[12] The hacking of corporations is rampant in the United States, prompting law enforcement to observe that there are two kinds of companies: those who have been hacked, and those who do not know they have been hacked.[13] In some cases, companies are not aware for an extended period that a breach is occurring. In January, the New York Times revealed that its computers were compromised by Chinese hackers for four months.[14] The problem is considered critical and its extent is much worse than has been reported. Companies generally do not disclose a breach unless required by law; many breaches, particularly those in small and mid-sized businesses go unreported.[15]

Data, including customer contact information, credit card data, health data, and valuable intellectual property, is most often the target of a breach. Surveys reveal the continued rise of the lucrative black market in credit card data, health credentials, and personal identifying information.[16] In late 2013,

10. RISK ALERT, *supra* note 8.

11. *U.S. SEC's Information Technology at Risk of Hacking—Report*, REUTERS (Apr. 17, 2014, 4:21 PM), http://www.reuters.com/article/sec-cybercrime-security-idUSL2N0N91GU20140417.

12. *See, e.g.*, Michael J. Lebowitz, *The Cyberenemy: Using the Military Justice System to Prosecute Organized Computer Attackers*, 2013 U. Ill. J.L. TECH. & POL'Y 83, 86–87 (2013) (discussing how to prosecute cyberattacks and organized groups using the military justice system).

13. James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (quoting FBI Director James Comey as having said on the CBS program *60 Minutes*, "[t]here are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.").

14. Nicole Perlroth, *Hackers in China Attacked the Times for the Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html. Experts believe the hackers were attempting to identify the sources for an article describing how Chinese Prime Minister Wen Jiabo accumulated a billion dollar fortune through questionable business dealings. Geoffrey Ingersoll & Michael B. Kelley, *A Digital Trail of Evidence Linked the NYT Hack to China*, BUS. INSIDER (Feb. 1, 2013), http://www.businessinsider.com/nyt-china-hack-how-we-know-203-2.

15. Fred Donovan, *Many Major Financial Data Breaches Go Unreported, Say IT Pros*, FIERCEITSECURITY (July 2, 2015), http://www.fierceitsecurity.com/story/many-major-financial-data-breaches-go-unreported-say-it-pros/2015-07-02.

16. Sophie Curtis, *Cyber Black Market 'More Profitable than Drug Trade'*; TELEGRAPH (Mar. 26, 2014), http://www.telegraph.co.uk/technology/internet-security/10724704/Cyber-black-market-more-

several data aggregator companies, including Dun & Bradstreet, LexisNexis, and Kroll Background American, were hacked by the introduction of botnet software on compromised servers.[17] Botnets are mechanized collection tools that can target organizations of any size for consumer and business data.[18] Attackers worked undetected for months to siphon massive amounts of personal identifying information.[19] Unlike credit card numbers, which can be cancelled, employment details, addresses, and social security numbers can be used repeatedly in a widening circle of fraud. The impact of this type of data theft can be long term as cyber criminals sell personal identifying information on the black market.

"Some of the largest attacks in the past year or so included eBay (145 million users), Home Depot (109 million customers), JPMorgan Chase (83 million customers), Target (70 million customers), and Michaels Stores (3 million customers)."[20] The attractiveness of most information is independent of the size of the organization, however, because automated techniques access multiple targets. Although not usually publicized, small and mid-sized businesses have been the target of about sixty percent of data-driven breaches.[21] These organizations are attractive to cyber thieves for a number of reasons. Smaller businesses typically have neither the in-house expertise nor the budget to implement sophisticated cybersecurity prevention measures.[22] In addition, many mistakenly believe cyber thieves prefer larger targets.[23] It is the data and the vulnerability of the organization, not its size, that make a company the target of a cybersecurity breach.

Cybercrime can also target securities market operations. Stock prices tend to increase during periods with a large volume of trading activity.[24] Criminals have taken advantage of this phenomenon using a variety of deceitful techniques. An example is the "pump-and-dump" scheme where promoters claim to have "inside" information about an impending development that will have a positive impact on the price of stock.[25] The promoters sell their own shares after the stock price is "pumped" up by the buying frenzy they

---

profitable-than-drug-trade.html.

17. Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*. KREBSONSECURITY.COM (Sept. 13, 2013), http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

18. *Botnets 101: What They Are and How to Avoid Them*, FBI (July 5, 2013), https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

19. Krebs, *supra* note 17.

20. William Atkinson, *Cybersecurity Challenges for Small Business*, BENEFITSPRO (Feb. 9, 2015), http://www.benefitspro.com/2015/02/09/cybersecurity-challenges-for-small-business.

21. Jay Jacobs, *Analyzing Ponemon Cost of Data Breach*, DATADRIVENSECURITY (Dec. 11, 2014), http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/.

22. Taylor Armerding, *Why Criminals Pick on Small Business*, CSO (Jan. 12, 2015), http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html#comments.

23. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

24. Ekkehert Boehmer & Juan Wu, *Short Selling and the Price Discovery Process*, 26 REV. FIN. STUD. 2, 287–322 (2013).

25. *"Pump-and-Dumps" and Market Manipulations*, SEC [hereinafter PUMP AND DUMP], https://www.sec.gov/answers/ pumpdump.htm (last visited Feb. 29, 2016).

created.[26] After the selling hype and after the fraudsters "dump" (sell) their shares, the price typically falls, and investors lose their money.[27] A variation of the scheme is the "hack, pump, and dump" which incorporates a cybersecurity breach to steal a company repository of customers' personal identifying information.[28] Stolen account information is used to generate a large volume of stock purchases which artificially manipulate stock prices.[29] As in the "pump-and-dump" technique, the criminal operation sells its shares when the price is high.[30] The stock's price plummets, leaving investors defrauded with "significant losses."[31] "Pump-and-dump" activity violates the Security Exchange Rule 10b-5.[32]

Hackers operate in a variety of ways. Technological similarity from company to company makes their work easier. Most companies, regardless of size, are operating with a technology-driven business model.[33] The typical technology infrastructure consists of a common set of software components including operating, network, and database management systems.[34] In the global commercial marketplace, there are relatively few vendors offering these systems when compared with applications.[35]

In addition, designs of these systems are based on quality standards that have evolved for the efficient and secure processing of data and the interoperability of components. Appropriately implementing secured coding standards adds additional, often significant, cost in areas including software developer training and product verification.[36] Unfortunately, mass-market software sales are not governed by appropriate product-risk norms; as a result, market conditions exist in which sellers profit by offering vulnerability-ridden software.[37] The prevailing consensus is that software programs are sold with an unacceptable number of security vulnerabilities that are gradually fixed

26. *Id.*

27. *Id.*

28. *See, e.g.*, Michael Riley & Jordan Robertson, *Digital Misfits Link JPMorgan Hack to Pump-and-Dump Fraud*, BLOOMBERG BUS. (July 22, 2015), http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack (describing the hack-pump-and-dump scheme against JP Morgan).

29. *Id.*

30. PUMP AND DUMP, *supra* note 25.

31. Brandon Stosh, *Three Men Arrested in Biggest Bank Hacking Scheme Breaching JP Morgan Among Others*, FREEDOM HACKER (Nov. 11, 2015), https://freedomhacker.net/three-men-arrested-biggest-bank-hacking-scheme-breaching-jp-morgan-4741/.

32. 17 C.F.R. § 240.10b-5 (2014).

33. HARV. BUS. REV. ANALYTIC SERVICES, THE REINVENTION OF BUSINESS: NEW OPERATING MODELS FOR THE NEXT-GENERATION ENTERPRISE (2012), https://hbr.org/resources/pdfs/tools/17360_HBR_Cognizant_Report_webview.pdf.

34. DAVID A. PATTERSON & JOHN L. HENNESSY, COMPUTER ORGANIZATION AND DESIGN: THE HARDWARE/SOFTWARE INTERFACE (5th ed. 2013).

35. DANIEL P. SIEWIOREK & ROBERT S. SWARZ, RELIABLE COMPUTER SYSTEMS: DESIGN AND EVALUATION (3rd ed. 1998).

36. Ronny Grey & Andrea Fried, *"Standard Bibles" and Mediators As a Way of Software Development Organizations to Cope with the Multiplicity and Plurality of Standards*, 12 INT'L J. IT STANDARDS & STANDARDIZATION RES. 57 (2014).

37. Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 U. ILL. J.L. TECH. & POL'Y 45 (2012).

through the release of software patches.[38] It is the responsibility of the software user to update the software version with a software patch in order to remove the vulnerability from the user's system.[39] The strengths and weaknesses of these consistently designed systems are well known to both technology professionals and the cybercriminal world. After the release of a software patch, cybercriminals can continue to take advantage of a software vulnerability on systems which the patch has not been installed.

This year, the University of California, Berkley, was hit with a data breach that exposed students' Social Security numbers and families' financial information.[40] Hackers accessed the information through a known vulnerability on an unpatched researcher's computer.[41] It is not surprising that reports of security breaches reveal that most attacks resulted not from clever attackers discovering new kinds of flaws, but rather from repeated tries of well-known exploits.[42]

As cyber-attacks on retail, technology, and industrial companies increase so does the importance of cybersecurity. From brute-force attacks on networks[43] "to malware compromising credit card information to disgruntled employees sabotaging networks from the inside, companies and their customers need to secure their data."[44] An organization's technical security architecture includes firewalls, hardened hosts,[45] intrusion detection systems, and other tools to form a complete system of protection. Without a technical security architecture, companies will be unable to create a comprehensive wall against attackers. Technical security architecture often includes defense-in-depth, which requires multiple countermeasures to be defeated for an attack to succeed.[46] This is important because every security measure has vulnerabilities.

It is never possible to eliminate risks and completely insulate information. It is technically impossible to protect against all future events. Even if it were technically possible to protect against all risk, comprehensive security protections would be prohibitively expensive and impede business operations. High-security environments tend to be inefficient.[47] Security is never free and

38. STEVE MAGUIRE, WRITING SOLID CODE (2013).

39. Janet Gilmore, *Campus Announces Data Breach*, BERKELEY NEWS (Apr. 30, 2015), http://news.berkeley.edu/2015/04/30/campus-announces-data-breach/.

40. *Id.*

41. *Id.* The vendors of the software components issue software fixes, "patches," to their customers in response to recommendations in internal quality control review reports and to cybersecurity breaches. It is the customer's responsibility to install the software patch to remove the vulnerability.

42. GEORGE CYBENKO ET AL., ADVERSARIAL AND UNCERTAIN REASONING FOR ADAPTIVE CYBER DEFENSE: BUILDING THE SCIENTIFIC FOUNDATION. INFORMATION SYSTEMS SECURITY 1–8 (2014).

43. A brute-force attack is a systematic attempt, usually through a simple computer program, of all possible keys or passwords until the correct one is found.

44. Riley Walters, *Cyber Attacks on U.S. Companies in 2014*, HERITAGE, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014 (last visited Feb. 29, 2016).

45. Any device (servers, routers, computers, tablets, etc.) connected to a network is a host. Each device requires cybersecurity protection to become a "hardened host."

46. *Datasäkerhet och integritet*, DALARNA UNIV., http://users.du.se/~hjo/cs/ik1080/presentations/som_pdf/ch2.pdf.

