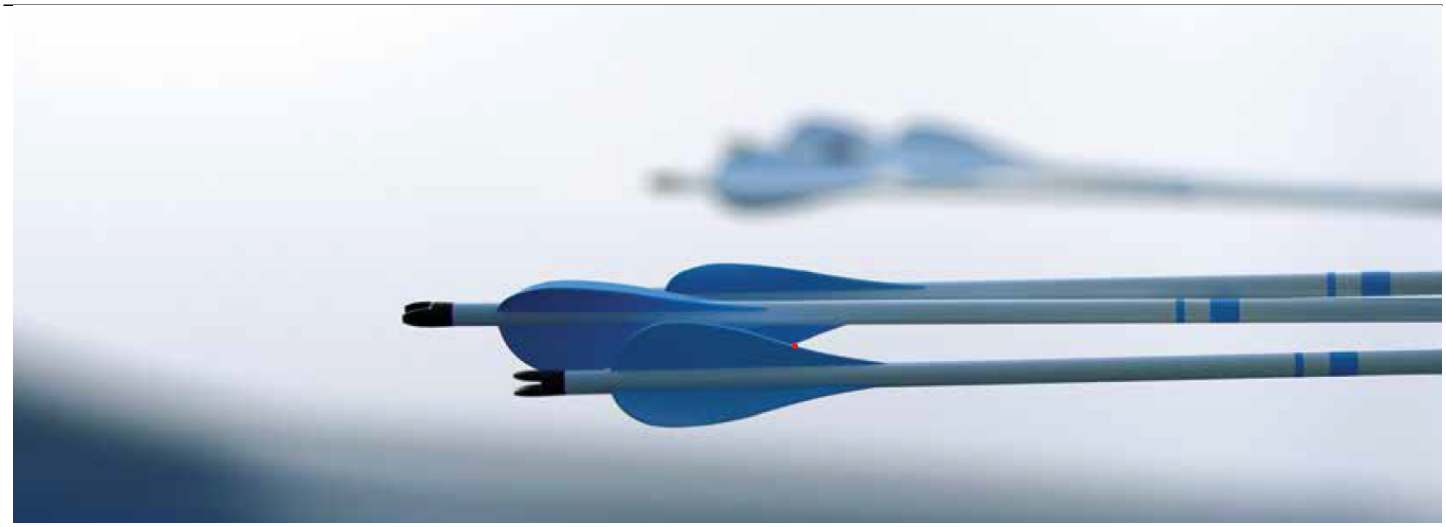
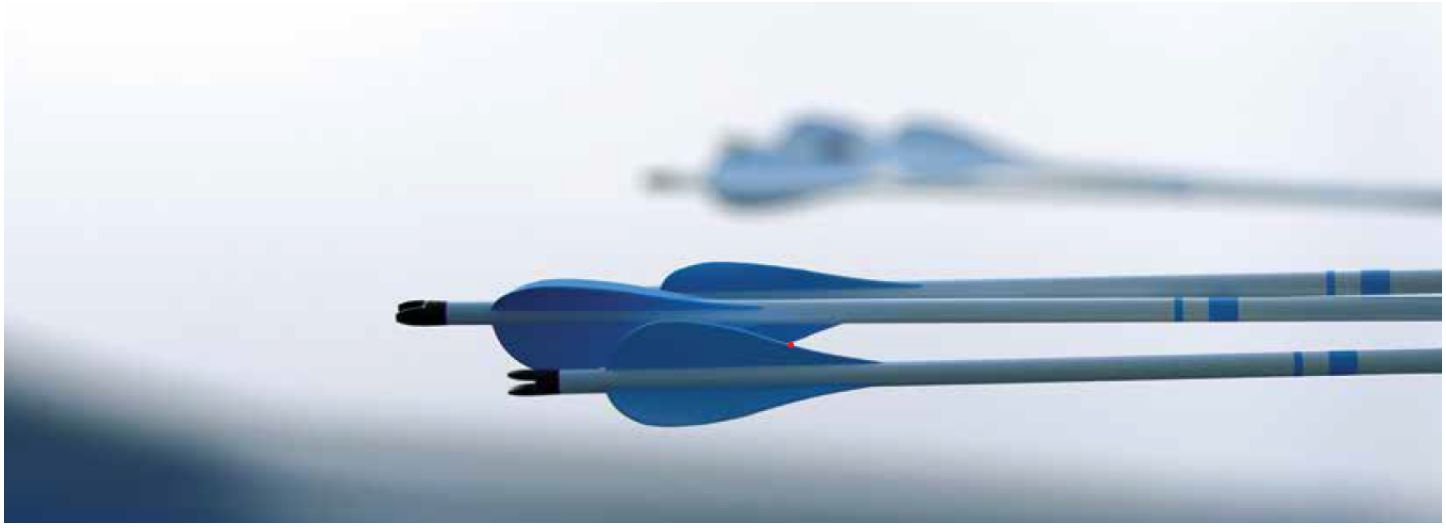


