Cyber Risk Director Network

February 10, 2020

CRDN

VIEWPOINTS

Cybersecurity: the need for public-private collaboration

"Security beyond the boundaries—it leads me to think of traditional models of security that come from the physical world: firewalls, perimeters, zero trust, the castle with a moat. But now we have the cloud, machine learning, the internet of things … All these are blurring the lines between the physical and cyber realms." – Director

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 the ways in which cyber risk transcends traditional corporate boundaries and requires new forms of collaboration between firms, and especially between government and the private sector. Members acknowledged the challenge of managing third-party cyber risk, but the conversation continually shifted toward corporate-government interactions. 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 9). For a list of meeting participants, see Appendix 2 (page 11).

Executive Summary

The conversation focused on the necessity of public-private collaboration to combat cybercrime, the obstacles that hinder that collaboration, and the vital role of private sector leaders in strengthening collaborative action.

- **The cyber threat links political and economic security** (page 2). Nation-states increasingly recognize that economic competitiveness is a cornerstone of their

security. Offensive cyber capabilities permit state actors to work across national boundaries, exploiting other countries' assets without physical appropriation. Reliance on third parties increases vulnerabilities, but the threat can also come from within.

- **Collaboration between government and the private sector is still embryonic** (page 3). While large companies and government agencies increasingly recognize the need to share information and work jointly, issues of trust are significant, and there are legal and structural challenges to overcome. Emerging practices, such as information-sharing pilots and the issuing of temporary security clearances, have a mixed record. Nevertheless, there is consensus that collaboration is essential.
- **Private sector leaders feel the need to take initiative to improve the extent and quality of public/private collaboration** (page 7). Directors and security experts believe that the private sector should foster better collaboration, not only changing their own approaches to working with government but also by educating public sector leaders on the needs of large companies.

The Cyber threat tightly links national and economic security

King & Spalding partner Zack Harmon put it bluntly: *"The national security paradigm has shifted."* He noted that many governments are increasingly focusing on *"building market share and economic advantage in key industries."* The Chinese government, for example, is determined to enhance the competitiveness of Chinese pharmaceutical companies using all of the tools at its disposal. The objective is to replicate what makes Western companies successful, even if this involves theft or business practices that could be viewed as unethical elsewhere. To gain access to desired assets—technologies, data, and other intangibles—hostile governments may leverage investment and business arrangements, or they may opt for cyber intrusions and other forms of theft. Certain nation-states, Mr. Harmon said, are even using organized-crime networks *"to increase their bandwidth."*

Brute force is not necessary to appropriate these resources. Once hostile governments have accessed key assets, *"the things that make our companies commercially successful are gone, turned over to companies operating in another country. You're left to try to fight your way through the court system,"* Mr. Harmon said.

What is more, attacks driven by a malevolent nation can appear to come from an entity that has no visible connection to that country. *"You think you're dealing with an IT*

service provider in the Netherlands," said Mr. Harmon, *"but, two steps removed, you're really giving access to a Russian company and the Russian government. Certain nation states, unconstrained by international norms or rules of law, are using national resources and even established organized crime networks 'to increase their bandwidth.'"* A director agreed that employees can be co-opted without their realizing it, which puts the threat *"inside the building."*[1] The situation is made worse by the propensity of large firms to work with hundreds, perhaps thousands, of third parties, up and down the supply chain. The need for protection *"extends to assets within and beyond the enterprise."*

A member noted that some large companies have been complacent in dealing with economic espionage: *"They believe that if the Chinese steal their information and take it to market, they are selling to different clients than U.S. companies are. There's still some denial."* Another director pointed out that what we know as the internet was *"originally designed for well-meaning academics and social networking. We didn't really think you were going to connect your uranium enrichment facilities to it."*

All of this, said CRDN members, points to the need for collaboration between government agencies and the leaders of large companies. *"I don't know that we can get to the answers,"* said a director, *"until the private sector can collaborate with government to write up intelligence requirements. Then, someone can figure out how to share the information with the private sector."* Some directors were leery of government involvement, but most agreed that nation-state threats are difficult to counter without government support: *"Do we let the market take care of the problem?"* asked a director, who then observed, *"The market is great, except when it isn't."*

Collaboration between government and the private sector is still embryonic

Although CRDN members and experts agreed that more extensive information sharing between government and the corporate sector is critical in the fight against cybercrime, they generally felt that collaboration is still in its early stages.

