Cyber Risk Director Network

August 2020

CRDN

VIEWPOINTS

Oversight of privacy compliance and reputational risk

In the first of three sessions, members of the Cyber Risk Director Network met virtually on June 30, 2020, to explore the board's oversight of data privacy, focusing particularly on strategy and reputational risk. They were joined by King & Spalding Partners Phyllis Sumner and Rob Dedman, Booz Allen Hamilton Executive Vice Presidents Bill Phelps and Kevin Richards, and Professor Steven Weber, University of California, Berkeley. *For biographies of the guests and a list of meeting participants see Appendices 1 and 2 (page 14).*

The discussion centered on four main topics:

- **Companies in all sectors must manage privacy**
- **Privacy is a board-level issue**
- **Privacy and cybersecurity must be managed together**
- **Managing privacy through new operational and organizational approaches**

Companies in all sectors must manage privacy

Leaders of consumer-facing companies have long been mindful of the need to protect the privacy of customers, employees, and other stakeholders. They constantly balance opportunities to capitalize on vast quantities of data against the legal and reputational consequences of misusing that data. But business-to-business (B2B) companies also face both legal and reputational risks and have grown increasingly alert to new and emerging obligations. And now, the novel coronavirus has presented all companies with new considerations about handling sensitive health and other personal data they collect from employees and third parties.

Privacy is a pressing concern for consumer-facing companies

In an era when companies collect more data than ever, customers, employees, and other stakeholders are voicing concerns about how their data is used. This has led to regulatory initiatives that impose significant limitations on how companies store, use, and share certain types of data. It has also raised public awareness about privacy, making privacy management an ever more important part of reputation management.

The challenges may be particularly acute for companies that make innovative use of data. A member noted that the line between *"intrusion"* and *"convenience"* has become increasingly

tricky to determine. In the auto industry, for example, cars now come with built-in services that record people's driving habits and the places they go. *"How do you protect all this data?"* a participant asked. Another noted that one automobile company *"goes to great lengths to lay out all the possible uses of the data, which is a legal protection, but most people just opt in,"* because of the convenience of the in-car devices that use such services. The participant continued, *"It's up to us to anonymize and protect their information."* A director from a consumer-facing company that had a cyber incident some years ago noted that lawsuits came immediately: *"People give you the information willingly, but they have an expectation of privacy. As we try to offer greater convenience to the customer, we're also putting more of a burden on the organization to capture information in a way that can't be shared, and to protect it."*

Privacy is increasingly important for B2B companies

Consumer companies are not the only ones that worry about data privacy. Business-facing firms must protect the data of employees, business partners and enterprise customers. A director remarked, *"Every company has data privacy as a concern, especially the PII [personally identifiable information] of employees, staff and near-term people in your network. But if you don't have a consumer-facing business, your principal vector of risk is your supply chain. With a lot of contractors, where does the line end? When do you stop worrying about privacy for your near and abroad partners? It doesn't trickle down to the same extent to every single thing a company does as in a consumer-facing company."* Another member noted that, although privacy may not occupy the board of a business-to-business (B2B) company *"to the same extent as for a consumer-facing business,"* it is nevertheless *"important to think about as part of hardening cyber risk"* and safeguarding confidential information such as *"product programs for customers and sensitive information like production schedules and engineering drawings."* A director noted that *"sensitive data resides throughout the organization at functional, departmental levels"* as well as in the supply chain. The director added that companies are increasingly using AI and algorithms to *"be more predictive"* throughout the organization, which means *"we must be vigilant about creating a culture of attention to data privacy in all companies, including industrials."*

Mr. Phelps commented that more B2B companies now have *"an extraordinary trove of information about locations, patterns of life, and the like. Most of them are tracking how individuals are using their products and they have a lot of PII—more than they might initially think."* Ms. Sumner added that as the definition of personal information has broadened, *"even in B2B organizations, if there's a security incident, information collected on business partners—contact information, emails—now may be considered personal information. Under GDPR [the European Union's General Data Protection Regulation], such business card type information may trigger some notification obligations. The line is blurring as the laws are expanding and it's increasing our obligations around protecting data."* Ms. Sumner added that *"there's so much overlap now in terms of personal information and business information that I*

often see B2B companies surprised that they have notification obligations, since they're not directly dealing with consumers. But almost all organizations collect personal information about employees and at least some business partners so those notification obligations may be triggered when there's a security incident."

