Cyber Risk
Director Network
August 2020

CRDN
VIEWPOINTS

Cyber risk and the corporate response to COVID-19

As companies rapidly implemented remote work in response to the COVID-19 pandemic, they faced new security risks. Many will encounter additional threats as they reopen or move to hybrid environments. CRDN members met on July 2, 2020, to discuss how remote work has changed cyber risk and to consider how companies can mitigate those risks. They were joined by Phyllis Sumner, Partner and Chief Privacy Officer, King & Spalding, Kevin Richards, Executive Vice President, Booz Allen Hamilton, and Steven Weber, Professor, University of California at Berkeley. *For a list of meeting participants, see Appendix 1 (page 8). For a list of guests, see Appendix 2 (page 9).*

Discussion centered on three main topics:

- **Noting successes and difficulties in the transition to remote work**
- **Reviewing risks that surfaced in the crisis**
- **Envisioning a post-pandemic future**

Noting successes and difficulties in the transition to remote work

Most CRDN directors felt that the transition to remote work, though carried out rapidly and under intense pressure, had been broadly successful. Leaders and staff showed great resilience; many companies continued or accelerated digital transformation journeys they had launched earlier. Contrary to earlier expectations, productivity did not generally decline, and by some estimates it actually increased. But many security challenges persisted, and the move to distributed work introduced new risks.

Investments in technology infrastructure and people paid off

A director reflected on the investments that contributed to the success of the transition to remote work and which have *"paid huge dividends"* in recent months: *"The companies that did well in this transition made investments ahead of time, not for reasons of the pandemic but for reasons of agility and the global scope of their businesses operations. They invested in cloud services, in bandwidth—not knowing what they'd need or when—so they had some excess capacity there. They invested in their employees, so employees understood their roles not just* *in the conduct of business but in cyber operations. And they had installed controls in systems in an increasingly dangerous cyber environment.'"*[1]

Another director agreed that *"all the investments we had made in our business continuity efforts and processes really paid off during the pandemic. You could see the return on investment from our tech capabilities, our distributed capabilities, and our IT support infrastructure to ensure that people we needed to be working remotely could actually do it and do it well. We felt good about our business continuity plans."*

A third director was *"heartened ... I was prepared to see all those perfect plans of where we were headed in cyber security fall off—you know, 'Oops, we have an economic crisis, we have a cashflow problem,' etc. That's not what I saw. Maybe it's a recognition of the situation we're in, but these companies have maintained their commitment to upping their cyber game."*

Persistent challenges remain, and new risks have appeared

Despite these achievements, the complexity of enabling distributed work on such a large scale in short order meant that companies faced a variety of challenges. Foremost among these was ensuring data security as employees shifted to home networks, often using private equipment. IT teams reported that securing multiple devices over which they had limited control proved difficult and remains a challenge today.

- **Intensified cyberattacks.** Malicious actors—including company insiders, adversary nations, and transnational criminal groups—exploited the disruptions and stresses of the transition to remote work. Ms. Sumner reported that the move to distributed work caused *"seismic shifts in the network architecture of organizations,"* and *"the number of endpoints went up exponentially."* Companies became more vulnerable to attackers as they rushed to increase cloud computing capacity and added devices to company networks without adequate endpoint protection, changing and expanding the attack surface. Tech teams were stretched to monitor suspicious activity across a larger number of endpoints whose visibility was limited. A director observed that although the nature of the cyber threat may not have changed fundamentally, the number of attacks *"over the last 90 days has been up three, four, fivefold."*
- **Insufficient controls around the digital infrastructure.** Employees' home networks were understandably less secure than their company networks. A director pointed out the importance of a dynamic approach in defending critical information from attack. Key data resides in digital infrastructure—corporate servers, for example—and is managed by humans who hold access privileges. But in the crisis, the director said, the humans moved, often from corporate offices to home networks, and in many cases the data also moved, sometimes into less secure areas of the digital infrastructure. *"Companies that tried to set up a sensor network around some of the digital infrastructure, using trip wires or analytics,*

found that they were protecting the wrong spaces. And the threats were more agile; they moved much more quickly into the new, less secure spaces."

