Cyber Risk
Director Network

February 10, 2020

CRDN

VIEWPOINTS

Cybersecurity: an evolving governance challenge

The increasing speed, miniaturization, and power of computing, as well as the connectivity of billions of devices, has led to deep change for even the most basic of industrial firms. *"We are fast becoming a tech company,"* said a director of one such enterprise.[1] *"If Amazon were to own our company, how would they reinvent us?"* Technologies such as 3D printing, 5G communication, augmented reality, and artificial intelligence offer alluring opportunities to the leaders of large, global firms. At the same time, they introduce unprecedented risks, unlike almost any that boards have thus far encountered. The director continued, *"It's a different conversation in the boardroom than we have had in the past. A cyberattack could wipe out a significant amount of our enterprise value. The wrong hiccup could cause a ripple effect throughout our economy."*

The Cyber Risk Director Network (CRDN) was founded to bring together business leaders and experts with a broad goal of enhancing national cybersecurity by strengthening board oversight of the largest US companies. The network's launch was sponsored by King & Spalding, an international law firm with a substantial data privacy and security practice, and by a grant from the William and Flora Hewlett Foundation, which saw the importance of catalyzing dialogue about cybersecurity among directors of large companies, top experts, and government leaders.

On December 11, 2019, CRDN members met in New York to discuss how the boards of large, complex companies oversee the evolving threat of cyber malfeasance. Professor Steve Weber of the University of California, Berkeley, joined the discussion, as did King & Spalding partners Scott Ferber, Zack Harmon, and Phyllis Sumner, along with Bill Phelps, executive vice president at Booz Allen Hamilton. For biographies of the guests, see Appendix 1 (page 12). For a list of meeting participants, see Appendix 2 (page 14).

Executive Summary

The conversation on the governance challenge posed by cyber threats focused on three themes: how the challenge differs from the familiar risks of the past, how boards are structuring their oversight of cybersecurity, and how boards and management are interacting on this crucial topic:

- **A new and different challenge for boards** (page 2). Cyber threats are constantly evolving, and the motivations and actions of bad actors are extraordinarily difficult to understand and predict. Risk governance models that have worked well in the past for physical and financial assets are, for the most part, proving inadequate for cyber risk.
- **A wide variety of oversight structures** (page 5). As cyber threats morph and grow, society is holding the boards of giant companies to account for failures to protect information assets and maintain privacy. Firms of the size and stature represented in the Cyber Risk Director Network often have highly sophisticated management systems for defending against cyberattacks and responding in a cyber crisis. But even in these firms, most boards are not satisfied that they have achieved mature practices for governance in this area.
- **Complex interactions between directors and management** (page 9). In many companies, boards entrust the chief information security officer (CISO) with responsibility for cybersecurity. But technology is so pervasive, information so distributed, and cybercrime so fluid that reports from the CISO to the board are, at best, table stakes in cyber assurance. Directors say they need to create further checks and build trust not only with their CISOs but across executive ranks, and in some cases at deeper levels of management than is customary.

A new and different challenge for boards

> *"It's never going to be routine: the landscape will continue to evolve; the bad actors will keep upping their game."* – Director

Cyber risk is tough to characterize and measure

Unlike almost any other risk, the impact of cyber risk is difficult to measure and can range from merely inconvenient to existentially threatening. One director said, *"The inputs and outputs of other risks are well known. You attribute a dollar impact and a likelihood. Cyber is more ephemeral; there's much more guesswork."* Another director noted that *"boards know how to deal with enterprise-wide risk—it's their core oversight function,"* but acknowledged, *"This risk is emerging, and boards are grappling with it. What's the particular vector? How will it impact us?"*

Risks can originate from the actions of employees, the leaders of powerful nation-states, and many actors in between. Additionally, cyber risk is always changing: *"The problem is that cybersecurity doesn't have a single meaning, and it is constantly evolving,"* a director noted. *"We need the ability to anticipate where risk exposure might be, and to prepare for it and protect against it. It's not static,"* said a director. This is frustrating for boards determined to exercise their duty of care to the highest standard. Conceptual confusion and inaccurate mapping of existing and potential risks to a firm's vulnerabilities can lead, experts warn, to underestimation of risk, confirmation bias, "aspiration-based risk taking," and overconfidence on the part of management and directors.[2]

What makes cyber risk unique?