Regulatory uncertainty intensifies risk for all companies

New laws and regulations are in force or in process in several jurisdictions, with others likely to follow. Implementing GDPR however, is not a perfect solution for US companies, as it is not fully commensurate with the California Consumer Privacy Act (CCPA). The combination of the GDPR, the CCPA, and potential additional state and federal privacy laws creates considerable uncertainty. International companies face further complexity from the multitude of privacy laws developing in jurisdictions around the globe.

Within the European Union, the GDPR requires member states to set policies in accordance with the EU-wide regulation, and country-level information regulators have levied substantial fines for violating their policies. Some of these have already survived legal challenges, as in the recent case of the $57 million GDPR fine France imposed on Google. In that case, France's data watchdog, the Commission Nationale de l'Informatique et des Libertés (CNIL), said that Google made it too hard for users to find key information about the types of personal data it was collecting, for what purposes, how it was stored, and for how long it would keep the data. France's highest administrative court, the Council of State (Conseil d'État), upheld CNIL's right to penalize Google even though it is headquartered in Ireland.[1] While this was the first such fine under the GDPR, and the largest to be finalized so far, larger fines are pending against British Airways ($230 million) and Marriott ($124 million) in the United Kingdom.

As directors of global companies operating in the United States, the EU, China, and many other countries, CRDN directors encounter starkly differing social and political views on privacy. Mr. Dedman noted that *"all nation states start from a policy position inherent in the values held by that society. The EU always valued the privacy rights of citizens, so you see GDPR enacting very strict privacy obligations. China is at the other end of the spectrum: the system prioritizes national security (which could include the prosperity of government-owned companies) over the rights of consumers. Depending on which state you find yourself in, the US is somewhere in the middle."* Members felt, however, that despite enduring differences, the US sensibility *"has migrated over the last 8 to 10 years toward the European view on who owns the data and who's calling the shots regarding its control."*

Privacy is a board-level issue

Directors have become increasingly attuned to the complexity of the privacy and security environments in which their companies operate, including consumers' growing control over the disposition of their data and the challenges of meeting a variety of data privacy regulations in force in the EU, the United States, Brazil, India, and elsewhere. One director noted that

simple privacy compliance may not be sufficient to protect reputations, but is necessary nonetheless, adding that privacy is *"susceptible to a rules-based approach. You can identify the '20 elements' of personally identifiable information and answer the question: Is the company doing everything we reasonably can to protect people's data?"* Others agreed that a rules-based approach alone cannot always ensure data privacy, nor does it necessarily protect companies from the reputational fallout of perceived mishandling of data. In the event of a breach—real or apparent—boards must help their companies manage the unpredictable ways that privacy violations can play out in the court of public opinion.

Beyond compliance and incident response, board oversight of strategy is required to achieve a workable balance among competing imperatives to use data creatively—for example, applying data analytics or AI to create and capture value—while managing privacy risk.

Companies' obligations as data keepers expand in the age of COVID

In addition to the already-pressing data privacy challenges facing management and boards, the coronavirus pandemic has introduced new concerns about how companies collect, use, and store the sensitive health and personal data of employees and third parties, such as vendor employees.