- **Relaxation of certain operational controls.** The practical realities of remote work required the relaxation of some protocols – for example, allowing printing at home or tolerating employees' workarounds. Companies struggled to find the right balance between flexibility and control. Directors raised a variety of related concerns as well. One asked, for instance, *"What's ok in terms of IP to share? The operations center, your crown jewels—who gets to say what can be thrown up on a screen? Whereas before, you're on the executive floor, and you need a passcode to get on there, and any piece of paper floating around is in an open but secure area."*

- **Weakened social cohesion and potential increased insider risk.** Some directors expressed concern that a weakening of firms' social fabric could lead to insider security breaches, whether inadvertent or intentional. One said, *"What we haven't yet figured out is how to sustain the social connection—the social fabric—in this new world, because most companies are not going back to where they were. So how do you enculturate people in a workplace and an environment where they never physically meet? How do you prevent physical distancing from becoming social distancing?"*

Reviewing risks that surfaced in the crisis

With a majority of employees working from home, many companies have gone from what Ms. Sumner called the *"reactive"* to the *"stabilization"* phase of the crisis. Management and boards are now stepping back to review risks that they may not have been able to address during the initial upheaval, and to consider those that could arise in the shift back to on-site work.

- **Control of physical and digital assets.** Ms. Sumner suggested that organizations should now pause and take stock of both physical and digital assets. As an example, her own firm, *"handed out laptops to users who never had them before because they worked in the office. Control of such assets is critical, and organizations may need to revise policies and procedures given the changes in operations."*

- **Visibility across endpoints.** Ms. Sumner said that unfortunately *"organizations don't immediately have the tools and capability to achieve visibility across all the new endpoints in a way that allows them to monitor and detect malicious activity."* She is concerned that companies may struggle to assess and respond appropriately to threats in this environment and that malicious activity may go undetected. *"The other part of visibility that I worry about is when an organization is in incident response mode. If they don't have it set up in a way where they can easily deploy agents, or already have agents deployed across the environment, then it's hard to do the forensics quickly and to respond appropriately to an incident … If you can't see, you don't know whether you've contained the incident or it's still spreading."*

- **Insufficient segmentation.** A director expressed concern about the lack of segmentation of networks—a *"preexisting condition"* that has not been remediated. *"Networks are way too flat, not only for global organizations but for almost every organization. It's low-hanging fruit that's not being taken advantage of. Ask yourself the question, 'against what standard will we as a company be judged with respect to our posture? Are we doing everything we reasonably can?' I frankly think that's a failing grade."*

- **Monitoring data flows**. Establishing a reliable baseline against which to measure anomalies has always been challenging in dynamic digital environments. Since COVID-19 invalidated much of what had been accepted as normal, re-establishing baselines will take time. Mr. Richards reported conversations with clients about *"monitoring data movement and building elements into the infrastructure so we can see that someone just copied something from their trusted work laptop to network-based storage or a USB drive, for example."*

  A director identified *"three pillars"* of an agile, dynamic approach to critical information asset protection:

  1. The consistent application of "least privilege," whereby access is allocated to distinct, assigned roles, rather than to broad groups of users: *"They manage that as if it's a commodity of some value, because it is."*
  2. A data architecture that identifies what information is important and prioritizes its protection, *"because you can't defend all things against all perils."*
  3. The use of behavior analytics to detect deviations from normal data usage, because *"the thing you're looking for probably has never happened before; it's an unexpected anomaly from the baseline, as opposed to some prescribed event."*

- **Insider threats.** Ms. Sumner agreed with directors who feared the potential for increased insider threats: *"We're seeing things like corporate information moving to personal emails. And that immediately raises red flags about whether someone did that intentionally to grab data or because it was more convenient and easier to access. So, the insider threat programs have to raise their game just as monitoring and detection of outside threats also have to go up."*

- **Envisioning a post-pandemic future**. While firms providing essential services—grocery retailers, for example—never closed, others that did are now facing decisions regarding how to reopen. Many companies are likely to adopt hybrid work models in which some employees continue to work remotely.