The Next Step in Cyber Risk Readiness

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Review and examine.*** Conduct a comprehensive review of your cybersecurity program and examine how cyber risk management practices are integrated into the business.
- ***Highest standards.*** Board members should look to model their company's cybersecurity standards after the National Institutes of Standards and Technology Cybersecurity Framework.
- ***Cyber insurance.*** Understand your current cyber insurance coverage, and identify what risks are not covered by it.
- ***Patch the holes.*** Address the company's basic vulnerabilities: lack of security awareness, poor technology patching, insecure code, inadequate crisis management plans, and immature technology management.

Cyber risks are dynamic, morphing, expanding, and shifting targets. They are constantly challenging our expectations and assumptions, and they are proving more difficult for businesses to prepare for and oversee than more familiar types of risk, such as natural disasters. Over the years, the scope of cyber risk for businesses has evolved from straightforward phishing schemes and data theft to more sophisticated cyberattacks designed to disrupt businesses and supply chains. And the risk exposures are only increasing as the rate of adoption of new technologies and digital devices within businesses continues to accelerate, creating an ever-larger surface for attackers to infiltrate and new opportunities for operational disruption.

The financial costs of cyber threats continue to grow. With the increase in material costs, the regulatory stakes are poised to rise as more regulators — particularly the US Securities and Exchange Commission (SEC) — begin to impose stricter requirements on businesses. While senior executives recognize that their operations are perpetually at risk and consistently rank cybersecurity as a top risk, SEC veteran Christopher Hetner, the National Association of Corporate Directors' (NACD) special advisor on cybersecurity and now a managing director within Marsh Risk Consulting, in conversation with NACD General Counsel and Managing Director Steve Walker, says most are struggling to effectively manage this risk in a cost-efficient manner.

NACD shared the following conversation between Hetner and Walker exclusively with ACC as part of NACD's ongoing commitment to provide expert content, services, and events related to cybersecurity oversight with the corporate governance community.

What resources exist specifically to address the unique board-level responsibilities related to cyber risk?

Walker: To address cyber risk from the board's vantage point, NACD partnered with the Internet Security Alliance to create the Director's Handbook on Cyber-Risk Oversight. Since its release in 2014, we have found that it is applicable to board members of public companies, private companies, and nonprofit organizations of all sizes and in every industry sector.

The handbook also was a catalyst for a broader initiative in partnership with Ridge Global and the CERT Division of the Software Engineering Institute at Carnegie Mellon University to create a cyber risk oversight certification. The goal of this program is not to create cybersecurity experts. Rather, the course is there to help board members and others in a position of oversight to better understand enterprise cyber risk issues. Directors earn a credential at the conclusion of this course.

During your four years at the SEC, how did you see cybersecurity regulation shift?

Hetner: Like many other regulating bodies, the SEC has for a number of years considered cybersecurity a top priority. The first major push came in 2011 when the Division of Corporate Finance issued guidance that called on companies to assess their disclosure obligations regarding cybersecurity risks and incidents. This was a good starting point, but it didn't go far enough in terms of setting expectations for both proactive and reactive cyber risk management.

