

Reproduced with permission from Corporate Accountability Report, 35 CARE, 02/23/2017. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## New NACD Cyber-Risk Handbook a Reminder of Critical Board Oversight Duties



BY ALAN CHARLES RAUL, COLLEEN THERESA BROWN  
AND DEAN C. FORBES\*

**O**n Jan. 12, 2017, the National Association of Corporate Directors (NACD) released its new “NACD Director’s Handbook on Cyber-Risk Oversight.” The NACD has suggested that directors can use this Cyber-Risk Oversight Handbook as a resource to “[l]earn foundational principles for board-level cyber-risk oversight” and gain insight into issues including how to:

- “allocate cyber-risk oversight responsibilities at the board level”;
- address “legal implications and considerations related to cybersecurity”;

\* Alan Charles Raul is the founder and leader of the Privacy, Data Security and Information Law practice at Sidley Austin LLP. He represents companies on federal, state and international privacy issues, including global data protection and compliance programs. Mr. Raul previously served as vice chairman of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, and of the U.S. Department of Agriculture, and Associate Counsel to the President. He can be reached at [araul@sidley.com](mailto:araul@sidley.com).

Colleen Theresa Brown is a partner with Sidley, where she focuses her practice on civil, criminal and constitutional litigation, internal investigations and privacy and information law. She has significant experience on privacy and data protection compliance, litigation and regulator enforcement actions. Ms. Brown can be reached at [ctbrown@sidley.com](mailto:ctbrown@sidley.com).

Dean C. Forbes is counsel with Sidley, where he advises on global privacy and compliance issues and has experience in the areas of privacy strategy, data governance and use, and consumer protection. Mr. Forbes can be reached at [dforbes@sidley.com](mailto:dforbes@sidley.com).

- “set expectations with management about the organization’s cybersecurity processes”;
- “improve the dialogue between directors and management on cyber issues”; and,
- “improve and enhance boardroom practices.”

The Cyber-Risk Oversight Handbook is part of the NACD’s “Director’s Handbook Series.” The Cyber Handbook provides cybersecurity oversight guidance and practical advice for board members of publicly traded and privately held companies, and non-profit entities, of all sizes and scopes and in all industry groups. The Handbook’s advice may also prove beneficial to government regulators and investors, companies involved in mergers and acquisitions, legal advisers, and others who support these organizations.

### A Proactive Means For Addressing Cyber Risks

High-profile breaches have launched the cybersecurity topic to the very top of the corporate hierarchy. The NACD Handbook sets forth five “Key Principles” that help frame cybersecurity issues, and promote a more proactive mindset to address cybersecurity risks:

- **Principle 1:** “Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT-issue.”
- **Principle 2:** “Directors should understand the legal implications of cyber risks as they relate to the company’s specific circumstances.”
- **Principle 3:** “Boards should have adequate access to cybersecurity expertise, and discussions about cyber-

risk management should be given regular and adequate time on board meeting agendas.”

■ **Principle 4:** “Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.”

■ **Principle 5:** “Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.”

The NACD Handbook’s provides practical overarching guidance, as well as nine Appendices of specific tips, templates, and resources for implementing the Handbook’s Key Principles and recommendations. For example, the NACD Handbook emphasizes that it is important for boards to be aware of the general risks that exist in the company’s “ecosystem” and to understand what “crown jewels” the company must protect, and how they are protected. A key recommendation in the Handbook is that boards and management need to work cooperatively on cybersecurity governance as part of broader enterprise risk management efforts, in order for the Key Principles to be effective. The Handbook also explains that boards should establish clear expectations that management: frame the company’s cybersecurity investment in terms of return on investment (ROI); inform the board about cybersecurity-related risks according to the board’s criteria for format, frequency, and detail; and, consider the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) in developing its defense and response posture. The guidance also warns directors to be mindful of potential tendencies by management to downplay the state of cyber risk.

In merger and acquisition scenarios, the NACD recommends that boards of directors ensure that management conducts a cyber-risk assessment for each stage of a transaction’s lifecycle. The guidance specifically recommends confirmatory due diligence during M&A on cyber risk and consideration of such risk in determining the transaction value. Before the deal closes, it is important to confirm that systems and processes are secure, and to quantify any risks that may impact the company after the deal closes.

## Expectations of Boards of Directors

Boards of directors are responsible for overseeing cybersecurity risk management as part of their broader duties to an organization. And, while the need for effective cybersecurity oversight is clear, processes to achieve that oversight appear to still be a work in progress. A 2015 survey of 200 directors of public companies revealed that 80 percent of directors say they discuss cybersecurity at most meetings. Yet, according to the survey, 66 percent lack confidence in their company’s ability to protect itself from cyber risk. A 2016 survey of independent directors and C-suite executives indicated that oversight of cybersecurity issues by board members of non-U.S./U.K. companies is further challenged, with 91 percent of respondents from such companies reporting that they are unable to interpret a cybersecurity report. Regulators increasingly articulate expecta-

tions that boards play an active role in managing cybersecurity risk. In highly-regulated industries such as financial services, where a number of regulators have overlapping jurisdiction, this expectation can be explicit, requiring that boards approve a firm’s written information security plan and receive reports from management at least annually on the status of the firm’s information security program. As the market becomes ever more sophisticated in considering cyber risk, increased expectations for internal controls and oversight may also come from shareholders. In response, forward-thinking companies are following the NACD’s advice to formally integrate cybersecurity into the board’s overall enterprise risk management process.