Ms. Sumner said, "*We're seeing the collection of health and other information that companies have previously not gathered."* A director's recent experience illustrates this clearly: *"We had an incident as we were preparing to send employees to work from home. There was an IT vendor who unwittingly sent someone to their office who had a raging case of COVID-19 and exposed more than 100 of our employees. This led to discussion about what we will ask of vendors. We already ask for certifications of cyber hygiene; will we also be asking for certification of health status?"* Mr. Dedman explained that "*now every organization has to ask, 'How effective are the processes of our vendors and suppliers, and how much risk are we exposed to?' It is natural in this environment to inquire how well those organizations deal with infectious disease. But that becomes a real minefield, because you might, in some situations, have information about those vendors' employees as well, without those employees necessarily even knowing you have it."*

Companies are collecting health data without time to consider privacy issues

Ms. Sumner commented that organizations have moved very quickly into collecting health data for safety reasons, *"but they have not had time to assess the associated risks."* Now, companies are asking whether they should really be collecting this data and what they should be doing with it. One participant shared some of the questions companies are asking about the health data they suddenly find themselves with: *"Should we be sharing this data? What kind of consent should we be receiving from individuals? Should we be requiring them to give us this information? We're not the government after all … and there are enormous privacy issues surrounding this."* Ms. Sumner is concerned that *"we will see legal issues arising out of*

this for a long time to come, especially as we move out of reactive emergency mode and organizations are faced with security issues around some of this data and the fact that they haven't had time to do risk assessments before launching into these collection processes … I fear we will begin to see some significant repercussions."

Noting that the COVID-19 pandemic *"short-circuited the debate you might normally have on the use of health information by employers,"* Mr. Dedman advised companies planning to reopen to take time to consider how to balance *"employees' rights to privacy about their health against the wider safety issues in returning to the office."* He remarked that contact tracing might soon be part of this calculus. In the UK, for instance, *"we're now looking down the barrel of a track-and-trace system where the government tells friends on your behalf that you've been infected, so they can self-isolate … There is no doubt that the way personally identifiable information (PII) is handled in the pandemic will change how people view their privacy rights in the future."*

Data hygiene and rigor are essential …

Companies have an obligation to protect a wide variety of information, including proprietary business intelligence and PII of employees, customers, and suppliers. In addition, as a director pointed out, with *"data aggregators, and because of social media, there are a lot of third-party sources of companies' data,"* and companies' obligations related to such *"third-party repositories"* is still unclear. This data, the director continued, *"can include everything from religious orientation, behavior, patterns of life, political opinions, health, union membership, race, and gender … even when you don't mean to collect these things or collect them intentionally. So it is important for management and boards to agree upon and articulate a rule-based approach and to explain how the company will prevent accidental, unauthorized acquisition, loss, disclosure, or alteration of data."* Such an approach would include enacting explicit *"policies in writing prohibiting the use of sensitive data except under rules."* It would also include reasonable measures *"to notify, to mitigate risk of disclosure, to institute remediation, and to filter out sensitive data."*

… but simple compliance doesn't always protect companies from legal or reputational repercussions

Perceived privacy violations can play out in unpredictable ways and cannot be managed simply by applying rules. As with other aspects of corporate conduct, outcomes may be rapid and unexpected, and the court of public opinion can be harsh.

A director shared a recent experience that illustrates how following the rules can be insufficient, noting that companies can *"do what's right and required, but it doesn't mean you'll end up in a positive place on Main Street."* In making decisions about approving Paycheck Protection Program loan applications, the director's organization adhered to specific parameters for the loans and applicable regulatory requirements—including to "know your

customer." But the result was *"negative articles, blogs, phone calls from legislators to the chief risk officer, and accusations that we gave preferential treatment to wealthier clients. This all happened very fast; we did not step back and ask: What will happen to our reputation if we lend to the wrong company?"*

Privacy and cybersecurity must be managed together

Although some companies still place much more emphasis on cybersecurity than on privacy, members and experts agreed that cybersecurity and privacy risks should be considered together at the board, as splitting them up can lead to operational problems and potential liability for both executives and boards.

The events precipitating privacy breaches and cybersecurity incidents often differ. Cybersecurity incidents *"almost inevitably imply an adversary or some third party seeking to gain illicit access to data,"* said Mr. Phelps. Proper information security requires cybersecurity, but even the best cyber defenses don't guarantee immunity from privacy problems, as these are often the result of bad design or even a customer inadvertently disclosing information.