Directors shared varied and nuanced views on the fundamental nature of cyber risk. Some said that cyber could be managed like other risks within a firm's enterprise risk management framework. *"We treat it as we treat security over any asset: do we have the right staff, resources, and procedures?"*

But most directors underscored the factors that distinguish cyber from other risks. One emphasized two unique characteristics of cyber risk: directors' lack of familiarity with the issues and companies' near-total dependence on the internet. *"Boards are illiterate about cybersecurity and the company's reliance on information technology. But enterprise access to the internet is fundamental to delivering value, and all those transactions that rely on access to the internet are inherently unsafe. That's not true of any other aspect of risk that boards deal with,"* the director said.

Another director stressed the newness of the dangers: *"For most enterprises, it's a brand-new risk associated with 21st-century business and social life that most directors didn't grow up with. We've shifted from physical risk of damage to the enterprise to one that's being manipulated remotely with tools beyond the expertise of most directors."*

Another director said that the many possible motivations for cyberattacks made defense planning more difficult. This director raised the possibility of *"someone entering your systems, spending several years there, and the company never understands why. And when it's discovered, dealing with a blizzard of litigation, although there was no manifest damage to any consumer."*

And then there is the matter of the sheer scale of the risk. One director spoke of impacts ranging from "*significant impairment"* to *"a crippling loss of competitive* *advantage."* Another observed, *"The risks are existential, depending on your business, even in manufacturing."*

The "black swan" aspect of cyber threats makes managing cyber risk particularly difficult. According to a new report, *Resilient Governance for Boards of Directors*, "cyber professionals and boards are mindful that a major cyber event (including the most impactful and catastrophic ones) could very well come from a surprising or unanticipated direction. That makes failures of cyber defense in some cases—possibly the most important ones—not a failure of operational rigor but rather a failure of imagination."[3]

But many breaches lead to no immediate financial or operational damage, and the report also notes, "It is hard to identify a major firm or government organization that has ceased to exist as a result of a cyberattack."[4] Nevertheless, much harm can be done: a relatively simple attack can halt the operations of an entire company for extended periods and cause the loss of hundreds of millions of dollars.

Who will manage cyber risk?

Many directors acknowledge that because cyber risk is new and rapidly evolving, their board oversight processes are immature. Even boards skilled at overseeing complex financial risks, such as major banks, are still learning how best to oversee cybersecurity in their firms, given customers' and managers' unending demand for technology and connectivity.

Until recently, many senior executives and outside directors tended to assume that management of cyber risk could be delegated to a firm's information technology (IT) professionals. However, as it has become increasingly clear that attacks present potentially existential risks, these top leaders are trying to engage more deeply in cyber matters. "Boards now feel a deep sense of urgency to exercise a central role in improving cybersecurity postures and outcomes for the firm," says the report on resilient governance, which observes, "Cyber risk is no longer confined to a set of operational decisions to be left solely in the hands of IT management."[5] One director warned, *"If we limit cybersecurity to just IT, we're leaving ourselves vulnerable because as the interface between IT and operational technology becomes blurred—through movement to the cloud, autonomous systems, process automation, big data, business-to-business interfaces—it isn't just IT per se … As our business processes and the processes of third-party vendors evolve, that dynamic risk is the one that we're not well set up to manage."*

Directors often have more limited experience than top managers in overseeing these new risks. One remarked, *"People throw around this terminology and don't really have much idea, or worse, they think they know."* Directors are keen to deepen their understanding by learning why their companies are using particular systems, how those systems connect to the business, and how the technology introduces vulnerabilities.