Structural differences add complexity and risk

Directors and experts pointed to roles, missions, and constraints that distinguish government cybersecurity forces from those in large companies. *"National security is strategic, centralized, driven from the top. The internet is transactional, spontaneous, driven from the bottom up,"* one director said. Booz Allen Hamilton's Bill Phelps identified another difference: *"The US government is the best in the world at offensive*

cybersecurity—it can 'hack back,' which corporates cannot legally do—but there are companies around this table that are better at cyber defense." A member agreed: *"Dunkin Donuts may have more access to information threats that are relevant to other companies than the government does."*

Within government, there are differences between levels and agencies. One member commented that municipal governments—*"mayors"*—often have a better reading on threats that are genuinely new than federal agencies, simply because mayors can be closer to individual companies. Phyllis Sumner, from King & Spalding, pointed out that *"law enforcement has a different mission than regulators."* A member added, *"The culture of our security establishment is military, focused on foreign policy; law enforcement is domestic, and they have a duty to share. If a chief of police knows something and doesn't share it, they are fired. That's why we can't leave this to the national security establishment."*

Structural differences between government agencies and companies and differing or even clashing missions across government can limit the direct value of corporate-government interaction. Members repeatedly noted that the flow of information tended to be from companies to government, not the other way around. *"We did a war game at the Naval War College this summer,"* said one, *"with financial services companies. Treasury was there. We were frustrated with not getting anything back, and with not getting the help we wanted. And the fighting between the FBI [Federal Bureau of Investigation], DOD [Department of Defense], and DOJ [Department of Justice] was mind-boggling."*

But interaction and disclosure can also be risky. Directors worried that if they were to share threat information with law enforcement, it would be turned over to the company's regulators for use in civil-enforcement proceedings. Ms. Sumner emphasized the need for safe-harbor provisions: *"We need more protection,"* she said. *"Without it, there's still the issue of what's in the best interest of an organization, rather than what's in the best interest of national security. Government agencies will be reactive, not partners, and your regulators will hold you accountable."* A director expanded on Ms. Sumner's point: *"The business community has to figure it out. Companies now understand that cyber is everyone's problem, but there has to be an actual safe-harbor provision that allows people to come forward: no harm, no foul."* Another weighed in: *"You're entering into a big uncertain world, with jurisdictional uncertainty and uncertainty about individual government actors. More safe-harbor provisions: that's the crux of the problem."*

Trust remains a major barrier

> *"Unfortunately, government is still working to build a mature program. The best action we're seeing is one-on-one, where there's trust and an informal relationship." – Director*

Even if much-needed public policy changes could made, CRDN members said that corporate-government collaboration would not happen without effort. Several directors would like to see information sharing *"at machine speed"* but observed that the trust that would enable this is largely lacking. Beyond legal or regulatory risks, sharing information with government agencies could lead to disclosure of sensitive information that could be advantageous to a company's competitors. Mr. Harmon said, *"When our government has specific intel, we want it every which way. We want the government to share really specific information about what's happening in our industry, but if we're the company it's happening to, we don't want that detailed information shared with others."* Ms. Sumner warned that companies could be compelled to share information that they would not otherwise release: during litigation, she said, *"The first discovery request you're going to get is for everything you've provided to the government."*

In a few cases, corporate leaders or their advisers have created individual relationships with government agency leaders, enabling candor and sharing that might otherwise be impossible. *"Global collaboration is an important macro goal,"* noted King & Spalding's Scott Ferber, *"but there is also value on the micro level, through trusted relationships with the local FBI or Secret Service field office."* Members noted the benefits of these one-on-one interactions but felt that they didn't represent scalable or structural solutions.

Emerging practices have had a mixed impact so far

CRDN participants described approaches that they have used, seen, and recommended. Some of these have been effective, but all have encountered the problems of structural difference and trust described earlier.