When I joined the SEC in 2015 as senior cybersecurity advisor to Chair Jay Clayton, Chair Mary Jo White, and former acting chair Michael Piwowar, my role included helping to establish the SEC's position and shape its cybersecurity agenda.

In 2016, we focused on improving the coordination of cybersecurity policy efforts across federal financial regulators. We also improved the SEC's ability to assess cyber-related market risks and the SEC's own cybersecurity posture. These joint efforts across the commission's divisions and offices strengthened our ability to manage cybersecurity priorities, plan better for incident responses, and enhance threat intelligence capabilities.

In addition to my responsibilities as senior cybersecurity advisor, I also served as SEC senior staff representative to the US Treasury Department's Financial and Banking Information Infrastructure Committee, where I led the effort to enhance coordination and cooperation among federal financial regulators. My responsibilities included the oversight of efforts to harmonize cybersecurity regulations, respond to cyberattacks, and enhance market-wide cyber threat assessments.

The frequency and scale of breaches have prompted congressional inquiries, heightened investor expectations for corporations' oversight of cyber risk, and increased regulatory oversight of cyber risk management practices. This work culminated in the SEC unanimously approving new interpretative guidance in 2018 that outlined requirements for publicly traded companies to disclose cybersecurity risks and material incidents. This heightened focus will likely result in more intense cyber risk management requirements by the SEC and other regulatory bodies, as well as financial penalties for organizations that don't appropriately manage their cybersecurity exposures.

You mentioned that the SEC has taken a particular interest in cybersecurity. As the former senior cybersecurity advisor to the SEC chair, what advice would you give directors for navigating the regulatory landscape?

Hetner: During my time at the SEC, I helped to establish the commission's position and shape its cybersecurity agenda. I also provided leadership on enhancing coordination and cooperation among federal financial regulators.

> It's important to remember that basic cyber-hygiene practices are your first line of defense. Adversaries prey on organizations with poor cyber hygiene, often using basic tactics and methods such as phishing, social engineering, and malware to exploit existing vulnerabilities.

In my current role as special advisor on cyber risk for NACD, I regularly meet with board members from several organizations and industries and hear their reactions to the policies the commission worked to put into place. I frequently hear them talk about the need for actionable advice, and about the economic effect that cyber risk can have on their business.

And my advice to them is always:

- Conduct a comprehensive review across the cybersecurity program;
- Evaluate the governance structure;
- Ensure that the senior cybersecurity executive is in a position to influence the agenda across the enterprise; and
- Examine the cyber risk management practices and integration into the business.

It's important to remember that basic cyber-hygiene practices are your first line of defense. Adversaries prey on organizations with poor cyber hygiene, often using basic tactics and methods

such as phishing, social engineering, and malware to exploit existing vulnerabilities. As we saw with the NotPetya and WannaCry attacks, these breaches can have direct and potentially crippling business impacts.

I suggest that board members ask the following questions:

- Are we mapping our program to standards such as the National Institutes of Standards and Technology Cybersecurity Framework?
- Have we carried out a recent quantitative review to truly understand our exposure?
- What are the most sensitive assets that are susceptible to a cyberattack, and where are they positioned?
- What is our current insurance coverage, and are there any inherent or residual risks that are not addressed by it?
- What is our cybersecurity budget, and how are we spending it?
- Are we focusing on addressing the company's basic vulnerabilities, such as lack of security awareness, poor technology patching, insecure code, inadequate crisis management plans, and immature technology asset management?
- Is cybersecurity an integral piece of the enterprise risk management program?
- Is cybersecurity an integrated portion of our crisis management plan? Is that plan frequently tested?

It is imperative that the board understand how cybersecurity issues permeate the fabric of the company, and one of the best ways of gaining that wisdom is by having a collective discussion with the chief information security officer and other senior executives. This will help ensure there are integrated security processes across the organization. Your board should also implement a thorough cybersecurity planning and exercise strategy that is supported by continuous threat monitoring.