Boards also worry that their own skills, collectively and individually, may not keep pace with swiftly evolving cyber threats. *"Even if you have expertise on board,"* noted a director, *"if you're not practicing, you'll quickly be out of practice. How do we ensure that as a group we're thinking through the issues so that we can ask the right questions at the right time? How do we even know what we want to see on the dashboard?"*

A wide variety of oversight structures

Because cyber risks are so novel and evolve so rapidly, boards of large companies have developed many different structures for overseeing them. One director said, *"What we struggle with is, where does management end and the board begin from a governance perspective, when it comes to cybersecurity? There are lots of questions around knowing what to react to, how to react, and how to do it on a timely basis. You think about financial statements, and it's clear what our role as a board is; for something like cybersecurity, it's not."*

Another director asked, *"How would a board know whether what it's hearing is worth the time it takes to hear it? Management doesn't have any more literacy than boards do. Management and boards want to know what's the right thing to do. How do I know it's the right thing to do? How do I know that I'm doing it in the right way? What's the plus/minus variance that I should be OK with? How do I prove it to other people?"*

The models that boards use continue to evolve. A director described how, after a major breach, his audit committee decided to devote the first hour of every committee meeting to cyber matters: *"We invited every board member who wants to attend. Several do, some by phone."*

Members agreed that the full board bears ultimate responsibility for cybersecurity, but they discussed several models for operationalizing that oversight.

Oversight by the audit committee

Many boards delegate substantial oversight to their audit committee, which typically discusses cyber at every meeting. *"Cyber is important enough that the full board* *should have exposure,"* said one director, *"and they do this via the audit committee, which has primary responsibility for all things risk, including cyber. The full board is invited once a year to a long discussion led by key company personnel."* Some directors, however, were concerned that adding cybersecurity oversight to already crowded audit committee agendas may not always be effective, and that cyber could get crowded out by other items.

Another director noted that while oversight of cybersecurity usually defaults to the audit committee, this committee is not *"put together with cybersecurity expertise in mind, so their ability to do cybersecurity governance is not clear. What should happen is a robust discussion at the governance committee about the alternatives. That discussion should result in clear guidance on how cyber will be governed. In my experience—five public company boards—four of five defaulted to the audit committee; one has a technology committee, not uncommon with large, globally important banks."*

Oversight by other existing committees

One board considered existing committee responsibilities and ended up delegating cybersecurity oversight to its nomination and governance committee. *"It started with a foundational look at the workload of the board, the fiduciary obligations of the board, how they were allocated at the full board and on committees. Then we looked at risks in Qs and Ks, qualitative and quantitative. We sought to balance the workload of the committee. It seemed that nominating and governance and public affairs would be good for cybersecurity. After we made that allocation, we rethought the membership of the committees to make sure we had the right members for the role of each committee and this issue of overlapping membership."*

Another director reported that cybersecurity oversight belonged to the risk committee at one company, whereas at another it was with a technology subcommittee. *"We're still navigating how to include other committees: risk plus audit, risk plus finance, etc. Who needs to hear? Different elements belong in different committees,"* the director said.

Oversight by a cybersecurity committee

A few boards have created special cybersecurity committees. These can make sense for companies with strategic interests in IT or those that would benefit from a sharp governance focus on cybersecurity and cyber risk.

One board that elected to establish a cybersecurity committee is General Motors. Linda Gooden, the committee's chair, said that the board looked at its products, considered a future of driverless cars and the internet of things, and realized,

> Our number-one goal is safety for everyone who uses GM products and services by ensuring we are building products that are as cyber and tamper-proof as possible. To understand the challenges associated with achieving the objective, the board established a committee to look at cyber across GM. The committee spent the first year understanding and assessing the cyber environment; defining the approach and tools to be used to measure progress and identify areas for improvement; and developing the best techniques to inform the board in English. Our second year was devoted to institutionalizing best practices and testing to gain a better understanding of where the cyber programs could be strengthened. This year the cyber committee is being moved under the risk committee as part of the broader risk portfolio.[6]

Ms. Gooden said the cybersecurity committee "borrowed liberally from the audit committee for process and flow" and that it acts like an audit committee in that it functions as the eyes and ears for cybersecurity to validate what is being reported.[7]

John Inglis, a former deputy director at the National Security Agency, is currently chair of the IT oversight committee at FedEx. He explained why FedEx established an IT committee:

> In the last 10 years, it was apparent that as much as the strength of the business depended on good people and risk quality, it also depended on the quality of IT. More importantly, we believe that if you're talking about IT, which is a meld of technology and people and roles and responsibilities, you're really talking about an operational activity, not just an enabling one. IT is the lifeblood of FedEx, as it is for banks and other enterprises which stand on substantial and widespread digital infrastructure, so you need oversight at the board. Cybersecurity is a subset of that oversight. We didn't want to give less time to the topic.[8]

A CRDN director described how an attack on a major industrial facility led the board to create a special working group. *"The nature of risk is changing,"* the director said, *"and we're a rapid adopter of machine learning and artificial intelligence, maybe the most cutting-edge in our industry."* The board worried that security testing of industrial control systems was immature: *"We're not fully comfortable that we can test and* *assess at a high-quality level, given the sophistication of the systems we have in place."* The working group brings in external experts and seeks to establish indicators of cybersecurity performance. *"We're struggling,"* said the director. *"We may end up with a hybrid audit and HSE [health, safety, environment] structure to manage this risk. Someone has to stay at the leading edge."*

Oversight by the whole board

Some boards do not delegate cyber risk oversight. One director reported that cybersecurity *"comes before the board five times a year. We debated whether to have a cyber committee or house it in the risk committee; we decided on boardwide."* Another said that the full board *"discusses cyber several times a year, [with particular topics being covered] on a cadence of 18 months to two years. We cycle through every aspect of cybersecurity to build up literacy and an understanding of the reliance that the company has, the state of the infrastructure, new approaches, new strategies. It gives visibility to the board. Then we look at the broader environment. What is everyone facing? What are we facing?"*

Another director reported, *"Our entire board sets priorities and strategy for cyber. What's the strategy for how we think about cyber in the company? Where does it touch the company? How do we think about it? Who thinks about it—where do they sit and to whom do they report?"* Many agreed with a director who said, *"There need to be full-board discussions. No matter what committee is designated, there should be time for the full board."*

The "best" structures are likely to be company specific. One director remarked, "*Unfortunately, there's no right answer and no good answer here. It's very situational. You must start with the question, what is the risk that cybersecurity poses to the organization? Cybersecurity is a different kind of risk; it can impact different businesses in different ways, so you manage and govern differently. Regulated industries have their own nuances; critical-infrastructure companies have theirs."*

Regardless of the structures they use, boards need to ensure that they are fulfilling the oversight responsibilities that regulators and courts will demand. King & Spalding partner Phyllis Sumner described these as "table stakes":

- Reports that go to the full board.
- Deep dives—sessions devoted to cybersecurity, in a designated committee or the board as a whole. *"It's the amount of focus and time that the committee needs to ensure a real understanding of the risk,"* said Ms. Sumner.

- Education on cybersecurity, across the board.
- Risk, capability, and maturity assessments. *"The expectation is that the board will hear the results of assessments and the ways that management is addressing any gaps."*
- Third-party reports. *"Increasingly, outside experts come in to report directly to boards,"* Ms. Sumner commented, *"not just through management."*

These table stakes are minimum requirements, she noted, *"and expectations are much higher when a company is faced with a significant incident."*

Complex interactions between directors and management

In many risk areas, directors have found practical ways to assure themselves that management is aware of exposures and has put mitigation and recovery mechanisms in place. Building this confidence is never easy in a large global firm, but most directors and committees—risk and audit, for example—know which executives they need to be in dialogue with.

Directors at the CRDN meeting suggested that working with management on cyber issues is less straightforward. For example, most banks are able to identify who has authority to extend credit and to trace credit risk back to specific decisions. Cyber risks, in contrast, are hard to isolate—they crop up during product design, in a company's use of third parties, and every time an employee in any part of the firm responds to a phishing message. *"With the internet of things,"* said a director, *"people bolt things onto their systems; who knows how much we have?"*

Second, even where risk can be focused under the CISO, many directors worry about complacency or hesitation to pass along bad news. *"How are you getting assurance that what you're getting from management is accurate?"* asked Booz Allen Hamilton's Bill Phelps. *"The lights on the dashboard are all green until suddenly they turn red."* Mr. Phelps called for additional checks on a CISO's judgement and felt that these should happen at a level below the board. "*In one case,"* he said, *"internal audit became suspicious that the CISO was overconfident, but where were the internal checks and balances?"*