Companies must educate employees, customers, and suppliers

Strong privacy may also involve educating employees, suppliers, and even customers. Mr. Phelps shared the example of an incident that had *"almost become crisis level"* at a financial services institution. It *"stemmed from a case of accidentally sending one customer's data to another, because customers were asking for information related to their account or their business and someone entered an email address that was auto-filling and it went to the wrong place."* In this case, the organization's chief information security officer was called in and said, "It's not a cyber incident, it's not significant, nobody is stealing your data." But because this happened at a financial services institution, the company felt it was a significant regulatory issue, and that each of those privacy violations was a disclosable event.

A director described another case: *"Some of our customers were putting incredibly confidential data in freeform areas. It comes back to this rules-based vs. principles-based approach to privacy. We were following the rules, but we could see this data and took an active role to partner with customers to get it out of there. So we worked hard to be diligent on all the attributes of privacy, questioning, what's in there, why is it in there? Even though our contracts were specific that customers should not provide any data that we had not requested, it was a convenience point for customers. We had to make sure we didn't have unidentified process risk; we had to hold ourselves accountable to the principles as well, and we took an active role to get the information out of there. We had to engage customers directly on this."*

Inadvertent disclosures can lead to exploding risk

Ms. Sumner gave an example of how an internal error can lead to external pressure: *"We are seeing how inadvertent access to personal information can damage an organization's brand and create risk for the organization. Individuals do not hesitate to express outrage via social*

media, which can get the attention of the media, plaintiffs' counsel, and regulators. We're currently defending an organization in multiple class actions relating not to criminal actors accessing the data, but to limited inadvertent access, which would not have generated class actions several years ago."

Ms. Sumner remarked that *"Whenever you're dealing with cybersecurity incidents, you're inevitably dealing with privacy issues. Organizations faced with answering regulatory inquiries will get the full gamut of questions, and the lawsuits start being filed immediately after a press release or a blogger starts reporting on an incident. The litigation focuses not just on cybersecurity issues but on privacy of individuals and the potential impact on those individuals. And then the focus comes back to the leadership, the culture of the organization and sometimes the directors."*

Managing privacy through new operational and organizational approaches

Boards are finding ways to bring cybersecurity and privacy together in support of both compliance and business goals by helping management achieve internal coordination among executives and business leaders responsible for privacy and cybersecurity policies and procedures. Management, for its part, said Ms. Sumner, should supply boards with privacy risk assessments as well as cybersecurity risk assessments, so that the board can understand the global privacy strategy and how the *"different jurisdictional approaches are coming together."*

Boards should resist artificial separation of cybersecurity and privacy

"More and more boards are very focused on cybersecurity and reviewing third-party assessments." Ms. Sumner remarked, *"Boards are not as frequently focused on reviewing global privacy impact assessments or on privacy-by-design that should occur early."* One factor that contributes to the separation of cybersecurity and privacy in global organizations, a director explained, is that different regulators handle privacy and cybersecurity issues differently. *"In the case of the EU, they have competence for privacy; security is the competence of the nation state. And various oversight organizations give emphasis to one wholly over the other. And then if you've split that inside your company, it becomes a worse proposition, because you'll find that your company is in a channel or a stovepipe dealing with one or another—privacy or security alone. If you're being asked questions that disproportionately emphasize either cybersecurity or privacy, then you have to force that back into an alignment such that you're never taking the bait: you're never essentially serving only one master."*

While no one method offers a perfect solution, boards are finding various ways to avoid siloing privacy and security issues.

Integration within the audit committee

One director described a traditional, heavily burdened audit committee, but reported that the committee had *"evolved to become as comprehensive as possible: We grew from cybersecurity into privacy areas, but often find ourselves reacting to what's in front of us. It's about trying to manage the agenda and the audit committee's limited time."*

Another director's company *"views privacy, cyber risk, and data security as integrally linked,"* and the audit committee *"takes an hour to an hour and a half to do a briefing on cyber and privacy at each and every single meeting."* Cyber and privacy are always first on the agenda, and at meetings, and *"all board members are invited. Most generally do attend that portion. Annually, we take it up to the board level and review in more detail what's happening in these areas."*

