Cyber Risk Director Network

February 10, 2020

CRDN

VIEWPOINTS

Cyber incident response: the board's essential role

"When you're in the middle of a cyber crisis, the facts never look like you thought they would. You can end up with inconsistent narratives." – 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 how companies plan for major cyber incidents and actually respond to them. In particular, they examined the role of the board and its independent directors. Professor Steve Weber of the University of California, Berkeley, joined the discussion, as did three partners at King & Spalding: Phyllis Sumner, leader of the firm's Data Privacy and Security practice; Scott Ferber, recently associate deputy attorney general at the US Department of Justice; and Zack Harmon, recently chief of staff to the director of the Federal Bureau of Investigation (FBI), Christopher Wray. From Booz Allen Hamilton, CRDN members were joined by Bill Phelps, executive vice president, and Jerry Bessette, leader of the Cyber Incident Response Program. All of these experts agreed to speak on the record. For biographies of the guests, see Appendix 1 (page 8). For a list of meeting participants, see Appendix 2 (page 10).

Executive Summary

The conversation on responding to cyber threats focused on what motivates cyberattacks, how corporations should respond, and the role of the board:

- **Mixed motivations underlie recent major attacks** (page 2). Although cyber criminals continue to steal data and deploy ransomware for financial gain, many

recent high-profile incidents have had different motivations—for example, disabling a company's operations as an act of revenge. Varying motives for attack make incident response planning complex and challenging.

- **The corporate response to an attack needs to go beyond technical or legal matters** (page 3). At some firms, the focus after a breach is on containment and satisfying legal and regulatory requirements. CRDN members discussed a customer-focused approach that may seem risky and expensive, but many companies are learning that starting with customers and their perceptions and fears can in the long run reduce legal risk, reputational harm, and total cost.
- **The board's involvement in both planning and response is critical** (page 4). The speed and ambiguity of a cyber incident and the company's response make it difficult for non-executives to engage, but members agreed that boards must actively participate, especially in assuring themselves about the company's overall incident response planning.

Mixed motivations underlie recent major attacks

> *"It's creepy—almost as if someone broke into your house, took a picture of your TV, and left."* – Director

Senior corporate leaders know that for many years, the most serious cyberattacks have come not from isolated hackers but from highly organized networks, frequently motivated by financial gain. Nation-state adversaries steal intellectual property so that their own resident companies can exploit it; bad actors plant ransomware to reap payments for decrypting their victims' data; criminal syndicates steal troves of personal and financial information, selling it on the dark web.

These attacks have typically been pursued for direct monetary gain. But recent crises reveal other motivations. In recent high-profile cases, cyberattacks were designed to disable corporate operations or embarrass the victim company. This is not to say that victims of this style of attack don't suffer economically, but the perpetrators' motives are less clear these days, and this makes response planning more difficult. *"Don't think about a cyber event just as data theft,"* advised Phyllis Sumner. *"It's about the many different ways your business could be compromised by an intrusion into your system."*

Bill Phelps observed, *"It's not always obvious that there's been a cyberattack."* In some cases, criminals plant software that remains dormant for long periods, or malign actors can use their software foothold in company networks to collect invaluable information about the company's operations and practices. They are increasingly sophisticated and skilled at covering their tracks.

Jerry Bessette managed the 2014 Sony case for the FBI. He described a process that unfolded over a year: the attackers *"took malware used in Seoul in 2013, tweaked it, and it slipped through. Sony knew they were a target; they spent a lot on cybersecurity."* Nonetheless, the criminals were able to extract large amounts of data from Sony's network over several months without being detected.

Some members insisted that the attack was preventable. *"Unpatched vulnerabilities are the single most important source of attack,"* said a director.[1] But Mr. Bessette pointed out that Sony had invested heavily in *"people, processes, and technology for cybersecurity. It only takes one of your employees to click on something."* He noted the difficulty of monitoring an ambiguously motivated attack, one driven less by money than by revenge, in this case for Sony's release of a film mocking North Korea. *"Something that is unusual [isn't necessarily] bad. A 2-gigabyte upload in Singapore might not be a problem, but you still need to monitor it."*

Corporate response: beyond technology and legal issues

Members discussed the tension between on the one hand conducting a full forensic investigation, remediating breached security systems, sorting out legal and regulatory liabilities and on the other hand, delivering a quick and satisfying response to customers. Consumers and regulators expect speed, transparency, and accountability. *"Amazon sends you stuff immediately,"* said a member. *"This is coming into our expectations, even of government."* Another member warned of the downside of prioritizing speed and transparency: *"It becomes a problem that you know so little in the beginning. As you hunt to try to figure out how they got in, are they still there, what did they take—can you do that without them knowing you're aware? Once they know you know, they're good at backing everything out."* In some cases, directors noted, law enforcement officials ask companies not to make a breach public.

Nonetheless, Ms. Sumner advised companies, *"Think in advance about your public response, not just what you're legally required to do. You may have more risk if you do only what's legally required, rather than using your brand and culture as a guide to action."* She gave the example of an airline that *"went out with great speed and made public representations to their customers. That entailed some risk, but it was important*

to their brand and culture to manage it that way. They got great positive public feedback and weren't blistered by the press."