47. *Boyle Applied Security Chapter 2 Flashcards*, QUIZLET (Feb. 17, 2016, 5:48 PM), https://quizlet.com/76382653/boyle-applied-security-chapter-2-flash-cards/.

seldom inexpensive with costs including not only the initial cost of the security device but the labor to implement, operate, and maintain. "The wave of recent data breaches at big-name companies such as JPMorgan Chase, Home Depot, and Target raises questions about the effectiveness of the private sector's information security."[48]

A. Effects on Stock Price

Industry analysis has shown that the stock price of an organization is not adversely impacted by the news of a data breach.[49] When an official announcement of a cybersecurity breach is made, stockholders react indifferently. What explains this phenomenon? Recovering from a cybersecurity breach is typically very expensive; why isn't the announcement of a breach reflected in the price of stock? Several factors may explain this.

It is difficult to quantify the cost and recovery timeline associated with a cyberattack on a business. While the short-term stock price is unaffected in the wake of a cybersecurity breach, companies face long-term consequences, including spending millions of dollars to upgrade security systems and to settle lawsuits. Once the extent of the breach is determined, stock prices react as they do to other triggers that adversely impact the long-term earning potential of the corporation.[50]

Determining the cost of a cybersecurity breach is a difficult task and should include both direct and indirect expenses incurred by the organization.[51] "Direct expenses include legal fees, regulatory fines, call centers, and credit monitoring subscription fees."[52] Once a breach is discovered, the full value of direct expenses is difficult to estimate because of the extended timeframe for discovering all parties impacted by the breach.[53] "It is even more difficult to calculate indirect costs, such as the loss of revenue and the expenses from the negative impact on the reputation, brand, and marketplace image."[54] "The average cost of cybercrime incidents rises significantly each year for U.S. organizations with an annual average in 2014 of $8.6 million for a retail company."[55] "It is even higher in other sectors; the annual average cost per company of successful cyber-attacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries."[56] "Post-breach share-price declines have only

48. Walters, *supra* note 44.

49. Elena Kyochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV. (Mar. 31, 2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

50. *Id.*

51. Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/.

52. *Breach Costs*, CYBER RISK HUB, http://www.cyberriskhub.com/breach-costs/ (last visited Feb. 29, 2016).

53. Kristin Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. J. 345 (2015).

54. *Breach Costs*, *supra* note 52.

55. Walters, *supra* note 44.

56. Michael A. Robinson, *Get in on the "Ground Floor" of this National Security Investment*, STRATEGIC TECH INVESTOR (Sept. 9, 2015), http://strategictechinvestor.com/2015/09/get-in-on-the-ground-

had lasting effect following company disclosures of clear, direct and immediate impact on business operations, such as warnings that high costs would hurt profitability."[57]

B. How the SEC Has Addressed Cybersecurity

Given the risk of substantial losses, the SEC has taken up the cybersecurity issue. This is consistent with its mission to protect the investing public by requiring disclosure of material information.[58] Whether the information it has thus far demanded on cybersecurity is actually "material" and whether the SEC is equipped to handle the sensitive cybersecurity information it is gathering in its examinations, however, is questionable.

1. The SEC's Job

The SEC has a "public policy mission of protecting investors and safeguarding the integrity of the markets."[59] This has been further refined by the agency itself as a mission to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[60] The agency was formed in the wake of the 1929 market crash:[61]

> The need for protective reform was pointed out clearly by the *House Report of the 73d Congress* which stated that "During the post war decade some 50 billion dollars worth of new securities were floated in the United States. Fully half or 25 billion dollars worth of securities floated during this period have proven to be worthless. These cold figures spell tragedy in the lives of thousands of individuals who invested their life savings, accumulated after years of effort, in these worthless securities . . . Alluring promises of easy wealth were freely made with little or no attempt to bring to the investors" attention those facts essential to estimating the worth of any security.[62]

The SEC protects investors by requiring disclosure of information material to their investment decisions. The theory is that armed with this information, they can make their own choices—good or bad—in a free and fair market.[63]

---

floor-of-this-national-security-investment/.

57. Jennifer Booton, *Three Reasons Why Cyberattacks Don't Hurt Stock Prices*, MARKETWATCH (Apr. 3, 2015), http://www.marketwatch.com/story/3-reasons-why-cyberattacks-dont-hurt-stock-prices-2015-04-03.

58. *See* SEC v. Rind, 991 F.2d 1486, 1490–92 (9th Cir. 1993) (describing the importance of material disclosure).

59. *Id.* at 1491.

60. SEC v. Wilson, No. 12-cv-15062 2012 U.S. Dist. LEXIS 165248 (E.D. Mich. Nov. 20, 2012) (quoting *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, SEC http://www.sec.gov/about/whatwedo.shtml (last visited Mar. 6, 2016)).

61. Lori A. Richards & John H. Walsh, *Compliance Inspections and Examinations by the Securities and Exchange Commission*, 52 BUS. LAW. 119, 120 (1996) (stating "[t]he Exchange Act . . . was enacted after the stock market crash of 1929 revealed shocking misconduct and marketplace anarchy").

62. Alan B. Levenson, *The Role of the SEC as a Consumer Protection Agency*, 27 BUS. LAW. 61 (1971).

63. *Id.* (stating that "[t]he economic justification for disclosure as the keystone of investor protection

> The laws and rules that govern the securities industry in the United States derive from a simple and straightforward concept: all investors, whether large institutions or private individuals, should have access to certain basic facts about an investment prior to buying it, and so long as they hold it. To achieve this, the SEC requires public companies to disclose meaningful financial and other information to the public. This provides a common pool of knowledge for all investors to use to judge for themselves whether to buy, sell, or hold a particular security. Only through the steady flow of timely, comprehensive, and accurate information can people make sound investment decisions.[64]

The securities laws, therefore, require public companies to report material information to the investing public; information is material if "there is a substantial likelihood that a reasonable investor would attach importance [to it] in determining whether to purchase the security."[65] "The SEC's reporting requirement is designed to provide investors with the information necessary to make informed decisions, and provides the SEC with a basis to police the actions of companies subject to the requirement."[66] The requirements of the SEC "are satisfied only by the filing of complete, accurate and timely reports."[67] These include quarterly and annual reports, in Forms 10-Q and 10-K,[68] as well as reports of extraordinary events as they occur, in Form 8-K.[69]

On Form 10-K, public companies must report, among other things:

- *Risk Factors.*[70] The report must discuss "the most significant factors that make the offering speculative or risky." Companies are not supposed to provide boilerplate disclaimers reporting generic risks that would affect all public companies. Instead, they are required to describe company or industry-specific risks.[71]
- *Management's Discussion and Analysis of Financial Condition and Results of Operations.*[72] In this section, management provides "information that the registrant believes to be necessary to an understanding of its financial condition, changes in

---

lies in the belief that material corporate and financial information disseminated to prospective investors provides a rational basis to evaluate securities and this is a necessary precondition to efficient markets").

64. *The Investor's Advocate*, *supra* note 60 ("The hiding and secreting of important information obstructs the operation of the markets as indices of real value . . . Delayed, inaccurate and misleading reports are the tools of the unconscionable market operator and the recreant corporate official who speculates on inside information . . . The reporting provisions . . . are a very modest beginning to afford that long delayed aid . . . in the way of securing proper information for the investors."); H.R. Rep. No. 73-1383, at 13 (1934).

65. 17 C.F.R. § 230.405 (2012); March Sadowitz, *Environmental Disclosure: What Is Required and What Is Needed*, 16 ENVTL. HIST. REV. 69, 70 (1992).

66. Abella v. Barringer Res., Inc., 615 A.2d 288, (N.J. Super. 1992).

67. SEC v. IMC Int'l, Inc., 384 F.Supp. 889, 893 (N.D.Tex. 1974); *See also* Abella v. Barringer Resources, Inc., 615 A.2d 288, 293 (N.J. Super. 1992) (describing qualified and conditional privilege).

68. 15 U.S.C. § 78m (2012); 17 C.F.R. §§ 240.13a-1, 13a-13 (2012).

69. 15 U.S.C. § 78m (2012); 17 C.F.R. § 240.13a-11 (2012).

70. 17 C.F.R. § 229.503(c) (2012).

71. *Id.*

72. 17 C.F.R. § 229.303 (2012).

financial condition and results of operations."[73] Management must "[d]escribe any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations and, in each case, indicate the extent to which income was so affected."[74]

- *Business Description.*[75] This section includes descriptions of the company products, relationships with important customers and suppliers, and competitive conditions.[76]
- *Legal Proceedings.*[77] In the Legal Proceedings section, companies are required to briefly describe "any material pending legal proceedings, other than ordinary routine litigation incidental to the business . . ."[78]
- *Financial Statement Disclosures.*[79] SEC regulations state that financial statements "not prepared in accordance with generally accepted accounting principles are presumed to be misleading . . ."[80] "To meet the requirements of full disclosure," GAAP-compliant financial statements must have explanatory notes "to help users interpret some of the more complex items."[81] Material extraordinary charges must be individually explained.[82]

To ensure the integrity of the markets and the purchase-and-sale process, the SEC also has sweeping authority to demand records and to conduct compliance examinations of "national securities exchanges and their members," those selling securities, and other related entities.[83] The SEC Office of Compliance Inspections and Examinations (OCIE) focuses its "attention on the firms, and on the areas within firms, that need regulatory scrutiny the most."[84] There are four types of examinations conducted by OCIE: compliance examinations of regulated entities, oversight examinations of entities also regulated by a self-regulatory organization, inspections of the self-regulatory organizations themselves, and "special purpose, sweep, and cause examinations."[85]

During compliance and oversight examinations, the OCIE staff interview

73. *Id.*
74. *Id.*
75. 17 C.F.R. § 229.101 (2012).
76. 17 C.F.R. § 229.101(c) (2012).
77. 17 C.F.R. § 229.103.
78. *Id.*
79. Regulation S-X, 17 C.F.R. § 210 (2012).
80. 17 C.F.R. § 210.4-01 (2012).
81. BELVERD NEEDLES & MARIAN POWERS, FINANCIAL ACCOUNTING 50 (11th ed. 2011).
82. *See* William C. Norby, *Accounting for Financial Analysis: SEC Adopts an Activist Role in Accounting*, 28 FIN. ANALYSTS J. 96 (1972) (describing material charges).
83. 15 U.S.C. § 78q; SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, EXAMINATION PRIORITIES FOR 2014 (Jan. 9, 2014) [hereinafter 2014 EXAMINATION PRIORITIES], https://www.sec.gov/about/offices/ocie/ national-examination-program-priorities-2014.pdf; Richards, *supra* note 61 at 132–33.
84. Richards & Walsh, *supra* note 61 at 147.
85. *Id.* at 136.

management, request documents for review and copying, and question knowledgeable employees.[86] Examinations result in a letter indicating whether the examiners found compliance failures or deficiencies.[87] If a deficiency letter is issued—and most examinations result in them—the OCIE follows up to ensure that the deficiencies are remedied. If they are not, an enforcement action may follow.[88]

Special purpose examinations are conducted in a similar manner, but are used to collect information from numerous entities at once on matters of particular concern to the SEC. "From time to time, the Commission, another division, or the examination staff determines that some development or market practice warrants special inquiry. Special purpose examinations are then used to gather the needed information on an expedited schedule. In sweep examinations, several teams conduct simultaneous examinations."[89]