Cyber risk is sufficiently pervasive that a board's assurance will rarely come from answers to simple questions. One director noted that for a board to fulfill its oversight responsibility requires *"not just asking specific questions, but developing additional insight on the strength of the organization."* This may involve interrogating the skills of managers at a much deeper level than is usual for the board. *"When there's an intrusion,"* a member said, *"you'll deal with things you never thought of. So part of the exercise is to get a few layers beyond what's reported, in order to understand how management thinks about these problems."*

Directors discussed how they pursued this difficult goal. One described an intense set of interactions with executives across a global institution: *"I do half-days with people; I'll soon be at one of our cyber fusion centers."* The same company provided corporate email accounts for board members so that management could communicate with them in a safe and trust-building way. Yet not all management teams welcome such energetic oversight, and some experience it as a lack of trust. *"It's harder when companies are sensitive about the board intruding into supervision,"* noted a director.

Directors who focus on cyber risk need to do more than build trust and establish easy communication paths; they need to constantly sharpen their skills because digital transformation of large companies seems to be unceasing, and cyber risk is constantly shifting. *"It's a dynamic issue,"* said a director. *"A governance committee needs to be thinking about where we're going, not just where we are today."*

In some cases, the emergence of new technologies and new risks drives boards to change their models for cyber risk supervision. *"Committees should be looking at emerging topics,"* said a director, citing the firm's rapid adoption of artificial intelligence and machine learning. *"When the audit committee oversaw cyber, not many people were thinking about faking out the algorithms. Now, we need an annual discussion about whether we need a technology or risk committee."* Several directors were keen to find ways to assess their boards' current capabilities. *"The NIST [National Institute of Standards and Technology] Cyber Security Framework is an enabler,"* noted one director, *"but it's just a way to start a conversation, not a cure-all."*

* * *

Compared with risks that firms have managed for many decades, cyber risk is new, immature, and growing rapidly. Board governance of cyber risk is still in its infancy and far from stable. *"This kind of risk represents a unique set of competencies,"* noted a director. *"Not all audit committees or risk committees have the skills to match the issue. And it's evolving."*

About this document

The Cyber Risk Director Network (CRDN) was founded to bring together business leaders and experts with a broad goal of enhancing national cybersecurity by strengthening board oversight of the largest US companies. The network's launch was sponsored by King & Spalding, an international law firm with a substantial data privacy and security practice, and by a grant from the William and Flora Hewlett Foundation, which saw the importance of catalyzing dialogue about cybersecurity between directors of large companies, top experts, and government leaders. Tapestry Networks organizes and leads the network.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting directors, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Guest biographies

Scott Ferber is a partner in King & Spalding's Data, Privacy, and Security practice. He has held senior positions at the US Department of Justice (DOJ), during which time he led national security investigations involving international cyber threats and economic espionage. He has also been an assistant US attorney in Atlanta and has served as an assistant district attorney at the Manhattan District Attorney's Office.

At King & Spalding, Mr. Ferber counsels clients on the full range of privacy and security issues created by global data collection, use, storage, and transmission.

Zack Harmon is a partner in King & Spalding's Special Matters and Government Investigations practice. He has served in leadership roles in the DOJ and Federal Bureau of Investigation (FBI), including most recently as FBI chief of staff. While at DOJ and the FBI, Mr. Harmon oversaw hundreds of cases across the full spectrum of government investigations.

At King & Spalding, Mr. Harmon has defended clients ranging from individuals to Fortune 100 corporations in dozens of high-profile cases and enforcement proceedings. He has led extensive internal corporate investigations in over 30 countries.

Bill Phelps, a Booz Allen Hamilton executive vice president, leads the firm's US commercial business. As the commercial lead, Mr. Phelps drives the firm's advancement in cyber, analytics, cloud, internet of things, and agile systems development to address the most mission-sensitive challenges facing commercial organizations today. He also directs delivery of integrated consulting and advanced technology solutions to clients that include large commercial and investment banks, utilities, oil and gas companies, major retailers, auto manufacturers, and large pharmaceutical manufacturers.