Do you think boards are getting the information they need from management to perform sound cyber risk oversight?

Hetner: The SEC has made it clear that it expects boards to understand, quantify, and oversee cyber risk. Unfortunately, the cyber risk information that boards typically receive from their general counsel, chief information security officers, and enterprise-risk teams does not always provide meaningful visibility into overall cybersecurity exposures. As part of my role within NACD, I have seen that the average public company director has, what I would describe as, a "headline cyber risk" understanding of cybersecurity. Because they are avid readers of the Wall Street Journal or the Financial Times, they are aware of notable breaches. However, they do not fully understand the cyber risk implications of integrating technology into their own critical business processes.

Walker: According to the 2018-2019 NACD Public Company Governance Survey, boards believe that they have improved their understanding of cyber risks. For example, 50 percent of directors indicate that cyber risk reporting from management is of much higher quality than it was two years ago. More than half of directors (52 percent) are confident that they sufficiently understand cyber risks to provide effective cyber risk oversight.

But from what we see in our board advisory services work at NACD, more improvement is needed. NACD faculty brief boards and C-suites in their boardrooms to help them gain visibility into the key metrics that provide clarity on cyber threats and progress on preventing them.

As Chris Hetner and other NACD faculty explain to boards, board members should have an idea of the cost of an attack on their business; an understanding of its likelihood; and a sound assessment of the effectiveness of their cyber capabilities, including people, processes, and technology, in mitigating this risk. Not only is it possible to project financial losses associated with a large cybersecurity event, but this has also become critical in order to effectively manage cyber risk and make informed decisions on risk transfer. Boards also need this information to comply with today's more rigorous investor inquiries and regulatory approach to cyber risk management.

Finally, what advice would you give corporate counsel in terms of keeping boards of directors informed on cyber risk issues?

Walker: Directors don't often feel that they lack information on cyber risk from management. Rather, they often feel like they have too much information, rendering the information useless. Boards need to work with experts and management to develop clear and compelling reports that capture only the information needed to monitor issues effectively.

Counsel also needs to stay abreast of emerging regulatory possibilities and translate to the board what compliance looks like. Finally, it is important for counsel to know whether or not the board itself could pass muster on a cybersecurity assessment of its own practices — for example, passwords for board portals, etc.

Hetner: As regulations around cybersecurity develop, legal and compliance roles become increasingly important in keeping other stakeholders informed and engaged. As part of its 2018 guidance, the SEC advises companies to disclose, as part of their proxy statement, the board's role and engagement in cyber-risk oversight, and notes that the discussion "should include the nature of the board's role in overseeing the management of [cyber] risk."

Effectively managing cyber risk requires the continuous risk management practices that are already being applied to other organizational risks. Board members must understand their cyber risk exposure, measure that exposure, and then decide how to guide management toward the ideal goal for the enterprise.

It's important to keep in mind that regulation is not going to slow down. As a board member, I would want to understand the regulatory landscape and how it applies to my industry and lines of business. And then I'd ask management how we can streamline our regulatory regimen to ensure that our cybersecurity program is unified while meeting local requirements.

ACC EXTRAS ON… Cyber risk

Articles

Quick Counsel: How to Hire, Train, Develop Objectives for, and Supervise a Records Management & Information Governance Team (Global) (March 2018).

Program Materials

Third-party Risk: Creating an Effective Information Security and Data Privacy Assessment Program for Third-party Vendors (Oct. 2016).

Sample Forms, Policies, and Contracts

Data Processing Clauses (compliant with the EU General Data Protection Regulation) (Sept. 2016).

Association of Corporate Counsel

Staff

ACC

Steve Walker



General Counsel and Managing Director

National Association of Corporate Directors

Christopher Hetner



Special Advisor on Cybersecurity

National Association of Corporate Directors

Hetner is the managing director of Marsh, the world’s leading insurance broker and risk adviser.