2. *SEC Response to Cybersecurity Risks*

On October 13, 2011, the Securities and Exchange Commission, Division of Corporate Finance, issued "CF Disclosure Guidance: Topic No. 2 Cybersecurity."[90] The purpose was to provide "the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents."[91] Further reflecting the heightened concern of the SEC about cybersecurity, the Office of Compliance Inspections and Examinations—the self-described "'eyes and ears' of the SEC"—named cybersecurity as an examination priority in 2014 and 2015.[92]

a. 2011 Cybersecurity Disclosure Guidance

On May 11, 2011, five United States senators wrote to then-SEC Chairperson Mary Schapiro about their cybersecurity concerns.[93] Citing "inconsistencies in reporting, investor confusion, and the national importance of addressing cyberspace security," they urged the SEC to publish guidance "regarding the disclosure of information security risk including material network breaches."[94] The senators said it was "essential that corporate leaders know their responsibility for managing and disclosing information security

86. 2014 EXAMINATION PRIORITIES, *supra* note 83.
87. Richards & Walsh, *supra* note 61 at 143.
88. *Id.* at 140–46.
89. *Id.* at 136–37.
90. TOPIC NO. 2, *supra* note 7.
91. *Id.*
92. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, EXAMINATION PRIORITIES FOR 2015 at 3 (Jan. 15, 2015) [hereinafter 2015 EXAMINATION PRIORITIES], http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf; 2014 EXAMINATION PRIORITIES, *supra* note 83, at 2.
93. Letter from Senator John D. Rockefeller, IV et. al. to Mary Schapiro, Chairperson of the United States Securities and Exchange Commission (May 11, 2011), http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4c21-92c7-a8e1dd5a707e.
94. *Id.*

risk."[95]

The SEC responded on October 13, 2011 with CF Disclosure Guidance: Topic No. 2, Cybersecurity (Guidance).[96] It did not add to or modify existing disclosure requirements.[97] The "guidance" did not have the force of law; it did not go through the notice-and-comment procedure of a regulation.[98] However, it informed regulated parties how the SEC staff charged with enforcing the laws interpreted them.[99]

Noting that their increased reliance upon digital technologies had opened registrants to cyberattack, the agency said that reporting entities and professionals had become concerned about how to meet their disclosure obligations about this kind of risk.[100] The SEC said its response was aimed to be consistent with the disclosure requirements for any other type of business risk.[101]

The SEC emphasized (twice), however, that "detailed disclosures [that] could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security— . . . are not required under the federal securities laws."[102] This assurance was cold comfort for, as one commentator put it, there was a "trade-off inherent in making Registrants' cybersecurity risks and prevention measures more transparent."[103]

> The trade-off can be summarized as follows: The more revealing a Registrant's cybersecurity disclosures become, the greater the likelihood that they will provide information useful to hackers and

95. *Id.*

96. TOPIC NO. 2, *supra* note 7; Roland L. Trope & Sarah Jane Hughes, *The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-Thieves More?*, AM. BAR ASS'N: BUS. L. TODAY (Dec. 19, 2011), http://www.americanbar.org/publications/blt/2011/12/03_trope.html ("On October 13, 2011, the SEC's Division of Corporate Finance quietly issued a new guidance . . . describing disclosures of cybersecurity incidents and attacks and the prevention and remediation measures that public companies . . . have suffered or may suffer, and of the prevention and remediation expenses they have expended or may expend . . . This Guidance is not a rule or a commission interpretation. It did not appear in the *Federal Register* for comment or otherwise. Its issuance is likely to cause substantial amounts of work among Registrants and legal professionals who represent them.").

97. Peter Romeo & Richard Parrino, *SEC Issues Guidance on Disclosure of Cybersecurity Risks and Cyber Incidents*, HOGAN LOVELLS SEC UPDATE (Oct. 25, 2012), http://www.hoganlovells.com/sec-issues-guidance-on-disclosure-of-cybersecurity-risks-and-cyber-incidents-10-25-2011/.

98. *See generally* 5 U.S.C. § 553 (2012) (describing the rule making process for federal regulations).

99. RESEARCHING THE FEDERAL SECURITIES LAWS THROUGH THE SEC WEBSITE, SEC http://www.sec.gov/investor/pubs/securitieslaws.htm (last modified Dec. 4, 2012) ("The Commission occasionally provides guidance on topics of general interest to the business and investment communities by issuing 'interpretive' releases, in which we publish our views and interpret the federal securities laws and SEC regulations. Interpretive releases . . . are not positive law but provide useful guidance as to the position of the SEC staff on various issues."); *see also* Romeo & Parrino, *supra* note 97 (discussing the ramifications of the SEC's cybersecurity disclosure guidance).

100. TOPIC NO. 2, *supra* note 7.

101. *Id.*

102. *Id.*

103. Trope & Hughes, *supra* note 96; Will Daugherty, *The Evolving Landscape of Cybersecurity Disclosures*, 23 SECUR. LIT. J. 6, 6 (Summer 2013) ("Providing detailed disclosures of cyberattacks can create the risk of providing a road map for future cyberattacks. Yet, a company's failure to adequately disclose cyber risks and incidents that have a material impact on the company's operations or financial condition may violate the federal securities laws.").

> competitors (Adversaries). Specifically, a Registrant's cybersecurity disclosures, which the longstanding SEC interpretations require be specific to the Registrant rather than generic, will be understood far better by a cyber Adversary, than by a potential investor, and, accordingly, more valuable to Adversaries . . . Registrants and their lawyers will not know, for a while at least, what the precise consequences of the new Guidance, intended and otherwise, will be. It also may take time for the SEC staff to discover how much value investors will gain from the required cybersecurity disclosures, or whether, as we fear, the earliest beneficiaries and the ones who stand the most to gain will be the Adversaries, not investors.[104]

The Guidance did not create any new reporting requirements, but made it "clear that the agency expect[ed] public companies . . . to have undertaken an assessment of the risks they face, the consequences that may occur in the occasion of a cyber event and how they might respond."[105] Rather than creating new requirements for cybersecurity, it took the approach of explaining how the old requirements applied to this new problem.

> The staff has typically handled new "disclosure areas" and "hot topics" by starting with the premise that our rules require disclosure of material information. So, our disclosure experts have provided guidance about how to address particular topics within the framework of providing information that is necessary for exercising an investment or voting decision . . . When the Commission adopted rules decades ago requiring a description of the company's business, risk factor disclosure and MD&A, there were no such things as smartphones, tablets, or even the internet. And, so it was not thinking about the risks presented by cybersecurity attacks or breaches. Even though cybersecurity attacks were not specifically contemplated, the disclosure requirements generally cover these risks. That is because, even in the absence of a line item requirement, the basic standard of "materiality" governs. Depending on the severity and impact of the cybersecurity attacks, disclosure is either required or not. And the staff of Corporation Finance, relying on the materiality standard, issued guidance in October 2011 to help companies work through the disclosure questions that arise when considering cybersecurity matters.[106]

Five 10-K report sections that might be affected by cybersecurity

104. Trope & Hughes, *supra* note 96; Howard M. Privette et al., *The SEC Guidance on Cybersecurity Measures for Public Companies*, L.A. LAW. Sept. 2014, at 14 ("Disclosure of cybersecurity problems by public companies . . . presents an interesting confluence of policy considerations for which there is still no consensus. On the one hand, investors may be interested in whether and to what extent a corporation may be burdened by cybersecurity expenses—whether they be the cost of building defenses or the losses arising from a breach. On the other hand, detailed discussion of the value of vulnerable assets or the reasons for their vulnerability may attract predators.").

105. Melissa Maleske, *Life's a Breach*, INSIDE COUNSEL (Dec. 29, 2011); *see also* Daughetry, *supra* note 103, at 6–7 (articulating the risks to investors from cybersecurity threats).

106. Mary Jo White, Chairwoman, SEC, Address at 2013 Leadership Conference of Nat'l Assoc. of Corp. Dir.: The Path Forward on Disclosure (Oct. 15, 2013), http://www.sec.gov/News/Speech/Detail/Speech/1370539878806#.VPTPHkun3cY.

incidents or risks were cited.[107] In the "Risk Factors" section, the Guidance said companies "should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[108] This did not sound new. It parroted the threshold definition of risk materiality in the regulatory instructions for 10-K reports.[109] Then, the agency spelled out what it expected for cybersecurity risks.[110] Companies were advised to evaluate cybersecurity risks by considering the frequency and severity of past events and the probability and magnitude of future incidents, including their financial and disruptive costs.[111] Companies were also instructed to factor in threats of attack, preventive measures, and insurance.[112] If, considering all these factors, management concluded the risk of a cybersecurity breach was material, necessary disclosures might include aspects of the business that were creating the risk and what the costs might be, risks related to outsourcing, descriptions of past cybersecurity breaches, risks of undetected breaches, and insurance coverage.[113]

Similarly, the "Management's Discussion and Analysis of Financial Condition and Results of Operations" (MD&A) section was to include "a discussion of cybersecurity risks and incidents if cyber incidents have had or are likely to have a material effect on a company's liquidity, results of operations or financial condition or would cause reported financial information not to be necessarily indicative of future operating result or financial condition."[114] Examples provided were the effects of intellectual property loss, a significant loss of customers following a cybersecurity breach, and materially elevated costs from remediation, litigation, or prevention.[115]

Likewise, the "Business Description" section was expected to include any cybersecurity breaches that affected the products, services, important customer or supplier relationships, or the ability to compete.[116] Disclosures might also be required in the "Legal Proceedings" section for actions relating to cybersecurity breaches, if the outcome could be material to the results of the company or in the "Financial Statement Disclosures" to explain extraordinary expenses, contingent losses, diminished cash flows, impairment of assets resulting from cybersecurity incidents or prevention tactics.[117]

In addition to these regular disclosures in annual 10-K reports, companies were required to report significant events as they occurred in a Form 8-K report "if necessary to maintain the accuracy and completeness of information

107. *Id.*
108. TOPIC NO. 2, *supra* note 7.
109. 17 C.F.R. § 229.503(c) (2011).
110. TOPIC NO. 2, *supra* note 7.
111. *Id.*
112. *Id.*
113. *Id.*; Elizabeth A. Ising & Alexander G. Acree, *SEC Issues Guidance on Cybersecurity Disclosures*, 25 INSIGHTS: CORP. & SEC. L. ADVISOR 34, 34–35 (2011).
114. *Id.*
115. TOPIC NO. 2, *supra* note 7.
116. *Id.*
117. *Id.*

in the context of securities offerings."[118] Companies were expected to disclose "the costs and other consequences of material cyber incidents" in an 8-K report.[119]

Although, in theory, the Guidance did not have the force of law, practitioners recognized that the failure to follow the "views" of the SEC staff could lead to an enforcement action.[120] As one attorney and former SEC staffer said,

> From my enforcement perspective, . . . these guidelines set up the situation where the SEC's going to bring an enforcement action against some company for making false or misleading statements about cybersecurity and exposure inside a major . . . company that failed to provide necessary notifications, and then experienced a massive breach. I can't say that tomorrow there will be an enforcement case, but the SEC doesn't write about stuff it's not concerned about.[121]

Close on the heels of the Guidance was the February 2012 justification for the Fiscal Year 2013 SEC budget.[122] In asking Congress for more funds, the SEC pointed to cybersecurity concerns.[123] "Financial entities are recognized as particular targets for cyber attack attempts. SEC monitoring of cyber security at the various securities exchanges and the growing number of trading and clearing platforms will require additional staff to further enhance this function in FY 2013."[124]

By the summer of 2012, staff reported that in reviews of 10-K reports, cybersecurity was an area of interest "particularly at companies that [had] been infiltrated."[125] In April 2013, the SEC was being pressured to make more stringent requirements and this was under review.[126] Applying "pressure on companies using . . . enforcement powers under existing disclosure requirements" was an additional possibility.[127]

By early 2014, practitioners reported that the SEC staff was regarding the Guidance with the force of a fully vetted regulation.[128] The SEC determined, based on the Guidance, that 2012 cybersecurity disclosures by six major

118. Ising & Acree, *supra* note 113, at 36.

119. *Id.*

120. Maleske, *supra* note 105.

121. *Id.*

122. SEC, IN BRIEF FY 2013 CONGRESSIONAL JUSTIFICATION, 6 (Feb. 2012), https://www.sec.gov/about/secfy13congbudgjust.pdf.