Mr. Phelps is a trusted adviser to senior client executives, helping them understand and address complex cybersecurity challenges as well as broader technology-driven business disruption. He is also a widely respected keynote speaker and panelist at major security conferences, where he has spoken on topics related to cybersecurity, situational awareness, IT resiliency, and real-time compliance.

Phyllis Sumner is a partner with King & Spalding. She leads the Data, Privacy and Security practice and is the firm's chief privacy officer. Ms. Sumner has served as an assistant US attorney in the Northern District of Illinois and the Northern District of Georgia and has successfully prosecuted numerous high-profile cases involving public corruption, domestic terrorism, credit card fraud, money laundering, healthcare fraud, and other complex criminal matters.

At King & Spalding, Ms. Sumner regularly counsels corporate boards and senior executives on data breach prevention, emergency response, remediation, compliance, regulatory enforcement, internal corporate investigations, and other critical privacy and data security concerns. She assists clients with the development of mature incident response plans and leads them through security incidents, including investigations, containment, remediation, communications, and contractual and legal obligations.

Steve Weber is a professor in the School of Information and the department of political science at the University of California, Berkeley, and faculty director of the Center for Long-Term Cybersecurity. He is a specialist in international relations and international political economy with expertise in international and national security; the impact of technology on national systems of innovation, defense, and deterrence; and the political economy of knowledge-intensive industries, particularly software and pharmaceuticals.

Trained in history and international development at Washington University and in medicine and political science at Stanford, Professor Weber joined the Berkeley faculty in 1989. In 1992, he served as special consultant to the president of the European Bank for Reconstruction and Development in London. He has held academic fellowships with the Council on Foreign Relations and the Center for Advanced Study in the Behavioral Sciences and was director of the Institute of International Studies from 2004 to 2009. He is senior policy adviser with the Glover Park Group in Washington, DC, and actively advises government agencies, private multinational firms, and international nongovernmental organizations on issues of foreign policy, risk analysis, strategy, and forecasting.

Appendix 2: Meeting participants

CRDN members participating in all or part of the meeting on December 11, 2019 sit on the boards of over 29 public companies:

- Joan Amble: Zurich Insurance Group, Booz Allen Hamilton, Sirius XM
- Marianne Brown: Northrop Grumman
- David Ching: TJX
- Frank D’Souza: General Electric, Cognizant
- Bill Easter: Delta Air Lines, Concho Resources
- Fritz Henderson: Marriott International
- Leslie Ireland: Citigroup
- Tom Killalea: Capital One Financial, Akamai
- Holly Keller Koeppel: AES, British American Tobacco
- Jane Holl Lute: Union Pacific
- Mona Sutphen: Pioneer Natural Resources
- John Thompson: Norfolk Southern
- Jan Tighe: Progressive, Goldman Sachs Group
- Suzanne Vautrinot: Wells Fargo, CSX, Ecolab
- Sue Wagner: Apple, BlackRock, Swiss Re
- Al Zollar: Public Service Enterprise Group, Bank of New York Mellon, Nasdaq

ENDNOTES

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Hersh Shefrin, "The Forgotten Lesson of Huawei: Cyberattacks Will Be a Constant Threat to Manufacturing Firms," *Forbes,* December 10, 2018.

[3] Bill Phelps, Ann Cleaveland, and Steve Weber, *Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk* (Berkeley, CA, and McLean, VA: Center for Long-Term Cybersecurity and Booz Allen Hamilton, 2020), 6.

[4] Ibid.

[5] Ibid.

[6] Audit Committee Leadership Summit, *Cybersecurity Governance,* ViewPoints (Waltham, MA: Tapestry Networks, July 2019), 4.

[7] Audit Committee Leadership Summit, *Cybersecurity Governance,* PreView (Waltham, MA: Tapestry Networks, June 2019), 7.

[8] Audit Committee Leadership Summit, *Cybersecurity Governance,* ViewPoints, 4.