That director emphasized that privacy is integral to many functions and decisions, *"The protection of privacy and confidential information is so integral to how you run your systems and to cybersecurity … There are differences in their focus, of course: what information should be collected, what rules you have with respect to the retention of information, how to destroy and when. These are more of an operating responsibility of the company, including marketing; but we as a board oversee it on an integrated basis."*

The risk committee

At another company, a director said, the risk committee looks at risks for both cybersecurity and data privacy: *"There's a natural intersection between cyber and data privacy. You can't have pure privacy without having protections of that data. We look at both at the same time in the risk committee. We have a risk dashboard. Both cyber and privacy are on that dashboard, and we get quarterly updates. Once a year, we do a deep dive. We have reviewed privacy in particular at every meeting this year."*

Cooperation of the risk and cyber committees

One director described a model of close cooperation between the risk and cyber committees. The board *"is focused on cybersecurity—it comes in through the technology lens—but appreciates that there's a people component and a doctrinal component to that. The risk committee deals with some of the other traditional issues of risk attendant to privacy disclosures. There's always a shared meeting between those two, each quarter, and we try to ensure that each committee is asking both majority and minority questions … and there's always the opportunity to crosswalk that between the two committees."*

Privacy by design is becoming integral to product development

Many members' companies are working to build privacy safeguards into new devices, applications, computer systems, and networks, starting at early design stages. Mr. Richards noted that, in areas ranging from vehicle information to digital medical devices, *"the design team is much more open and transparent,"* and privacy by design has become *"part of the*

bigger business conversation. Rather than letting the technology drive policy, now we're having policy drive the technology."

Directors described multiple challenges to full implementation of privacy by design:

- **Legacy systems.** Older systems pose significant obstacles to privacy by design, and in some cases, the risks of retaining them may not receive sufficient attention. While executives and board members *"have a good understanding of business risk,"* a director said, "*they may not fully understand the digital risk, and this applies doubly for legacy systems."* In addition, many companies lack the resources to undertake wholesale redesign of older systems. As one director said, *"You can wrap your whole system in privacy with new devices, but you're often hamstrung by your past. Not everyone has the same opportunity to rebuild."*

- **Organizational obstacles.** Building in privacy by design often involves organizational and related cultural challenges of split responsibility for privacy, such as the need to overcome silos and create cross-functional product-oriented teams. *"One part of an organization may be focused on tech issues and the other on business and customer-facing issues,"* a director explained. Ms. Sumner stressed the importance of increased coordination, since problems arise when *"those who are focused on privacy compliance are not plugged in with IT and security in a meaningful way."* As chief privacy officer of a global law firm, she chairs the firm's privacy committee and sits on the technology governance committee, because even when looking at privacy *"from a compliance perspective,"* she said, *"you have to understand data mapping and the architecture of the organization's network … just like they are important from a security perspective. You run into issues when it's not coordinated, and the communication process is siloed."*

  A director explained how one company created a special management committee to address the problem of *"working across the inevitable silos or verticals in an organization. We created a management committee focused on risk. A cross-section of people—the CISO, CIO, marketing, revenue, operations people, our internal auditor, plus privacy and legal people—are members. Their job is to talk about evolving issues, and legacy issues as well."* This committee addresses issues such as those that arise *"as the marketers start talking about using data to accomplish their missions. In new business ventures, we've found that historically the risks were not talked about as much as they should've been, so now they do in this forum that allows them to pull it all together."* Another director's company had also included *"public affairs and government relations people in discussions on privacy, so they are up to speed and aware and can prepare accordingly."*

  A third director elaborated on specific organizational and procedural pitfalls. *"You often find you didn't have a data architecture, or you didn't have a simple taxonomy that says who can access data under what conditions … Those authorized to take risk are different from those expected to mitigate risk. Traditionally, you'd find the folks in the operations sector were*

authorized to extend business, sometimes necessarily, into risky areas. They understood the nature of the business risk but not the digital risk. Then they handed over to the IT crowd the responsibility of that risk, but the IT crowd didn't know it was being taken in the first place. You have to rationalize that up front."