123. *Id.*

124. *Id.*

125. *Dialogue with the Director of the SEC Division of Corporation Finance*, 26 INSIGHTS: CORP. & SEC. L. ADVISOR 37, 37 (Sept. 2012).

126. Daugherty, *supra* note 103; Ernest Badway, *SEC Again Looking at Cybersecurity Issues*, SEC. COMPLIANCE SENTINEL (Oct. 28, 2013).

127. *Id.*

128. Gerry H. Grant & C. Terry Grant, *SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement*, 84 CPA J. 69 (May 2014); Norah C. Avellan, Note, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 220–21 (2014).

publicly-traded companies did not go far enough.[129] "Requests" for additional information not honored could have resulted in sanctions or fines.[130] Moreover, according to some observers, the staff was ignoring the materiality requirement in the Guidance.[131]

> The SEC requested that Amazon disclose a cyber attack that stole millions of addresses and credit card information from its Zappos unit. Amazon eventually complied with the SEC's request, but only after arguing that the disclosure was not required because Zappos did not contribute material revenue. Hartford presented a materiality argument as well, but the SEC responded that any cyber attack should be disclosed.[132]

Commentators began urging the SEC to adopt the Guidance as a formal rule. In 2013, Senator John D. Rockefeller wrote to SEC Chairperson Mary Jo White that "given the growing significance of cybersecurity on investors' and stockholders' decisions, the SEC should elevate [the staff's] guidance and issue it at the Commission as well."[133] This, of course, would have subjected it to notice-and-comment procedure under the Administrative Procedure Act.[134] Chairperson White declined immediate action, "equating cybersecurity risks 'with other business risks' that should be 'among the factors a public company would consider in evaluating its disclosure obligations.'"[135]

The December 2014 spending bill required the SEC to report to the Appropriations Committees of the Senate and House of Representatives on efforts to modernize disclosure requirements, including those directed at cybersecurity.[136] The report was to be submitted within 90 days of passage of the bill.[137] Since then, there have been reports that the SEC has been weighing more stringent cybersecurity reporting requirements.[138] In June 2015, two more lawmakers pressed the SEC to require "regular disclosures from firms outlining their cyber practices, as well as a more consistent standard for Form 8-K disclosures following a successful cyberattack."[139]

---

129. Grant & Grant, *supra* note 128.

130. *Id.*

131. *Id.*

132. *Id.*

133. Letter from John D. Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci. and Transp. to Mary Jo White, Chairperson, SEC (Apr. 9, 2013), http://www.privacyandsecuritymatters.com/files/2013/04/Rockefeller-SEC-letter.pdf; Howard M. Privette et al., *The SEC Guidance on Cybersecurity Measures for Public Companies*, L.A. L. 14, 15 (Sept. 2014).

134. 5 U.S.C. § 553 (2012).

135. Letter from Mary Jo White, Chairperson, SEC, to John D. Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci. and Transp. (May 1, 2013), http://www.steptoe.com/assets/ attachments/4544.pdf; Privette, *supra* note 104, at 15.

136. H.R. Res. 83, 113th Cong. (2014) (enacted).

137. Jim Hamilton, *Spending Bill Funds SEC and CFTC, Amends Dodd-Frank Swaps Push-Out Provision*, SEC. REG. DAILY (Dec. 12, 2014), http://www.dailyreportingsuite.com/securities/news/spending_bill_funds_sec_and_cftc_amends_dodd_frank_swaps_push_out_provision.

138. Cory Bennett, *SEC Weighs Cybersecurity Disclosure Rules*, HILL (Jan. 14, 2015); Andrew Lustigman & Mason A. Barney, *Legal Landscape for Cybersecurity Risk Is Changing as Federal Government and SEC Take Action*, INSIDE COUNSEL (May 8, 2015), http://www.insidecounsel.com/2015/05/08/legal-landscape-for-cybersecurity-risk-is-changing.

139. Cory Bennett, *Lawmakers Want SEC to Force Detailed Cyber Disclosures*, HILL (June 18, 2015), http://thehill.com/policy/cybersecurity/245428-lawmakers-want-sec-to-force-detailed-cyber-disclosures.

b. Cybersecurity Examinations

In addition to spelling out how public companies should meet their disclosure obligations, the SEC has placed increasing emphasis on cybersecurity in its examinations of investment advisors and investment companies, broker-dealers, exchanges and self-regulatory organizations, and clearing and transfer agents.[140] In January 2014, the Office of Compliance Inspections and Examinations (OCIE) outlined twelve priority areas for its National Examination Program including "Technology," which, in turn, included "information security."[141] By April, cybersecurity was the subject of its own "Risk Alert" bulletin.[142] The OCIE declared that it planned to,

> conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats."[143] The purpose of the examinations was to "help identify areas where the Commission and the industry can work together to protect investors and our capital markets from cybersecurity threats.[144]

Attached to the Risk Alert bulletin was a sample information request that OCIE might use in its upcoming examinations.[145] The request was highly detailed—28 requests, with as many as 14 subparts, some tracking the "Framework for Improving Critical Infrastructure Cybersecurity," released earlier in the year by the National Institute of Standards and Technology.[146] Selected broker-dealers would be required to disclose such information as:

- Which of a list of security practices a firm used, how often they were used, who was responsible for them, and if they were not used firm-wide, which parts of the firm did use them;
- A copy of the firm's information security policy;

---

140. These entities are subject to SEC cybersecurity requirements in Regulation S-P requiring them "to adopt written policies and procedures with administrative, technical and physical safeguards to protect customer records and information" and Regulation S-ID (requiring those regularly extending credit "to develop and implement written identity theft prevention programs designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.") Luke T. Cadigan & Sean P. Mahoney, *Developments in Cybersecurity Law Governing the Investment Industry*, 21 INVESTMENT L. 9–10 (2014).

141. 2014 EXAMINATION PRIORITIES, *supra* note 83, at 2.

142. RISK ALERT, *supra* note 8.

143. *Id.* at 2; Two weeks earlier, Commissioner Luis A. Aguilar told the Mutual Fund Directors Forum to "expect that SEC examiners will be reviewing whether asset managers have policies and procedures in place to prevent and detect cyber-attacks and whether they are properly safeguarding their systems against security risks." Luis A. Aguilar, Commissioner, SEC, Address at Mutual Fund Directors Forum 2014 Policy Conference: Taking an Informed Approach to Issues Facing the Mutual Fund Industry (Apr. 2, 2014), (transcript available at http://www.sec.gov/News/Speech/Detail/Speech/1370541390232).

144. RISK ALERT, *supra* note 8.

145. *Id.*

146. *Id.*

- Which of a list of network security practices a firm used; and
- The software or other method used to discover fraudulent attempts at customer transactions.[147]

"Cybersecurity" received its own heading in the "Examination Priorities for 2015."[148] The SEC expanded the prior year examination program directed at broker-dealers to include transfer agents in 2015.[149] Observers "expected that the SEC [would] expand its examinations to all U.S. public companies . . . ."[150]

In February 2015, after "the staff collected and analyzed information from . . . selected firms," the SEC released a summary of its findings.[151] In short, the SEC found, among other things, that of the 57 broker-dealers and 49 investment advisers examined: (1) most had been victims of cyberattacks; (2) the "vast majority . . . had adopted information security policies;" and (3) a smaller number—quite small in the case of investment advisers—applied their policies, periodic assessments, or training to vendors with access to their networks.[152]

c. Weaknesses in the SEC Response

The steps the SEC has taken suffer from serious shortcomings. For actual breaches, even though the Guidance reiterates the materiality standard, the SEC has required companies to disclose immaterial cyber incidents, which can cause either undue alarm or desensitization to events of true concern.[153] For cybersecurity risks, the Guidance does nothing to help investors evaluate the likelihood of a cyber incident with a material impact on operations.[154] Companies have responded to the Guidance with boilerplate language that fails to provide meaningful information.[155]

The OCIE cybersecurity examinations also pose a security risk. The SEC is gathering highly confidential information while its own system was recently criticized as insecure.[156]

147. *Id.* at app.

148. 2015 EXAMINATION PRIORITIES, *supra* note 92.

149. *Id.*

150. Stuart A. Krause et al., *Cybersecurity Insurance: It's Not Just for 'The Good Wife,'* CORP. COUNSEL (Feb. 5, 2015), http://www.corpcounsel.com/id=1202717092188/Cybersecurity-Insurance-Its-Not-Just-for-The-Good-Wife?slreturn=20150705005831.

151. SEC, OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, NAT'L EXAMINATION PROGRAM, CYBERSECURITY EXAMINATION SWEEP SUMMARY (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

152. *Id.*

153. SEC, DIV. OF INV. MGMT., *Cybersecurity Guidance* (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

154. *Id.*

155. Joseph Menn, *Major Companies Keeping Cyber Attacks Secret from SEC, Investors Report*, INS. J. (Feb. 2, 2012), http://www.insurancejournal.com/news/national/2012/02/02/233863.htm.

156. Daugherty, *supra* note 103.

d. The Guidance Has Been Ineffective

Investors read about what appear to be major cybersecurity breaches in the news and want to know how they have or will affect publicly-traded companies. They also need to know how likely a company is to suffer a breach that will materially affect operations. The disclosures following the Guidance have not provided this information.

In 2012 and 2014, Yahoo!, Inc., an American multinational technology company known for its web portal and search engine experienced two significant breaches.[157] Information associated with approximately one-half million user accounts was stolen in July 2012 through two separate weaknesses in Yahoo's cybersecurity architecture.[158] In early 2014, Yahoo experienced a breach of its email customer information through mobile code, which exploited a programming language vulnerability and impacted advertisements on Yahoo's webpages.[159] Nevertheless, the Yahoo 10-K reports for the fiscal years 2012, 2013, and 2014 contain almost identical language.[160] Neither of the cybersecurity breaches is described.[161] The topics of outsourcing of countermeasure functions and the purchase of cybersecurity insurance coverage are not present.[162] In the Risk Factors section, Yahoo acknowledges that there have been past breaches and may be future breaches, which have or could cause certain types of harm.[163]

Other companies experiencing breaches have not been any more illuminating about them in their 10-K reports. Apple, Inc., an American multinational technology company that designs, develops, and sells electronics, software, and online services, also experienced two breaches: the first in 2012 and another in 2014. In September 2012, Apple device identifiers along with personal data of their owners were stolen and then published on the Internet.[164] Later in 2014, invaders accessed celebrity iCloud accounts by breaching Apple's authentication system.[165] The Annual Reports for 2012, 2013, and

157. Katherine Bindley, *Yahoo Password Check: Has Your Email Account Been Compromised?*, HUFFINGTON POST (July 12, 2012, 4:58 PM), http://www.huffingtonpost.com/2012/07/12/yahoo-password-email-hack_n_1669047.html; Jay Rossiter, *Important Security Update from Yahoo Mail Users*, YAHOO.TUMBLR.COM (Jan. 30, 2014), http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users.