  Directors reported that they seek to adapt the lessons learned so far during the crisis to the new tactical challenges raised by the return to work. One reflected that just as the pandemic had *"pulled the future forward"* by forcing *"further digital transformation efforts and investments in how we communicate with customers,"* the postcrisis phase will force companies to develop new responses. *"We have to think carefully about what in our reentry will be key risk indicators. Will they be the same in the post-pandemic environment? The pandemic has caused all of these questions to come into focus with a new urgency."* Ultimately, directors hope to leverage insights from the crisis to formulate longer-term strategies for ensuring business continuity, promoting growth, and preparing for new crises.

Third-party risks

Third-party cybersecurity has been a long-standing challenge for IT teams as well as for board oversight. With the pandemic, many well-established supply relationships have been disrupted, and companies have taken on new, untested partners, forcing their teams to consider the level of third-party risk they are willing to accept. A director remarked, *"Many companies are now accelerating how we view our highest-risk suppliers, monitoring what they're doing, how they're changing things. It's critically important to understand where we already had risk, what suppliers were we depending on where we had concerns, and how we can minimize their impact on our business versus finding different suppliers that we're more confident in."*

A director pointed to a special category of risk that merits attention: *"We are concerned about third parties we use around our IT systems, not just suppliers. We spend a lot of time perfecting contracts, obligating them to adhere to certain standards, and holding themselves open for audit. But the question is, how do you ensure that? Because you can't constantly go around to a lot of these operations."*

In addition, Ms. Sumner noted, *"often these diligence practices and audit rights are built into third party contracts, but the reality is that most organizations don't have the resources to do it. So regulators look to the organization and say, 'Well, you've got this right to audit; why weren't you in there diligencing that third party?' It's a balance of: if you're going to put a process in place, you must ensure that you have some mechanisms to follow through."*

Increased adoption of cloud services

The sudden imperative to support large, remote workforces has further reinforced companies' interest in cloud computing. *"There has been a huge acceleration of cloud adoption in the last three months,"* a director said. *"One contributor was that in the early parts of this pandemic, the supply chain for data center equipment was meaningfully constrained."*

Cloud services can be a key enabler as companies move beyond the limits of legacy systems, but the security challenges are significant, and many management teams must update their skills. *"There's a lot to learn,"* the director said. Cloud systems need different monitoring points and methods, as well as different ways to aggregate signals into dashboard indicators. The director explained, *"The set of cloud services that companies are adopting is complex, and the degree of training among workforces is not where it needs to be. It's easy to get these services up and running, more challenging to get them running in a coherent and well-*

integrated way." Despite this, the director argued, the security improvements that can be realized *"because of automation and a coherence across a footprint"* are significant. For example, many cloud platforms allow IT teams to deploy machine-learning capabilities for user behavior analytics. The need and opportunity, the director said, is *"to build up a new baseline of what normal looks like in a world where almost all of your applications are running on cloud. The tooling and the richness of monitoring data and capabilities are stronger there than they might have been in your legacy data center."*

The director added, *"This pandemic changes things forever. Advantages accrue to companies that are able to experiment, to course correct, to double down on what's working, and to achieve greater organizational agility. The cloud is certainly enabling that, and it's a challenge for CISOs [chief information security officers] and directors who take an interest in the security dimension."*

Balancing tighter security against collaboration and innovation

Directors discussed some of the ways in which cybersecurity models may need to change in the wake of the pandemic.