Redesigning systems to build in privacy protections

Sometimes, implementing privacy by design requires rebuilding older systems. A director shared the example of a large auto manufacturer that did not originally build in privacy protections to its onboard tracking technologies. Such protections were *"not in the inherent design because people were not thinking about that as much as today 15 to 16 years ago."* In redesigning its technology to build in privacy protections, the automaker faced challenges driving the redesign through suppliers, partners, and dealers, some of which had their own legacy systems that may not have been compatible. However, the company successfully completed the redesign two years ago, with data protections built in. Now, says the director, *"since we're doing more in the autonomous field, we think of cyber at every step of the way throughout our processes. The company has driven to centralize all customer information so it can be fully encrypted, stored, and they know when they're retiring that data."*

A director argued that the most *"successful strategy is to view data as a foundational tool, not a commodity."* Specifically, *"companies that define a data architecture and describe the attributes of the data up front are more likely to succeed in rationalizing that data to the purposes of the business. You can define the interaction of people to that data, and the fundamental action within the company's architecture will be exercised critically against that data."*

Secure multiparty computation

An emerging technology—secure multiparty computation—could easily become highly relevant for data privacy. Noting regulatory and reputational risk concerns that can arise from the data used for artificial intelligence and machine learning, a director described this important new technology as *"privacy preserving … It allows you, for example, to aggregate data or enable machine learning across a whole lot of data without ever actually seeing the data itself. This isn't: 'Send me your data and I'll keep it secure for you.' This is: 'You never have to send me your data at all, but I can still run machine learning algorithms over your data and get the results.'"*

The director surmised that this could have important regulatory implications, noting that *"GDPR mandates that everything has to be done using minimal revelation of data."* The director continued, *"If this technology allows minimal revelation of data, to the point where there's no revelation of data, then GDPR actually requires you to use it. I*

Secure multiparty computation

think, increasingly, we'll see this technology coming onto the market and regulatory pressure will force people to adopt it."

For further information on secure multiparty computing, see Multi-Party Computation.

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.

Endnotes

[1] Kyle Brasseur, "French Court Upholds Google's $57M GDPR Fine," *Compliance Week*, Jun 22, 2020.

Appendix 1: Guest biographies

- **Rob Dedman** is a partner in the Special Matters and Government Investigations practice at King & Spalding and former head of enforcement at the Bank of England/Prudential Regulation Authority.
- **Steven Weber** is a professor at the University of California, Berkeley School of Information; a senior policy advisor at Glover Park Group in Washington, DC; and adviser to governments, multinational firms, and international nongovernmental organizations.

Appendix 2: Meeting participants

- Joan Amble: Zurich Insurance Group, Booz Allen Hamilton, SiriusXM
- Marianne Brown: Northrop Grumman, Akamai, VMWare
- David Ching: TJX Companies
- Bill Easter: Concho Resources, Delta Air Lines, Grupo Aeroméxico
- Linda Gooden: ADP, General Motors, Home Depot
- Pat Gross: Liquidity Services, Perdoceo Education, and Rosetta Stone
- Fritz Henderson: Marriott International
- Chris Inglis: FedEx, Huntington Bancshares
- Leslie Ireland: Citigroup
- Tom Killalea: Akamai, Capital One Financial
- Holly Keller Koeppel: AES, British American Tobacco
- Jane Holl Lute: Union Pacific, Marsh & McLennan Companies
- Bill Phelps: Executive Vice President, Booz Allen Hamilton
- Kevin Richards: Executive Vice President, Booz Allen Hamilton
- Stuart Russell: Intact Financial
- Sherry Smith: Deere & Co.
- Phyllis Sumner: Partner, King and Spalding
- Mona Sutphen: Pioneer Natural Resources
- John Thompson: Norfolk Southern
- John Veihmeyer: Ford
- Lynn Vojvodich: Booking Holdings, Dell, Ford
- Sue Wagner: Apple, BlackRock, Swiss Re