158. Bindley, *supra* note 157.

159. Rossiter, *supra* note 157.

160. Yahoo! Inc., Annual Report (Form 10-K) (Feb. 29, 2012), http://www.sec.gov/Archives/edgar/data/1011006/000119312512086972/d258337d10k.htm; Yahoo! Inc., Annual Report (Form 10-K) (Mar. 1, 2013), http://www.sec.gov/Archives/edgar/data/1011006/ 000119312513085111/d442073d10k.htm; Yahoo! Inc., Annual Report (Form 10-K) (Feb. 28, 2014), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

161. *Id.*

162. *Id.*

163. *Id.*; Yahoo! Inc. Annual Report (Form 10-K) (Feb. 27, 2015), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

164. Louis Goddard, *One Million Apple Device IDs with Personal Information Allegedly Stolen from FBI Laptop*, VERGE (Sept. 4, 2012, 9:22 AM), www.theverge.com/2012/9/4/3290789/antisec-fbi-udid-breach-iphone-ipad-apple.

165. Jacob Kastrenakes, *Apple Denies iCloud Breach in Celebrity Nude Photo Hack*, VERGE (Sept. 2, 2014, 2:41 PM), www.theverge.com/2014/9/2/6098107/apple-denies-icloud-breach-celebrity-nude-photo-hack.

2014 include the same general wording to describe business operations, cybersecurity issues, and the risks of breach.[166] The Form 10K reports that while a breach places customer relation and operations at risk, Apple has countermeasures in place to reduce the risk.[167] Facebook, Inc., the online social networking service experienced a breach of customer personal information during 2013.[168] While Facebook explains the reality of cybersecurity risks to customer relationships and operations, information describing the impact of the breach is not included in its 2013 or 2014 annual report.[169]

The reports of actual attacks, buried as they are with language about risk of future attacks, are further diluted because the SEC requires reports of immaterial cybersecurity events.[170] The Supreme Court recognized the effect of requiring insignificant information nearly forty years ago in *TSC Industries, Inc. v. Northway, Inc.*:[171]

> Some information is of such dubious significance that insistence on its disclosure may accomplish more harm than good . . . If the standard of materiality is unnecessarily low, not only may the corporation and its management be subjected to liability for insignificant omissions or misstatements, but also management's fear of exposing itself to substantial liability may cause it to simply bury the shareholders in an avalanche of trivial information—a result that is hardly conducive to informed decision making.[172]

Nevertheless, one commentator who studied correspondence between the SEC and ten large companies about cybersecurity observed "a kind of Kabuki exchange, in which the SEC would question the initial 10-K, the company would object to including more information because no attack has been material or materially adverse, the SEC would renew its request, and the company would concede, agreeing to include a sentence or two."[173] One such revised disclosure by the American International Group, Inc., acceptable to the

166. Apple Inc., Annual Report (Form 10-K), (Oct. 31, 2012), http://investor.apple.com/secfiling.cfm?filingid=1193125-12-444068&cik=; Apple Inc., Annual Report (Form 10-K), (Oct. 30, 2013), http://www.sec.gov/Archives/edgar/data/320193/000119312513416534/d590790d10k.htm; Apple Inc., Annual Report (Form 10-K), (Oct. 27, 2014), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=10264100-899-414610&type=sect&TabIndex=2&dcn=0001193125-14-383437&nav=1&src=Yahoo.

167. *Id.*

168. Facebook, Inc., Annual Report (Form 10-K), (Jan. 29, 2015), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=10436894-799-387648&type=sect&TabIndex=2&dcn=0001326801-15-000006&nav=1&src=Yahoo; Facebook, Inc., Annual Report (Form 10-K) (Jan. 31, 2014), http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=9741731-748-413456&type=sect&TabIndex=2&companyid=673740&ppu=%252fdefault.aspx%253fcik% 253d1326801.

169. *Id.*

170. SEC, DIV. OF INV. MGMT., *Cybersecurity Guidance* (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

171. 426 U.S. 438 (1976).

172. *Id.* at 448–49.

173. Matthew F. Ferraro, *"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 335 (2013–14). The ten companies studied were Amazon.com, Inc., American International Group, Inc., Anheuser-Busch Inbev SA/NV, ConocoPhillips, Inc., Eastman Chemical Company, Google, Inc., Hartford Financial Services Group, Inc., Quest Diagnostics Inc., Verizon Communications, Inc., and Wyndham Worldwide Corporation. *Id.* at 324–35.

SEC, illustrates the problem: "Like other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions."[174] From this sentence, an investor cannot determine whether AIG is reporting a devastating hack of customer data or the annoying spam email that anybody using the internet receives.

In disclosures about the risk of future attack, reporting companies cannot be and have not been expected to provide damaging details about their cybersecurity weaknesses. There is no mechanism allowing an investor to judge the vulnerability of a company. Rather, the focus has been on the types of possible cyber breaches and the harms a company could suffer from them. Yahoo, for example, provides an informative qualitative description, but investors are left perplexed about their real question: The likelihood of a cyber invasion with a material effect on operations.[175]

> Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.[176]

174. American International Group, Inc., Annual Report (Form 10-K) (Feb. 15, 2013), http://www.sec.gov/Archives/edgar/data/5272/000104746913001390/a2212976z10-k.htm.

175. Yahoo! Inc., Annual Report (Form 10-K) (Feb. 27, 2015), http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm.

176. *Id.*

e. Problems with the Cybersecurity Examinations

Gathering information about the level of preparedness among broker-dealers through special purpose examinations is an appropriate regulatory exercise. The trouble is the SEC has demanded highly sensitive information and its own cybersecurity system is flawed.[177] The question is whether that system is responsible for keeping sensitive information protected.

i. The SEC Has Serious Flaws in Its Own Cybersecurity

The United States Government Accountability Office (GAO) 2014 Fiscal Year Audit Report cites weaknesses in the SEC's comprehensive security environment in two major areas: (1) maintenance and monitoring of configuration baseline standards; and (2) implementation of password setting and network service standards.[178] The appropriate management of these two areas is critical in defending against breaches. An adequate defense is manifested through a comprehensive security policy that addresses the network, hosts, access points, applications, and user procedures.

The GAO report cited as issue number one, "maintenance and monitoring of configuration baseline standards" and recommended that SEC security management address the need for a comprehensive approach in the identification and management of security for all hardware and software within its technology infrastructure.[179] After a management process is designed and implemented, most remaining aspects of configuration management are automated to speed the process of applying software patches to correct problems that have been identified as security issues.[180] Organizations without viable configuration management are not able to respond quickly to the discovery of security issues in system software. As a result, they are vulnerable to a cyber-attack that exploits that weakness.[181] In 2015, the University of Southern California experienced a cyber breach in which hackers took advantage of a known security issue on a server. The breach would not have been possible if the available software patch had been installed on the server. This breach had the potential of putting 30–40,000 student records containing personal information at risk.[182] Like USC, the SEC is not protecting its technology infrastructure through comprehensive configuration management and has placed its network, data, and programs at risk.[183]

177. Sarah N. Lynch, *U.S. SEC on the Prowl for Cyber Security Cases*, REUTERS (Feb. 20, 2015, 4:07 PM), http://www.reuters.com/article/sec-cyber-idUSL1N0VU2AV20150220.

178. U.S. GOV'T ACCOUNTABILITY OFF., REPORT TO CHAIR, SEC, INFORMATION SECURITY: SEC NEEDS TO IMPROVE CONTROLS OVER FINANCIAL SYSTEMS AND DATA (2014).

179. *Id.*

180. *Id.*

181. Dave Shackleford, *Secure Configuration Management Demystified* 3, SANS INST. (2012), https://www.sans.org/reading-room/whitepapers/analyst/secure-configuration-management-demystified-35205.

182. *Examples of Security Breaches and Corresponding Recommended Practices*, VIVA UNIV. (Sept. 2012), https://vivauniversity.files.wordpress.com/2012/09/examplesofsecuritybreach.pdf.

183. U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-387R, MGMT. REPORT: IMPROVEMENTS NEEDED IN SEC'S INTERNAL CONTROLS AND ACCOUNTING PROCEDURES (2015).

The GAO report cited as issue number two, "implementation of password setting and network service standards" and recommended that the SEC address the need for a comprehensive approach to managing both administrator and end-user accounts.[184] These accounts have different levels of access to and control over organizational networks, programs, and data. An administrator account has unlimited access.[185] Technical support staff know the user name and password of the administrator account and can perform any task through this account.[186] The elevated privileges of this account give the user full control over the system.[187] This control is needed to support the system but can be abused to cause a data breach, complete unauthorized transactions, or interrupt system service.[188] Cyber breaches caused by the exploitation of administrator accounts are involved in many data breaches.[189] Neither Edward Snowden's National Security Administration breach nor the Target breach of late 2013 could have been successful without the compromise and exploitation of the privileged credentials of administrator-type accounts.[190]

A comprehensive approach, following industry-tested standards, for end-user accounts is also critical.[191] The GAO audit reports that the SEC did not consistently implement strong password controls for identifying and authenticating users.[192] Weak login security credentials is considered the root cause of the Anthem breach.[193] Organizations, like the SEC, should take a proactive approach to protect the integrity and privacy of confidential corporate and customer-client information by answering key questions like "Who has access to what?" and "What did they do?"

ii. The SEC Is Asking for Highly Sensitive Information

The OCIE is gathering information about the level of preparedness among broker-dealers through special purpose examinations.[194] The examination's request for very detailed information is separated into several topics including:

184. *Id.*

185. J. MICHAEL BUTLER, SANS INST., PRIVILEGED PASSWORD SHARING: "ROOT" OF ALL EVIL 2 (2012) (explaining that administrator user accounts are also known as root, super user, and domain admin accounts).

186. DAVID J. JOHNSON, SANS INST., THE USE AND ADMIN. OF SHARED ACCOUNTS 14 (2012).

187. BUTLER, *supra* note 185.

188. *Id.*

189. *Id.*

190. Press Release, Cyberark, New Report: Advanced Cyber Attacks Reliant on Privileged Credential Exploitation (June 11, 2014), http://www.cyberark.com/press/new-report-advanced-cyber-attacks-reliant-privileged-credential-exploitation/; Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBSONSECURITY (Sept. 21, 2015), http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

191. *The CIS Critical Security Controls for Effective Cyber Defense*, CTR. FOR INTERNET SEC. (Oct. 15, 2015), https://www.ciscecurity.org/critical-controls.cfm.

192. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 183, at 16.

193. Lance Whitney, *Anthem's Stolen Customer Data Not Encrypted*, CNET (Feb. 6, 2015), http://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/ ("Because an administrator's credentials were compromised, additional encryption would not have thwarted the attack.").

194. RISK ALERT, *supra* note 8 ("This document provides a sample list of requests for information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) may use in conducting examinations of registered entities regarding cybersecurity matters .... This document should not be considered all inclusive of the information that the OCIE may request.").