## SEC Guidance

The NACD Handbook reflects themes and incorporates considerations from recent guidance by the U.S. Securities and Exchange Commission (SEC) on obligations of publicly-traded companies to report cybersecurity risks. In particular, the Handbook’s practical advice for directors is consistent with 2011 and 2014 guidance provided by the SEC. In 2011, the SEC’s Division of Corporation Finance provided disclosure guidance, which provides that company SEC filings (e.g., Forms 10-K, 6-K, 20-F), 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.” The SEC recognized that cyber attacks may cause companies to incur significant costs and experience negative consequences, indicating that:

■ objectives of cyber attacks may include theft of financial assets, intellectual property, or other sensitive information;

■ cyber attacks may also be directed at disrupting the operations; and,

■ remediation costs may include liability for stolen assets or information and repairing system damage.

Additionally, the SEC’s 2011 guidance calls for disclosure, depending on the registrant’s particular facts and circumstances, and to the extent material, of:

■ aspects of business or operations that give rise to material cyber risks and the potential costs and consequences;

■ any outsourced functions that pose material risks and how the company addresses those risks;

■ cyber incidents experienced that are individually, or in the aggregate, material, including a description of the costs and other consequences;

■ risks related to cyber incidents that may remain undetected for an extended period; and,

■ relevant insurance coverage.

Indeed, the SEC appears to prefer disclosure to provide specific details regarding cyber risks, provided that such disclosures do not betray the very security measures that an organization may take to protect itself. The disclosure guidance provides the example of a company disclosing that it has experienced a material cyber attack where malware was embedded in its computer systems and customer data was compromised.

The SEC stated that the company should not only “disclose that there is a risk that such an attack may occur,” but “may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences” as “part of a broader discussion of malware or other similar attacks that pose a particular risk.”

Public statements by SEC commissioners reinforce the importance of board cybersecurity oversight responsibilities. At a conference at the New York Stock Exchange on June 10, 2014, SEC Commissioner Luis Aguilar warned that “boards that chose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.” Commissioner Aguilar suggested that boards consider the NIST Framework as a conceptual roadmap for assessing the company’s cybersecurity measures, explaining that many firms have chosen to create a separate enterprise risk committee of the board with primary responsibility for overseeing cybersecurity, in order to translate the NIST Framework into action. He also emphasized the importance of having the appropriate personnel to carry out the cyber risk management function and to provide regular reports to the board.

---

### **Public statements by SEC commissioners reinforce the importance of board cybersecurity oversight responsibilities.**

---

SEC guidance and the NACD handbook also demonstrate that boards must be familiar with the potential consequences of cyber incidents in order to evaluate both cyber risk and to consider whether their disclosures are appropriate. Guidance from the Division of Corporation Finance further indicates that disclosure is appropriate if, for example: the costs or consequences represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s operations, liquidity, or financial condition; an incident or risk may have a broad impact on the registrant’s financial statements; a cyber incident results in legal proceedings; or, a cyber incident poses a risk to the registrant’s ability to record, process, summarize, and report information in such a way that would render the company’s disclosure controls and procedures ineffective. Awareness and understanding of these potential consequences will help boards ask the appropriate questions and more strategically weigh the potential significance of cyber risks and incidents.

### **Benchmarking and Frameworks**

There is no one-size-fits-all guide for appropriate cybersecurity and information security controls. Organi-

zations of different sizes and security risks may exhibit varying levels of maturity with respect to implementation of controls, governance and oversight. However, there are useful benchmarks by which any organization may evaluate and improve its controls and preparedness.

One key benchmark strategy is to align your program with recognized cyber frameworks. These include the NIST Framework, the International Organization for Standardization (ISO) Guidelines for cybersecurity, or ISACA’s COBIT Framework. The NIST Framework, a voluntary risk-based cybersecurity framework for identifying, assessing, and managing cybersecurity risks in the nation’s critical infrastructure, has become a leading framework for internal benchmarking. The NIST Framework’s flexible approach uses five core functions—Identify, Protect, Detect, Respond and Recover—to organize cybersecurity recommendations and standards. And, as the NACD has pointed out, the NIST Framework can voluntarily be adopted by entities in the private sector. Further, the NACD Handbook states that directors “should set the expectation that management has considered the NIST Cybersecurity Framework in developing the organization’s cyber-risk defense and response plans.”

Certain federal and state regulators have also issued regulations and guidance materials that typically establish minimum standards. These, too, can be useful benchmarks. Enforcement actions by regulators, and in particular by the Federal Trade Commission, provide concrete examples of the consequences of when companies fall short of these minimum standards. Notably, the FTC has provided guidance indicating that the NIST Framework is consistent with the approach to information security that the agency has followed since the late 1990s—in over 60 law enforcement actions, and in business education guidance. Indeed, the application of each of NIST Framework’s core functions has been highlighted by the FTC in its case law.

### **NACD Cyber-Risk Handbook Guidance**

The NACD Handbook concludes that “directors need to continuously assess their capacity to address cybersecurity, both in terms of their own fiduciary responsibility as well as their oversight of management’s activities, and many will identify gaps and opportunities for improvement.”

Taken together, the NACD Cyber-Risk Oversight Handbook’s five Key Principles and recommendations, and the nine Appendices, provide boards of directors with practical information, in a manner that is consistent with guidance provided by the SEC and the NIST Framework, to help them in fulfilling their fiduciary obligations with respect to cybersecurity.

The Handbook is available at <https://www.nacdonline.org/Cyber>.