- **Is the castle-and-moat model becoming obsolete?** A member reflected that *"companies have been comfortable with a wall that guarded the campus of the office, but once inside you have a lot of latitude to move around. But now, the boundary has expanded substantially, and a lot of third parties are exchanging information as well. So we have to reflect on how we want to segregate our environment. At the same time, because of the remote working environment, there's a sense that we need to make collaboration easier versus putting additional locks and walls around it. We know a change has to happen, but if we get too far into control, we could lose some opportunity for the collaboration and innovation that's required as we go forward."*

- **Should zero trust be the goal in a post-pandemic future?** Another director referred to the three key phases of a crisis—respond, recover, and thrive—and noted, *"We're still in the 'respond' phase, and a lot of enterprises are dealing with the boundaries of their enterprises having blurred since March. Envisioning a postcrisis future, some companies are saying it's time to call time on the traditional military-style perimeter security posture with firewalls, demilitarized zones, proxies, and so on. Many are moving to the zero-trust approach where, for each data access request, you strongly authenticate the person, the device, the current state of the device and its malware protection, and the relationship each person has to your enterprise applications."*

  The director continued, *"Companies are moving to that model rather than coming into the office through VPN [virtual private network] concentrators—which are now under massive attack because those are the nexus of a lot of control if you can get access to one. Rather than depending on that to give you an all-or-nothing view of the enterprise, be much more*

> *explicit and start from a zero-trust place, then work your way up to what you want to allow access to. That's a bit of a journey, and it opens up a digital divide since it's harder for legacy applications and systems to move to that model. But there's a big move toward capabilities of this kind in the early part of the 'respond' phase of the crisis."*

Ms. Sumner addressed member concerns about heightened risks as well as aspirations for enhanced postcrisis cybersecurity: *"Because of all of the risks that have increased and the opportunities for threat actors to take advantage of our employees, as well as the insider threats, employee training and system monitoring and detection are critical to cybersecurity programs."* A director agreed, noting that risk management is *"as much about employee behavior and expectation setting as about controls."* Taking a broad perspective on third-party risk, Mr. Richards noted, *"We are third parties to others and impart risk to them. We need a 360-degree view of organizational risk."*

Ms. Sumner concluded: *"I think we're heading into a scenario where the pandemic has made it more important to do all these things because the risks have gone up. From a corporate perspective, asset inventories, data mapping, access controls – already crucially important before the crisis and always difficult to get an organization's arms around – have become even more important today."*

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 is sponsored by King & Spalding, an international law firm with a substantial data privacy and security practice, and by Booz Allen Hamilton, a management and information technology consulting firm with deep cyber and industry expertise. 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

- **Steven Weber** is Professor, School of Information, University of California, Berkeley; Senior Policy Advisor, Glover Park Group, Washington DC, and adviser to government agencies, multinational firms, and international non-governmental organizations on issues of foreign policy, risk analysis, strategy, and forecasting.

Appendix 2: Meeting participants

- **Joan Amble**: Zurich Insurance Group, Booz Allen Hamilton, Sirius XM
- **David Ching**: TJX
- **Bill Easter**: Concho Resources, Delta Air Lines, Grupo Aeroméxico
- **Pat Gross**: Liquidity Services, Perdoceo Education, and Rosetta Stone
- **Chris Inglis**: FedEx, Huntington Bancshares
- **Tom Killalea**: Akamai, Capital One Financial
- **Jane Holl Lute**: Union Pacific, Marsh & McLennan
- **Kevin Richards**: Executive Vice President, Booz Allen Hamilton
- **Stuart Russell**: Intact Financial
- **Phyllis Sumner**: Partner and Chief Privacy Officer, King and Spalding
- **Mona Sutphen**: Pioneer Natural Resources
- **John Thompson**: Norfolk Southern
- **Jan Tighe**: Goldman Sachs Group, Huntsman, Progressive
- **Lynn Vojvodich**: Booking Holdings, Dell, Ford
- **Sue Wagner**: Apple, BlackRock, Swiss Re

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.