Identification of Risks/Cybersecurity Governance; Protection of Firm Networks and Information; Risks Associated With Remote Customer Access and Funds Transfer Requests; Risks Associated With Vendors and Other Third Parties; Detection of Unauthorized Activity; and the Other category for a wide range of information.[195] Much of the information in each of these categories is highly sensitive and could lead to a cybersecurity breach if accessed with criminal intent.[196]

Through the "Identification of Risks/Cybersecurity Governance" disclosure, the organization is revealing the details of how it has established and maintains cybersecurity policies governing its technology architecture.[197] An organization's technology architecture includes physical devices, software platforms, applications, data flow and storage, internal and external networking resources, and the user procedures.[198] Knowledge of the responsible personnel and the extent and timing of the inventory practices is highly sensitive. In general, cybersecurity breaches begin with reconnaissance.[199] Cyber attackers observe and probe an organization looking for entry and a plausible means to either disrupt the organization or steal information.[200]

To illustrate, a review of the information required in the OCIE examinations suggests the construction of a spear-phishing cyberattack in which the hackers would use social engineering tactics to gain access to an organization's technology resources.[201] From the insecure information obtained in the examination, hackers would learn the target personnel and could pose as an employee or vendor of the organization.[202] By revealing some highly sensitive information found in the examination report, the hacker would gain confidence of the target personnel.[203] The hacker would then request additional information or access privileges from the target personnel.[204] The Pentagon confirmed that its email system was breached through a spear-phishing attack aimed at one of its technology employees.[205]

The "Identification of Risks/Cybersecurity Governance" disclosure

195. *Id.* at 2.

196. *See id.* (highlighting sensitive categories where cybersecurity risk could exist for registered broker-dealers).

197. *Id.*

198. *See id.* (listing practices firms engage in for management of their information security).

199. Kelly Jackson Higgins, *How Lockheed Martin's 'Kill Chain' Stopped SecurID Hack*, DARK READING (Feb. 12, 2013), http://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125; Steve Hultquist, *Reconnaissance Is the Name of the Game in 2015*, SC MAG. (Jan. 1, 2015), http://www.scmagazine.com/reconnaissance-is-the-name-of-the-game-in-2015/article/390376/.

200. *Anatomy of Advanced Persistent Threats*, FIREEYE, https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html (last visited Mar. 6, 2016).

201. *See* FireEye, Inc., *Anatomy of a Spearphishing Attack*, YOUTUBE (Feb. 6, 2015), https://www.youtube.com/watch?v=2IUKrxVpw3M (describing cyberattacks where sophisticated hackers target individuals within an entity with privileged credentials using specifically tailored "bait" emails).

202. *Id.*

203. *Id.*

204. *Id.*

205. Tom Vanden Brook & Michael Winter, *Hackers Penetrated Pentagon Email*, USA TODAY (Aug. 7, 2015), http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/.

requests the description of "any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated."[206] This information is valuable in assessing an organization's ability to manage cybersecurity flaws because it identifies risks for which no countermeasure has yet been implemented.[207] It is also valuable for assessing weaknesses in an organization's technology infrastructure which can be used to initiate a cyber-attack.[208] This is the information needed by cyber-attackers to plan the entry and a plausible means to either disrupt the organization or steal information.[209]

Through the "Protection of Firm Networks and Information" disclosure, the organization identifies, if applicable, the standard model for its information security architecture and processes.[210] The disclosure also requests practices and controls regarding the protections of the organization's networks and information.[211] The first item on the list would catch the attention of a cyber-attacker: "written guidance and periodic training to employees concerning information security risks and responsibilities."[212] Employee activities generate the highest level of cybersecurity risk because they have detailed knowledge of the organization's operations and have access to its highly sensitive and valuable data.[213] The organization's guidance and periodic training of employees concerning information security and risks and responsibilities reveals the organization's posture on employee-generated cybersecurity risks.[214] For example, training related to the use of employee-owned devices on the company network along with document management guidelines are important to protect company operations and data.[215] Close evaluation of these practices can reveal weakness and provide the information needed by cyber-attackers.[216] Some organizations recognize the competitive advantage of employees conducting business operations without time and location restrictions.[217] Policies allowing the use of employee-owned devices support this agile computing environment, but special precautions and countermeasures are required to secure a processing environment that includes external devices.[218] It is not surprising that many organizations that allow

206. RISK ALERT, *supra* note 8 ("Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences.").

207. *See id.* (seeking information about firms' cybersecurity vulnerabilities).

208. *Id.*

209. FireEye, *supra* note 201.

210. RISK ALERT, *supra* note 8, at 2.

211. *Id.*

212. *Id.* ("Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.").

213. Rana Kanaan, *The Good, the Bad, and the Who-Knows About BYOD*, TECH.CO. (July 15, 2015, 11:00 AM), www.tech.co/good-bad-knows-byod-2015-07.

214. ERNST & YOUNG, *BRING YOUR OWN DEVICE SECURITY AND RISK CONSIDERATIONS FOR YOUR MOBILE DEVICE PROGRAM* (Sept. 2013), http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

215. *Id.*

216. *Id.*

217. Kanaan, *supra* note 213.

218. *Id.*

employee-owned devices to connect to the company network have experienced data breaches.[219] Through the information the SEC collected for its examination, the security management and policies for employee devices can be evaluated for weaknesses in protecting the organization from disruption and data breaches.

The disclosure topics "Risks Associated With Remote Customer Access and Funds Transfer Requests" and "Risks Associated with Vendors and Other Third Parties" address the cybersecurity exposure from providing external parties access to the internal network and sharing data.[220] Many organizations interact electronically with customers and suppliers, which builds and serves important relationships.[221] Operations are often designed so that the organization performs core competencies in-house and outsources remaining tasks.[222] Organizations implement an extranet, a secured private network that is accessed through Internet technology, to communicate and share data with customers and business partners.[223] Information the SEC collected about security weaknesses relating to third-party access could provide another path to cyber attack.

In late 2013, Target Corporation (Target) experienced a breach which resulted in the theft of 70 million customer debit and credit cards account information.[224] The breach was initiated when an HVAC vendor, using an authorized account, accessed Target's internal network and installed malware to collect the customer account information.[225] Target's supplier portal is accessible through a Google search and lists HVAC and refrigeration companies.[226] Cyber-attackers obtained access to Target's corporate network by compromising a third-party vendor.[227] The number of vendors compromised is unknown, but it only took one. Through a phishing email, an employee of the HVAC vendor installed the malware on the HVAC system.[228] Eventually, while accessing Target's network during a maintenance assignment at a Target site, the malware began the process of collecting Target's customer information.[229] Target's experience illustrates how an organization must protect the cybersecurity risk associated with its own technology architecture and the risk from all parties that interact with its

219. *Id.*

220. RISK ALERT, *supra* note 8.

221. Margot Slade, *BUSINESS TO BUSINESS; Sales? The Internet Will Handle That. Let's Talk Solutions,* N.Y. TIMES (June 7, 2000), http://www.nytimes.com/2000/06/07/business/business-to-business-sales-the-internet-will-handle-that-let-s-talk-solutions.html?pagewanted=all.EndFragment.

222. Laurie Collier Hillstrom, *Outsourcing*, REFERENCE FOR BUS. (2016), http://www.referenceforbusiness.com/encyclopedia/Oli-Per/Outsourcing.html.

223. Slade, *supra* note 221.

224. Meagan Clark, *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer*, INT'L BUS. TIMES (May 5, 2014, 11:39 AM), http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

225. Michael Kassner, *Anatomy of the Target Breach: Missed Opportunities and Lessons Learned,* ZDNET (Feb. 2, 2015, 8:29 PM), http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

systems. The examination request detailed information on how an organization evaluates external parties. Much of the information is highly sensitive and could lead to a cybersecurity breach if accessed with criminal intent.

C. *What the SEC Should Be Doing*

Cybersecurity breaches clearly pose a risk to an organization and its investors. The SEC protects investors by requiring disclosure of information material to their investment decisions and by overseeing the purchase-and-sale process.[230] The means by which the SEC directs the disclosure of cybersecurity management information and oversees cybersecurity in the market process should not increase the cybersecurity risk. Publicly reporting cybersecurity management policy and storing sensitive examination information in insecure SEC technology infrastructure increase the risk of cyberattacks.[231] Requiring reports of immaterial cyber breaches drowns out reports investors really need. There are alternatives that would give investors the information they need without providing the "roadmap" to criminals the SEC wants to avoid.[232] *First*, for actual cybersecurity breaches, reports should only be required when the events are material and should be required to include specific information. *Second*, to evaluate risk for the investor, companies could obtain and then publicly report a rating from a cybersecurity auditor. This would be a voluntary program; companies could continue to report cybersecurity issues as currently required. *Third*, broker-dealers and other participants in the market process could also be audited for cybersecurity as needed at the insistence of the SEC.

Companies should not be required to report cybersecurity breaches that are immaterial. Forcing companies to make the general disclosure that they have been breached will not be meaningful to investors if immaterial breaches are included. In determining whether the breach needs to be disclosed, the questions should be: (a) whether the breach could have a material effect on the financial position or operating results of the company; or (b) whether the breach indicates a fundamental flaw within the company system that will be impossible, expensive, or time-consuming to fix.

The general definition of materiality under the securities laws is well-settled: a fact is material if "there is a substantial likelihood that a reasonable shareholder would consider it important"[233] and that an "omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[234] The SEC has eschewed a

230. *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, SEC (last updated June 10, 2013), https://www.sec.gov/about/whatwedo.shtml.

231. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

232. TOPIC NO. 2, *supra* note 7.

233. Basic Inc. v. Levinson, 485 U.S. 224, 231 (1988).

234. TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

quantitative bright-line approach to materiality in the context of numerical misstatements on financial filings,[235] but some have cited a rule of thumb of "five to ten percent or more."[236] Costs to remediate cybersecurity breaches can reach these numbers, but breaches can be material even if they do not.

A breach of cybersecurity, even if not immediately material in a financial sense (because of the size of the company or insurance coverage), can still be material if it compromises future business operations. A cyberbreach may expose a widespread problem in the comprehensive cyber security of an organization. Sony Corporation, which has annual revenues over $70 billion, suffered three system breaches during 2011 through the use of Structured Query Language (SQL) injections to extract information from databases using Web interfaces.[237] SQL injection attacks involve sending modified SQL statements to a Web application that, in turn, modifies a database.[238] Attackers send unexpected input through their Web browsers that enable them to read from, write to, and even delete entire databases.[239] SQL injection can even be used to execute commands on the server.[240] It is a common attack method for many high-profile attacks.[241]

Based on news reports, the Sony breaches were orchestrated by the hacktivist organizations LulSec and Anonymous as revenge for the "persecution" of George Holtz.[242] Holtz was being sued by Sony for circumventing its copyright protections and jailbreaking its PlayStation 3 platform.[243] The first attack occurred on April 17, 2011 when information from over 70 million accounts was stolen from the Sony PlayStation network.[244] The second occurred on May 1, 2011 when information from twenty-five million accounts was stolen from Sony Online Entertainment Services.[245] The third occurred on June 2, 2011 when information from one million accounts was stolen from Sony Pictures.com.[246] Sony's security

235. SEC, SEC STAFF ACCT. BULL.: NO. 99—MATERIALITY (Aug. 12, 1999), https://www.sec.gov/interps/account/sab99.htm.

236. SEC v. Antar, 15 F. Supp. 2d 477, 509 (D.N.J. 1998).

237. Cynthia Larose, *Once More into the Breach: Are We Learning Anything?*, WESTLAW J. BANK & LENDER LIAB. Aug. 1, 2011, https://privacyandsecuritymatters.mintzlevinblogs.com/wp-content/uploads/sites/6/2013/01/SonyCommentary_Larose1.pdf.

238. Tim Sammut & Mike Schliffman, *Understanding SQL Injection,* CISCO, http://www.cisco.com/c/en/us/about/security-center/sql-injection.html (last visited Mar. 6, 2016).