- **Temporary clearances.** Because of the national-security implications of cybercrime, information about threats and incident response outcomes can quickly become classified. Some information security executives and a few board members hold security clearances, but many do not. Ms. Sumner noted that information that comes

to companies from government agencies is often not only classified but comes with nondisclosure agreements: it may be provided to select members of management but usually not to board members.

Recognizing the problems this situation creates, a few government departments have created programs that grant temporary clearances to named corporate leaders, arranging for them to be "read in" to threat information or to view data in a highly secured room. Members were generally skeptical of the value of these arrangements; *"clearance for a day is overrated,"* one said. A member described an experience as a chief information officer: *"I've been in the room with a colleague, and I got clearance. The information was vast, deep, and complex, and you couldn't take documents out of the room. Then we had to go home and personalize it, make a clear connection between what we heard, how it impacted our risk environment. When I've done this as management and then had to translate it to the board, all that's left are crumbs."*

Some directors retain high-level clearances. *"Our folks in DC will meet periodically with the FBI,"* said one. Some directors are calling for expanded clearances, but most were not optimistic either that these would be forthcoming or that they could be used effectively by board members who lacked a strong grip on agency priorities or intelligence methods. A member noted the ease of assuming that *"the harder a piece of information is to get, the more valuable it must be. That's not necessarily true."*

- **Information-sharing pilots.** In critical industries like energy, government agencies have granted limited, specific safe-harbor provisions that have allowed for high-level and extensive "machine-speed" sharing. *"There is a safe harbor,"* said a director, *"though I don't know if it's a big or a tiny little safe harbor. But this made me feel like it's a good thing."* Ms. Sumner warned, however, of the need to establish rules and parameters at the outset. *"You can't negotiate how to share information after the fact,"* she said. *"At that point, the benefit is gone."*
- **Deeper and more widely promulgated standards.** A few directors said that standards could be helpful in establishing safe communications between business and government. A former government official noted, *"Industry fought us on the NIST [National Institute of Standards and Technology] framework. Before I give safe harbor, before the conversation begins between government and industry, can you answer some basic questions? How would you demonstrate that you know what's running on your network?"*

One director agreed: *"I was a big supporter of the executive order and NIST and the work you did on it. Businesses should be willing to commit to maturity improvement. And if not, then you get what you deserve."*

Whatever attitude corporate leaders take to standards, they may be forced to adopt them. Mr. Phelps spoke of the Cybersecurity Maturity Model Certification (CMMC) Initiative, announced last summer by the US Department of Defense. Its aim, according to a DOD website, is "to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' … networks."[2] When implemented, all vendors to the DOD will require CMMC certification; any given procurement will specify the level of cyber maturity required for bidders.[3]

Mr. Phelps pointed out that changes in this enormous procurement process will go far beyond direct suppliers to the DOD. *"I think it's a back door to broader mandates,"* he said.

Throughout the conversation, directors and experts returned to the theme of basic cyber hygiene, still not at a level most in the room find acceptable. *"Companies are not engaging in cyber hygiene, yet they want safe harbors,"* said a member. Another felt that broader collaboration needed to take second priority to maturity within a company and its board: *"It's better for you to get your own act in order. There's much more you can do to improve yourself."*

A call for action

"The bad guys are cooperating with each other." – Director

Members were forthright with their concerns about working with government and sharing information with potential competitors. But many felt that difficult as collaboration may be, it is essential, given the threat posed by hostile nations in the cyber realm. Mr. Harmon agreed that cooperation between the government and the private sector is still *"in early stages and ad hoc,"* but said that Congress and agencies are getting more and more involved. *"There are key people in senior government positions,"* he noted, *"who firmly believe that our only hope of addressing the new national security challenges is to fundamentally improve the partnership between government and the private sector."* He called on corporate leaders to take initiative:

"People on the private side have to embrace the view that this critical partnership should be working better and propose to government what it should look like." A member added, *"The business community has to figure it out."*

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 Department of Justice (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] "DOD Cybersecurity Compliance," Simpatico, accessed February 3, 2020.

[3] See "CMMC FAQ's," Office of the Under Secretary of Defense for Acquisition & Sustainment: Cybersecurity Maturity Model Certification, accessed January 21, 2020.