In large companies, the existence of multiple specialist teams can slow down customer response. A director described a response: *"With the involvement of the CEO, the CIO [chief information officer], the CISO [chief information security officer], their teams, and legal and consumer-facing teams, it took a lot more time to communicate. There were several board phone calls each week in this period. [The audit committee wanted] to go through complete forensics, which we did in detail; we summarized and reviewed it with the board. It went from September to January, a tremendous amount of time."* A member warned, *"I'm surprised at boards' consistent sense that they can keep the public out. It's not possible."* Ms. Sumner agreed: *"There's no doubt that the public, the Hill, regulators, [and] customers all want speed and transparency."*

Professor Steve Weber asked, *"How do you think about incidents that might not require telling the SEC, but can still be significant to consumers?"* Ms. Sumner replied that companies need to determine thresholds for informing the public, triggering a legally protected investigation, and informing the board. *"It may depend on the type of information, the number of consumers involved, or certain customers that have been affected. Each organization faces different risks,"* she said. *"If the incident involves a blogger who's going to say something, for instance, you'd want to inform the board, and you may want to go public first."* The company should decide its threshold for informing the board about a breach at the same time that it decides when it will inform consumers of an incident.

Ms. Sumner warned that attorney-client privilege is not retroactive: unless internal or external counsel are involved early, legal privilege may not hold.

The board plays a critical role

Members engaged in a lively discussion about when and how a board should be notified of an incident. In general, directors preferred to have the board be informed, even if the information is incomplete. *"If you have to notify your regulator,"* one said, *"then you have to notify the board."* Another added, *"I would expect an ongoing conversation about our threat level, our risk profile, a dashboard that says whether all patches were applied within 72 hours, the number of attacks we fended off. I don't want to distract management from handling the immediate impact, but I don't want to be surprised either. Once it goes public, or if it has financial impact, I expect at least a call that says, 'I don't have a lot to tell you yet, but here's what I know.'"*

But expert guests challenged this. *"Organizations notify attorneys general all the time about one-off security incidents. You don't necessarily send those to the board,"* said Ms. Sumner. Zack Harmon described a situation in which *"there's a penetration, and they have accessed something critical and sensitive, but only your CISO knows about it"* because no data has been stolen and no operations disabled. *"It could be an existential event, and you may not know about it for six months."*

A director offered further nuance. *"There's a cascade with the board. First reach out might be to committee chairs. Let's make sure people know what is going on, to the best of our ability You don't want to be in the way of the executive team, but someone is going to ask you, 'What did you know, and when did you know it?'"*

Most companies have formal Incident Response Plans (IRPs), but many of these are technically oriented and don't reach top management, let alone the board. Ms. Sumner insisted that *"every organization should have an enterprise-wide IRP"* and described characteristics of such a plan:

- **It should cover the business as a whole.** It should not be focused solely on technical or even legal security, but should take a holistic perspective.
- **It should be streamlined and accessible.** *"If you bring in a 100-page IRP during a crisis,"* said Ms. Sumner, *"no one will look at it."* The enterprise-wide IRP needs to be short and practical.
- **It should identify a high-level incident response team,** which should include board members. *"Are you comfortable with that team?"* she asked. *"Do you know who's in charge?"*
- **It should have clear escalation policies** (from the CISO through the legal and executive team and eventually to the board). *"You need a policy or a form of understanding. If it isn't written down or discussed, expectations may not be aligned."*
- **It should have crisis communication methods.** Corporate resources like email and internet phones are likely to fail, as they did in the 2017 attack on international shipping firm Maersk. Ms. Sumner warned, *"Personal devices shouldn't be used unless strictly necessary. If personal devices are used, we have to image and confiscate them because they are communicating about the breach."*

- **It should identify expert counsel:** legal, technical, forensic, logistics, public relations, etc. Directors and experts noted that it's important to ensure that external resources have been identified, commercial terms settled, and services retained well before an incident. *"You want to have an organized group coming in that you're not meeting for the first time. [They should] take charge and immediately get on top of the work,"* said Ms. Sumner. A member noted that there may be competition for the services of top advisers and that more than one company is often affected by a cyberattack. *"Have the firms on retainer, so you can deploy them."*

A director added, *"In an incident response plan, board members should look at when different executives are notified. It's good to scrutinize at what point the CEO gets engaged. You can be surprised at how soon or not the different escalation points trigger."*

Following this last point, members discussed the merits of boards participating in "tabletop" exercises to test their IRPs. Most agreed that boards need to be involved. *"If the board has never rehearsed with management, there's no excuse today,"* warned a director. Others described observing a tabletop exercise rather than participating in it: *"It was helpful to see where lessons were being learned. One takeaway for me was the sensitivity of communications: something you say in email could invalidate your cyber insurance policy. I also learned that the cure can be worse than the disease. Shutting down our network would have shut down the local stock exchange. I'm observing the exercise to learn, not to write a report card."*

The general view of the group was that most boards could engage more deeply with IRPs. First, boards could be involved in the preliminary work to get the plan at a suitably high level and in thinking *"holistically about who is affected by our business."* Second, they could be involved in establishing a communication and management-to-board escalation policy that would state clearly that *"we have to report the following things, and the risks associated with them … [without having to] wait until we have a financial materiality issue."* And finally, the board could get involved in simulations or tabletop exercises: *"There has to be a global exercise,"* said a director, *"and at some point, you've got to get the board involved in all of it."*

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.

This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated network names and logos are trademarks of Tapestry Networks, Inc.

Appendix 1: Guest biographies

Jerry Bessette leads Booz Allen Hamilton's Cyber Incident Response program, which addresses the full incident lifecycle, including preincident preparation, incident response, and postincident remediation.

Prior to joining Booz Allen, Mr. Bessette was a managing director with Ankura Consulting, where he managed incident response investigations and proactive services for clients ranging in size from Fortune 150 corporations to small, privately held companies across business areas. Engagements included information security assessments, risk assessments, incident response, and technical services such as penetration testing, vulnerability scans, and tabletop exercises.

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

[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.