239. *Id.*

240. *Id.*

241. *Id.*

242. James Cook, *Here's Everything We Know About the Mysterious Hack of Sony Pictures*, BUS. INSIDER (Dec. 4, 2014), http://www.businessinsider.com/guardians-of-peace-hackers-sony-pictures-2014-12?r=UK&IR=T.

243. Sarah Jacobsson Purewal, *Sony Sues PS3 Hackers*, PCWORLD, http://www.pcworld.com/article/216547/Sony_Sues_PS3_Hackers.html (last visited Mar. 6, 2016).

244. Sebastian Anthony, *How the PlayStation Network Was Hacked*, EXTREMETECH, (Apr. 27, 2011, 9:07 AM), http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked.

245. Charles Arthur, *Sony Suffers Second Data Breach with Theft of 25m More User Details*, GUARDIAN (May 3, 2011, 2:00 AM), http://www.theguardian.com/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

246. *Sony's Hacking Woes Mount After PSN Breach (Roundup)*, CNET (June 23, 2011, 7:34 AM), http://www.cnet.com/news/sonys-hacking-woes-mount-after-psn-breach-roundup/; Julianne Pepitone, *Group Claims Fresh Hack of 1 Million Sony Accounts*, CNN MONEY (June 2, 2011, 6:50 PM),

measures were not strong enough to stop the SQL injection attack by the attackers.[247] However, after each attack, Sony indicated that it had strengthened its security to prevent future attacks.[248] Although monetary costs of the attack might not be material, at least not immediately, the series of attacks demonstrated a cybersecurity weakness and an inability to recognize its seriousness that might alter the total mix for investors.

Accordingly, materiality for cybersecurity breaches cannot be measured purely by the numbers. Management should be required to consider other factors that might cause the breach to have a significant impact on business operations and reputation, such as: (1) whether information technology is the business of the company or its use is incidental to sales; (2) whether the breach resulted from a flaw that was immediately repaired or will require major revisions to the components of the technology infrastructure; and (3) whether the breach was a single event or was repeated.

If a cybersecurity breach was material, investors need more information about it than the Guidance suggests. Informing investors that a material breach occurred, without more, is insufficient; additional information is necessary to have the "total mix" of information.[249] Moreover, that information should be immediate. In a Form 8-K report, the company should be required to disclose the date and timeframe of the breach (e.g., over a three-week period in June 2015), a general description of the type of information affected (e.g., customer credit card numbers), the approximate magnitude of the breach (e.g., one million customers), the estimated cost of remediation (e.g., costs to repair the system flaw and credit repair services for customers), the applicable insurance coverage, management's evaluation of the difficulty in repairing the flaw, if it is not already repaired, and the anticipated effect on the reputation of the company. Companies should not be required to disclose precisely how the attack occurred, since that might compromise their own future security or, once the flaw is fixed, the systems of their competitors.

For risks of future attack, the approach should be different. In the Risk Factors section, investors need to know whether a company is financially prepared for a material cybersecurity incident and how likely such a breach is. With respect to financial preparedness, management should be required to discuss its insurance or reserving practices for cyber breaches. This will allow investors to judge how well-prepared a company is compared with others in the market for a cyber event without increasing the danger of its occurrence. It is the second type of information, the likelihood of a successful cyberattack, which can cause problems. Disclosing vulnerabilities is counterproductive; it

---

http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/.

247. *See* Pepitone, *supra* note 246 (quoting the hackers "Lulz" website, "SonyPictures.com was owned by a very simple SQL injection.").

248. Larose, *supra* note 237 (detailing Sony costs and security tactics in the wake of the 2011 hackings, including "identity theft insurance for customers, improvements to network security, free access to content, customer support, and an investigation into the hacking incidents.").

249. Daugherty, *supra* note 103 ("While the guidance has had a positive impact on the information available to investors on [cyberattacks], the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cyber security practices.").

is more useful to hackers than to most investors.[250] Certified cybersecurity auditors would provide investors with the information they need: whether the company is using state-of-the-art countermeasures to ward off attacks. Companies would disclose a cybersecurity grade rather than expose their security plans. This would avoid providing the "roadmap" for attack that the SEC says federal securities laws do not require.[251]

Retaining experts is not a new approach. The SEC has required or permitted reporting companies to retain outside experts to express opinions in their annual filings before.[252] Expert audits provide investors and the SEC itself, when it does not have in-house expertise or staff,[253] independent verification of complex matters that are material to company reports. For financial statements it is mandatory: financial statements of reporting companies must be audited.[254] Oil and gas companies have the option of retaining outside experts to oversee their reserves.[255] Those companies representing that their reserves are prepared or audited by a third party must file reports based on the Society of Petroleum Evaluation Engineer's audit report guidelines.[256]

An audit is a systematic process of objectively evaluating an aspect of an organization.[257] External accounting auditors are "authorized by law to examine and publicly issue opinions on the reliability of corporate financial reports."[258] "The U.S. Congress shaped the external auditing profession and created its primary audit objectives with the passage of the Securities Act of 1933 and the Securities Exchange Act of 1934."[259] SEC regulations promulgated under these laws require independent financial audits of all publically traded companies.[260] Accountants conducting these audits become

250. *See* Amy Terry Sheehan, *Meeting Expectations for SEC Disclosures of Cybersecurity Risks and Incidents (Part One of Two)*, CYBERSECURITY L. REP. 1 (Aug. 2015), http://www.davispolk.com/sites/default/files/agesser.Cybersecurity.Law_.Report.aug15.pdf ("Regulators like the SEC have to find the right balance between encouraging companies to be helpful with investors by accurately and fairly disclosing their risks, and helping sort out what is and what is not material for investors, while not requiring companies to provide a roadmap for hackers as to where they are vulnerable.").

251. TOPIC NO. 2, *supra* note 7.

252. *Id.*

253. At the highest level, of the four current SEC commissioners, three are lawyers and one is an economist; none has any expertise in cybersecurity or information technology. *See Current SEC Commissioners*, SEC (Sept. 17, 2013), https://www.sec.gov/about/commissioner.shtml (containing biographics accessed by clicking on pictures of commissioners). The SEC is currently seeking employees with expertise in "information security technology." *Invest in Your Career at the SEC*, SEC (Oct. 16, 2014), http://www.sec.gov/jobs/jobs_fulllist.shtml.

254. 17 C.F.R. pt. 210 (2015); United States v. Arthur Young, 465 U.S. 805, 819 n.15 (1984); *All About Auditors: What Investors Need to Know*, SEC (June 24, 2002), http://www.sec.gov/investor/pubs/aboutauditors.htm.

255. Paul R. Bessette et al., *Securities Litigation and the Energy Sector*, 33 ENERGY & MIN. L. INST. 10 (2012).

256. Modernization of Oil and Gas Reporting Requirements, 74 Fed. Reg. 2158 (Jan. 1, 2010) (to be codified at 17 C.F.R. pts. 210, 211, 229, 249).

257. *Audit*, NEW OXFORD AM. DICTIONARY 103 (2d ed. 2005), http://www.oxforddictionaries.com/us/definition/american_english/audit (last visited Feb. 15, 2016).

258. *Audits, External*, INC., *http://www.inc.com/encyclopedia/audits-external.html* (last visited Mar. 6, 2016).

259. *Id.*

260. *Id.*

familiar with the bookkeeping procedures of the client.[261] A final report to management often includes "recommendations on methodologies of improving internal controls."[262] External auditors compile an audit report, which formally sets forth the independent auditor's findings about the business's financial statements and conformity with generally accepted accounting principles.[263] The audit report includes an "opinion paragraph" which includes the auditor's formal announcement "on whether the statements are in accordance with generally accepted accounting principles."[264] A recommended approach for the external reporting of the cybersecurity management of an organization in order to disclose information about the risk to investors could be modeled after the external auditing practice of the organization's financial systems.

As an external auditor, a Certified Public Accountant (CPA) verifies the content of financial statements and the internal control over financial reporting.[265] The financial reporting-related information technology (IT) systems and data that are examined through the external auditing process are a subset of the aggregate systems and data an organization uses to support its overall business operations.[266] The financial accounting audit responsibilities do not encompass an evaluation of cybersecurity risks across the entire technology platform of an organization.[267]

To address these concerns for investors, stock companies could retain cybersecurity auditors to issue graded opinions. A cybersecurity auditor validates attainment of three security goals, referred to as the CIA Triad: confidentiality, integrity, and availability.[268] Confidentiality means that sensitive information cannot be read either while on a computer or traveling across a network.[269] Integrity means that attackers cannot change or destroy information in a computer or network without detection and that changed or destroyed information can be restored.[270] Availability means that people who are authorized to use information are not prevented from doing so by a computer or network attack.[271]

To verify that an organization is meeting these goals, the cybersecurity

261. *Id.*

262. *Id.*; AICPA, *Communicating Internal Control Related Matters Identified in an Audit*, OVERALL OBJECTIVES OF INDEPENDENT AUDITOR AU-C § 265 (2012).

263. *Audits, External*, *supra* note 258.

264. *Id.*

265. *Id.*

266. *See CAQ Alert #2014-3: Cybersecurity and the External Audit*, CTR. FOR AUDIT QUALITY (Mar. 21, 2014, 4:47 PM), http://www.thecaq.org/docs/alerts/caqalert_2014_03.pdf?sfvrsn=2 (stating "[t]he financial reporting-related information technology (IT) systems and data that may be in scope for the external audit usually are a subset of the aggregate systems and data used by companies to support their overall business operations and may be separately managed or controlled").

267. *See id.* ("The financial statement and ICFR audit responsibilities do not encompass an evaluation of cybersecurity risks across a company's entire IT platform.").

268. RANDALL J. BOYLE & RAYMOND R. PANKO, CORPORATE COMPUTER SECURITY 3 (4th ed. 2014).

269. *See* Ed Tittel, ABCs OF IT SECURITY FOR CPAS: A CPAS INTRODUCTION TO IT POLICIES AND PROCEDURES 2 (2008), https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/CyberSecurity/DownloadableDocuments/ABCsSecurity2_PolicyProcedure.pdf (last visited Mar. 6, 2016) (describing the general application of the CIA's "confidentiality" tenet to cybersecurity).

270. *Id.*

271. *Id.*

auditor must examine the entire technology infrastructure including the network architecture, authentication systems, operating and application software systems, data management systems, and user procedures. Comprehensive security considers the strength of the cohesive operation of the security provisions in each component of the technology infrastructure. In addition, the cybersecurity auditor examines management policies and practices, including: assets management; human resources security; physical and environmental security; communications and operations management; access control policies; information systems acquisitions, development, and maintenance; information security incident management; business continuity management; and compliance.[272]

Cybersecurity breaches occur through vulnerability in the system security management of the technology infrastructure.[273] Many companies use one or more IT governance frameworks to guide them in developing a disciplined security management process because securing the technology infrastructure is too complicated to be managed informally.[274] A security management governance framework specifies the formal processes (planned series of actions) for planning, implementation, and oversight.[275] Several factors may motivate firms to formalize their security processes to minimize risk to their technology infrastructure. Motivators include: the high dependence on technology for business operation; direct and indirect expenses associated with cybersecurity incidence; and a growth in the number of compliance laws and regulations.[276] Many compliance regimes require firms to adopt a specific formal governance framework to drive security planning and operational management.[277] The most common governance frameworks include COSO, CobiT, and ISO/IEC 27000.[278]

The COSO and CobiT are self-certifying governance frameworks designed to guide implementation internally within an organization.[279] The Committee of Sponsoring Organizations of the Treadway Commission

272. *ISO/IEC 27002:2013: Information Technology, Security Techniques, Code of Practice for Information Security Controls*, ISO (Oct. 1, 2013), https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

273. *The Eight Most Common Causes of Data Breaches*, DARKREADING (May 22, 2013, 6:22 AM), http://www.darkreading.com/attacks-breaches/the-eight-most-common-causes-of-data-breaches/d/d-id/1139795 1139795; *see generally* SYLVESTER NGOMA, VULNERABILITY OF IT INFRASTRUCTURES: INTERNAL AND EXTERNAL THREATS (2012), http://www.congovision.com/IT-Security-Pub.pdf (describing general vulnerabilities commonly leading to cybersecurity breaches).

274. TED G. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY: DEFENDING A NETWORKED NATION 8 (2014).

275. BUS. SOFTWARE ALLIANCE, INFORMATION SECURITY GOVERNANCE: TOWARD A FRAMEWORK FOR ACTION 5 (2003), https://www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf ("A governance framework is important because it provides a roadmap for the implementation, evaluation and improvement of information security practices. An organization that builds such a framework can use it to articulate goals and drive ownership of them, evaluate information security over time, and determine the need for additional measures.").

276. BOYLE & PANKO, *supra* note 268, at 65.

277. *Id.* at 116.

278. *Id.* at 111.

279. *The Committee of Sponsoring Organizations (COSO)*, CHI. ST. UNIV., https://www.csu.edu/internalaudit/cosoandcobit.htm (last visited Feb. 15, 2016).

(COSO) provides a general control planning and assessment tool to organizations for guidance on enterprise risk management, internal control and fraud deterrence, and reduce the extent of fraud in organizations.[280] The framework includes seventeen principles across the five components of internal control.[281] The framework focuses on process controls, which include the security management of these controls.[282] Control Objectives for Information and Related Technology (CobiT) is a framework for information technology (IT) management and IT governance.[283] CobiT is strongly preferred for the establishment of an organizations cybersecurity management policy by U.S. IT auditors because it was created by the ISACA, the primary professional association for IT auditors in the United States.[284] CobiT includes four domains: planning and organization; acquisition and implementations; delivery and support; and monitoring.[285] Like the COSO tool, the focus of the CobiT framework is on internal control.[286]

The ISO/IEC 27000 series consists of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).[287] The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system.[288] The series design is broad in scope including privacy, confidentially, and IT security issues.[289] It may be applied to organizations independently of size or structure.[290] ISO/IEC 27001 specifies how to certify organizations as being compliant with the ISO/IEC 27002.[291] The focus of the ISO/IEC 27000 framework is specifications for an external review of an organization's system security management.[292]

280. *About Us*, COMM. SPONSORING ORGS. TREADWAY COMM'N, http://www.coso.org/ aboutus.htm (last visited Feb. 29, 2016).

281. J. STEPHEN MCNALLY, THE 2013 COSO FRAMEWORK & SOX COMPLIANCE: ONE APPROACH TO AN EFFECTIVE TRANSITION 5 (2013).

282. Ken Tysiac, *Align Your Controls with COSO's Principles*, J. ACCT. (Dec. 15, 2013), http://www.journalofaccountancy.com/news/2013/dec/20139279.html.

283. *What Is COBIT 5?*, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/cobit/pages/default.aspx (last visited Feb. 29, 2016).

284. BOYLE & PANKO, *supra* note 268, at 114; *What Is COBIT 5?*, *supra* note 283; *About ISACA*, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Feb. 29, 2016) ("[A]n independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.").

285. *Control Objectives for Information and Related Technology (COBIT)*, THE281GROUP, http://www.the281group.com/index.php/control-objectives-for-information-and-related-technology-cobit (last visited Mar. 6, 2016).

286. *Id.*

287. *An Introduction to ISO 27001, ISO 27002FalseISO 27008*, ISO 27000 DIRECTORY, http://www.27000.org (last visited Mar. 6, 2016) ("The ISO 27000 series of standards has been specifically reserved by ISO for information security matters.").

288. *ISO 2700 Series Security Standards*, CASTLE FORCE IT SEC., http://www.castleforce.co.uk/Compliance/ISO27001.aspx (last visited Feb. 29, 2016).

289. *Id.*

290. *Id.*

291. *Id.*

292. BOYLE & PANKO, *supra* note 268, at 116.

The cybersecurity auditors, following the ISO/IEC 27000 framework's specifications on the verification of an external review of an organization's system security management, will become acquainted with flaws in cybersecurity management policies and procedures. The final report to management should include recommendations for improving the cybersecurity controls. The external cybersecurity auditor should issue an audit report that formally sets forth the independent auditor's findings about the business' cybersecurity management policy and the level of conformity with the ISO/IEC 27000 framework. The audit report includes an *opinion paragraph,* which includes the auditor's formal announcement on whether the organization is in accordance with ISO/IEC 27000 framework. Various audit opinions should be defined which indicate that the organization confirms or does not confirm. The opinions should be worded so that they reveal neither the specifics of the organization's cybersecurity policy nor any particular vulnerability. The opinions could be issued in accordance with a rating system.

External auditors certified in cybersecurity management could be authorized by law to examine and publicly issue opinions on the reliability of the cybersecurity management of a business. Cybersecurity auditors typically hold certifications to validate their expertise.[293] Internationally recognized certifications of IT audit competency include the Certified Information Systems Auditor (CISA) credential by ISACA and the Certified Information Systems Security Professional (CISSP) backed by ISC, the globally recognized organization dedicated to advancing the information security field.[294] Both certifications meet the ISO/IEC Standard for information security.[295]

If cybersecurity audits were required for all publicly traded companies, initially, there would not be enough experienced CISAs and CISSPs to go around. Although there are about 100,000 CISAs[296] and 100,000 CISSPs[297] worldwide as of 2015, most have careers within industry and not in auditing.[298] The program would have to be voluntary and companies would have the alternative of disclosing cybersecurity issues as currently required. As the cybersecurity grade becomes accepted by investors, their market behavior would encourage companies to have their cybersecurity systems audited. The role of the SEC would be to establish a standardized grading system, in conjunction with the ISO and IEC, which would provide consistent and meaningful information to investors when companies choose to be audited. The grading system would give investors the information they need about risk without increasing the exposure of reporting companies.

293. Kevin Beaver, *Best Practices for Choosing an Outside IT Auditor*, TECHTARGET (Sept. 2004), http://searchsecurity.techtarget.com/tip/Best-practices-for-choosing-an-outside-IT-auditor.

294. *Id.*

295. *Id.*

296. *Certified Information Systems Auditor (CISA) Fact Sheet*, INFO. SYS. AUDIT & CONTROL ASS'N, http://www.isaca.org/About-ISACA/Press-room/Pages/CISA-Fact-Sheet.aspx (last visited Mar. 6, 2016).

297. *(ISC)² Member Counts*, (ISC)², https://www.isc2.org/member-counts.aspx (last visited Mar. 6, 2016).

298. Certified Information Systems Auditor, *supra* note 296.

Similarly, cybersecurity auditors could be used to assess the preparedness of the purchase-and-sale process, such as broker-dealers, transfer agents, and the markets themselves. Rather than conduct this function in-house where it has its own security problems, the SEC could entrust this function to cybersecurity experts whenever the agency determined that such an examination was necessary. This would permit the SEC to obtain the information necessary to gauge cybersecurity risks to the markets and its operators without adding to those risks through the examination process.

III. CONCLUSION

Startling headlines about cybersecurity breaches are a matter of concern to investors in publicly-traded companies. The types of information involved, the methods of breaching security, and the number of people affected vary widely. Protection is only as strong as the weakest link—the company must protect against every imaginable way in, since the hacker only needs to find one opening. To date, the impact on share price has been delayed while the effects of the breach are measured, but stock price has reacted negatively once the costs of remediation emerge.[299]

The SEC is charged with protecting investors by (1) requiring public companies to disclose information material to their investment decisions; and (2) ensuring the integrity of the markets themselves through examinations of broker-dealers, exchanges, and others involved in the selling process.[300] Regarding cybersecurity, the agency spelled out what companies are expected to disclose under existing requirements.[301] It also stressed that the securities laws did not require companies to give hackers a roadmap.[302] Its Guidance, however, has yielded useless boilerplate disclosures from the companies addressing the subject at all. In some cases, the SEC has demanded that individual companies follow up with immaterial information more likely to confuse investors.

The SEC has also conducted a special purpose sweep examination of broker-dealers to assess their preparedness for cyberattacks, requiring detailed, specific information about methods used to ward them off.[303] Because the SEC has its own cybersecurity flaws, questions arise as to whether the information it collects is kept secure.

The SEC has an important role in making sure investors have the information they need about company cybersecurity risks and incidents and in ensuring the markets themselves operate free of cyber vandalism. The approach taken to date, however, needs to be substantially reworked. Cybersecurity breaches should not have to be reported unless they are material

299. Sebastien Gay, *Strategic News Bundling and Privacy Breach Disclosures* 4, U.S. FED. TRADE COMM'N (unpublished manuscript) (Aug. 21, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/09/00017-97599.pdf.

300. *The Investor's Advocate*, *supra* note 230.

301. RISK ALERT, *supra* note 8.

302. *Id.*

303. CYBERSECURITY EXAMINATION SWEEP SUMMARY, *supra* note 151.

to the company, either financially or to business operations or reputation. If they are material, then specific information should be required in a Form 8-K report. The risk of future breaches should be treated differently. The agency should adopt rules permitting reporting companies to disclose ratings from outside cybersecurity auditors and should use such certified auditors to collect information about broker-dealers and others involved in the purchase-and-sale process. This would provide the market and the SEC with the information they need without disclosing specific weaknesses to those who would exploit them. Finally, to assess cybersecurity readiness among securities markets and those involved in the purchase-and-sale process, the SEC should retain cybersecurity auditors to perform examinations rather than collect highly sensitive information in-house.

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.

[49] 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.

[50] 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.

[51] "About FINRA," FINRA website, available at http://www.finra.org/about.

[52] *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.

[53] *Id.*

[54] "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.

[55] FINRA Report, page 5.

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

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

[58] *Id.*

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

[60] *Id.*

[61] 18 U.S. Code § 1030.

[62] 18 U.S. Code Chapter 119.

[63] 18 U.S.C. §§ 2510-2522.

[64] 18 U.S. C. Chapter 206.

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

[66] 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.

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

[68] *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.*

[69] 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=.

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

[71] *Id.*

[72] *Id.*

[73] *Id.*

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

[75] "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.

[76] *Id.*

[77] *Id.*

[78] 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.

[79] 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.

[80] 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.

[81] *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.

[82] *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_.

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

[84] "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.

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

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

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

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

[89] *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.

[90] 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.).

[91] 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.

[92] 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 ...."

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

[94] 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.

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

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

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

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

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

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

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

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

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

[104] *Id.*

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

[106] *Stone*, 911 A.2d at 370.

[107] *Caremark*, 698 A.2d at 967, quoted in Stone, 911 A.2d at 372.

[108] Delaware General Corporation Law (DGCL), Title 8, § 141 (e.,

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

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

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

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

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

[114] Securities Act of 1933, Section 11.

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

[116] *Id.* at 289.

[117] IU/Hanover article

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

[119] "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.

[120] *Id.*

[121] *Id.*

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

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

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

[125] *Id.* at 3.

[126] 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.

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] "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.

[131] *Id.*

[132] *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/.

[132] 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

Discovery COMMUNICATIONS
FINRA
Marriott
protiviti
Raytheon

KOGOD SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC