CYBERSECURITY MEETS REALITY

Cyber risk can't be eliminated, but it can be managed. Directors shared oversight strategies at *Corporate Board Member's* 2021 Board Risk Forum. Some ideas.

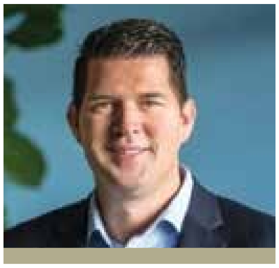
The notion of cybersecurity as a systemic risk for companies is not new, but the past year of remote work and the increased frequency of cyber crime certainly underscored that it has become one of the biggest risks facing boards today. Digital transformation and the Internet of Things have opened up points of entry in every area of operations, as well as all along the supply chain, and the resulting decentralized networks are trickier than ever to safeguard.

At the same time, regulators, investors, customers and other stakeholders are stepping up pressure on boards to actively demonstrate diligence in the area of cybersecurity; they expect personal information to be protected, systems to be resilient and processes to be in place to quickly address attacks when they happen. When companies fail to deliver on that, shareholder lawsuits inevitably follow, and directors have been increasingly named in derivative suits.

But for most board members, who typically have no background in technology or IT security, cybersecurity risk remains one of the most challenging areas of oversight. In March, directors gathered virtually to hear from industry experts and corporate chief information security officers about how to wrap their arms around this mushrooming risk and how to recognize it not only as a threat but an opportunity. Takeaways from *Corporate Board Member*'s Board Risk Forum follow.

CISOS SPEAK: WHAT THEY WISH THEIR BOARDS KNEW

From making sense of analytics to supply chain partner considerations, these are the most critical questions you should be asking.



Niall Browne, Senior Vice President and Chief Information Security Officer, Palo Alto Networks

Dawn Cappelli, VP, Global Security and Chief Information Security Officer, Rockwell Automation

Erinmichelle Perri, Chief Information Security Officer, The New York Times

The CISO's shift from primarily defensive triage and toward proactive offense has created a learning curve for directors accustomed to asking questions about reactive measures. "It's been a process, I'd say in the last five to 10 years, to get the board to understand that the questions they should be asking are quite a bit more about how are we securing our products and services? How are we getting this right from day one?" said Erinmichelle Perri, CISO for The New York Times.

Along those lines, the panelists recommended boards prioritize the following questions for their CISOs:

WHAT IS OUR "SHIFT LEFT" STRATEGY? It is no longer an option to build products, or really anything inside a company, without considering security from the ground up, said Niall Browne, senior vice president and CISO, Palo Alto Networks, who likened it to building a house without considering plumbing or electricity. "Then suddenly the electrician turns up and says, 'Oh, by the way, we've got a wire here, we're going to rip down the walls.'"

In most operations environments today, trying to update security piecemeal is complicated by "tremendous scale," says Browne. "You've got dozens of clouds. You could have hundreds of thousands of images that are spun up every single second and spun down. It's ephemeral, it's dynamic, it's continuously changing. So if you're using traditional models to go back there and try to fix the issues after they've occurred, it's game over. There's no way anybody can ever keep up."

HOW IS SECURITY BEING ADDRESSED HOLISTICALLY THROUGHOUT THE ORGANIZATION? Dawn Cappelli, VP, global security and CISO for Rockwell Automation, recalled that after the WannaCry ransomware attacks in 2017, Rockwell realized they had some potentially dangerous silos in their security programs, where manufacturing, products, services and other areas were individually protected. "But we needed to bring all of that together," she said.

To do that, the team developed what it called the connected enterprise ecosystem cybersecurity strategy. "Big mouthful there, but basically what it means is we have one comprehensive strategy that encompasses the entire ecosystem," says Cappelli. That includes IT, manufacturing, supply chain, third parties, the company's own products, security, M&A partners, services, connections to customers and cloud providers and all third-party software the company uses. "So, when we talk with our manufacturing or supply chain departments about risk in their area, it's part of this comprehensive program," she said.

WHAT IS OUR THIRD-PARTY RISK? The SolarWinds cyberattack—which involved thousands of companies' networks being infected by Russian malware downloaded via a simple software update—made clear that a company's products can be put at risk by any partner company's security breach. "A lot of companies haven't thought a lot about that," said Cappelli, who recalled another recent case of a company's file transfer product being infected with ransomware, which was then downloaded to customers, whose information was then stolen and who were then extorted for its return.

To get the full scope of the risk, Browne recommended conducting a tabletop exercise specifically focused on the supply chain and what the impact might be if attacked. "You want to have at least 10, 15, 20 departments in the room—legal, finance, etc.—and you want to run it from end to end. If there is a compromise, how do you detect it?" Then, consider what would be done in the first 24 to 48 hours to remediate "because that's going to be the most critical time," he said.

Companies that fail to do that end-to-end scenario-planning will wind up trying to come up with a solution during those first hours—and 48 hours can quickly become 72 or 100-plus. "That's a disaster," said Browne, "because you're creating material on the fly."

Rather, the whole team should sit down and figure out exactly what will happen in the event of a breach. What is the canned questionnaire that will be sent to every vendor on the network? Which team is set up in house to deal with the responses and do a risk assessment? "Oftentimes, if you have a breach, it's not the fact that you've been breached—because a lot of organizations have been," said Browne. "It all comes down to how transparent you were, how quickly you responded, how quickly you notify the customers. I'm a huge believer in that transparency, making sure you're prepared for that."

WHAT DOES OUR COMPANY'S SECURITY AWARENESS PROGRAM LOOK LIKE? The human element "is always the wild card, the weakest link," said Cappelli. And that was exaggerated during Covid with everyone dispersed and working from home. "We've had to keep security front of mind for them." To do that, Cappelli's team makes videos about the latest security-related news, holds monthly security lunch-and-learns with the entire cadre of engineers and invites in outside experts to give talks on relevant topics. "We had an Emmy Award-winning journalist come in and give a talk on social networking security because a lot of these attacks now are coming in using information gleaned from social media activity," she said. "Our security awareness has never been higher. My goal is, once we get back to the office, let's keep this online security awareness going."

WHAT POSITIVE LESSONS HAVE WE LEARNED? Perri noted that being forced to pivot over and over to solve challenges brought on by Covid and remote work stress-tested the system in real time and demonstrated the creative potential of the team. "So, I think really going into 2021, we're stronger than ever," she said. "In terms of opportunities here out of chaos, we're going to see a lot of great lessons learned."

She also emphasized the need for both management and the board to keep in mind the toll this past year has taken on IT employees. "The workforce is burnt out" after Covid, Perri said. "We need to keep the human element in mind. We need to be flexible, empathetic, meet employees where they are."

RANSOMWARE: AN EVER-EVOLVING RISK

Stats

Ransomware toll in 2019:

$11.5 billion

Estimated toll in 2021:

$20 billion+

Average cost of remediating in 2020:

$761,000

Average cost of remediating in 2021:

$1.85 million

Average ransom paid per company:

$233,817

Average downtime:

19 days

In March, a ransomware attack against insurance company CNA again illustrated how smaller companies can easily find themselves the victims of a larger hack, if the stolen data is used to extort money from the original target's customers. And the data demonstrating the prevalence of ransomware attacks shows no signs of abating. Since 2016, there have been more than 4,000 cases every day, according to FBI figures. "But that's likely a very low estimate," said Scott L. Howitt, SVP and chief information officer for McAfee. "They're using the stats that were reported to them and in a lot of cases, people don't report it because they don't want the bad press to follow them."

That's understandable—particularly considering the high financial toll this particular cyber crime has taken on targeted companies. Howitt offered steps to mitigate risk:

SEGMENT NETWORKS. Howitt recommends boards ask their CISOs about creating divisions between networks to ensure that when one is infected, the malware doesn't spread as easily to the rest. For example, as CISO of MGM Resorts International prior to McAfee, Howitt worked on segmenting the networks of the casino's hospitality, restaurant, retail and entertainment networks in order to mitigate potential damage to the whole business.

Internet of Things (IoT) applications have made the job of securing all points on the network even more complex, adding new risks, he added. At MGM Resorts, the refrigerator technology allowed temperatures to be regulated remotely. "So now [we had to consider], what if somebody came in and raised the temperature of the chicken, so now suddenly I've got poisoning risks, and it's a life safety issue instead of being a data leakage issue."

IDENTIFY THE POTENTIAL THREAT ACTORS. While active monitoring for potential attacks is critical, it's not enough. Your CISO should be able to identify the bad actors most likely to target the company and then ask what they are doing proactively to prevent those attacks. "Because that's one great thing about threat actors—they're not very inventive," said Howitt. "They only have to get it right once or twice, so they throw an attack against 1,000 people and if one or two catches, it's worth the money."

MAKE SURE THERE IS A COMPANYWIDE PREVENTION/AWARENESS PROGRAM—INCLUDING THE BOARD. Most malware is spread initially through a phishing email sent to an employee with network access, which is what happened to CNA. "They had a very robust cyber program, but that's the trick—it only takes one click for something bad to happen," Howitt said.

MAKE SURE SECURITY IS BEING ADAPTED FOR THE FUTURE. Most security people grew up primarily in a physical network environment, said Howitt. As companies go to the cloud and transition to a software-based world, how is your CISO retooling the security organization to adapt? To that end, he or she should be having conversations with all the company's business owners—not just internally with the security team. "It's okay to put your CISO on the spot and say, 'So, as the world changes to a network-based world, tell me what you know about the business. How are you adapting that to meet the strategy?'" he said. "If the CISO isn't thinking about it in terms of business strategy, it's checkbox compliance. That will get you past the audits, but it won't necessarily keep you secure."

TO PAY OR NOT TO PAY?

To be sure, ransomware attacks only thrive in a world where victims pay the ransom. But whether or not to pay is an age-old question without a clear-cut answer. "It's easy to be morally right and say you should never pay, but it has to be a business decision," said Howitt. Factors will include the ransom amount, the files that have been targeted, the cost to the business of having files stay locked, etc. According to the latest data, only 26 percent of firms pay, and that may be because their cyber insurance firms require it.

"From an actuarial standpoint for them, it's cheaper if they just hurry up and pay the ransom and take the chance of getting the attack over with," said Howitt. But he points out that payment does not guarantee the return of the data that was stolen. "It's always a very dicey proposition to pay them off because they might not unlock your files, and they'll just take your money and run."

Howitt recommends conducting a tabletop exercise that looks in detail at the potential impact of a ransomware attack on each area of the business. "The frequency of tabletop exercises should be every quarter," he said. "And it doesn't have to be a full day. You can accomplish a lot in an hour or two. It should be a very specific scenario.

"The ask is, what we need to do, and then is it working? Should we do more or less? Kill it? The data-driven decision is becoming more and more important."

WHAT ISS THINKS ABOUT YOUR CYBERSECURITY OVERSIGHT

Mark Brockway, Head of Corporate Solutions, ISS

Marija Kramer, Head of ESG Analytics Business, ISS

Cybersecurity ranked first on the list of concerns for 67 percent of investors, according to the 2019 RBC Responsible Investing survey. That number isn't likely to decrease, given the escalating costs to companies. The annual economic cost of cyber breaches is estimated to run as high as $1.5 trillion, according to Marsh & McLennan's Cyber Risk Center. And, in addition to the $8 million direct cost, on average, to U.S. companies, the indirect costs, including reputational risk, stock price performance risk and litigation risks—the last evidenced most recently by a recent class-action lawsuit against SolarWinds—are enormous.

Among ISS's Russell 1000 constituents over the past four years, almost all sectors were negatively affected when it came to financial returns post cyber breach. "Investors care about cybersecurity for many reasons, but most importantly because it can really impact the bottom line," said Marija Kramer, Head of ISS ESG Business.

As the investor community attempts to quantify cyber risk across its investments, many rely on ISS's Governance QualityScore to help assess and benchmark boards' information security risk oversight. Here are some key indicators ISS is looking at on behalf of investors:

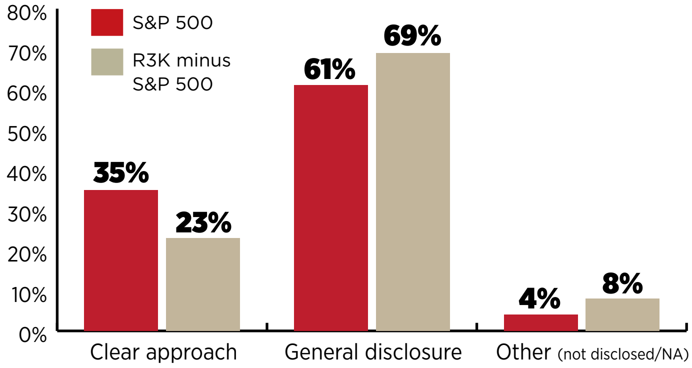
1. TRANSPARENCY. ISS looks not only at whether companies are providing disclosure related to cybersecurity risks but also at the quality of that disclosure, said Mark Brockway, head of corporate solutions at ISS. "So, is it more general in nature or do they have what we call a 'clear approach'?" A clear approach means a detailed discussion of the information security risks specific to the company and the strategies to mitigate this risk, Brockway explained, noting that while more companies are disclosing, few are taking a clear approach. (See chart, below.) Kramer added that investors want to know the expected costs of a potential breach so they can factor that in.

2. A COMMITTEE TASKED WITH OVERSIGHT. "That committee can either be on a standalone basis or part of an existing committee, oftentimes audit," said Kramer, who noted that a little more than three-quarters of the S&P 500 now have this in place. She added that there is also evidence that investors are going to hold portfolio companies to outside standards and assurance of their policies and practices being monitored by an ISO or other standard setter.

3. BOARD EXPERTISE IN CYBERSECURITY. This is becoming increasingly common among larger-cap companies. ISS found 92 percent of the S&P 500 and about 55 percent of Russell 3000 companies have three or more directors with information security expertise. "This is quite prominent in certain sectors where exposure is more significant," said Kramer, "but it's really front and center to the needs of investors is they're doing their assessments and looking to engage with portfolio companies."

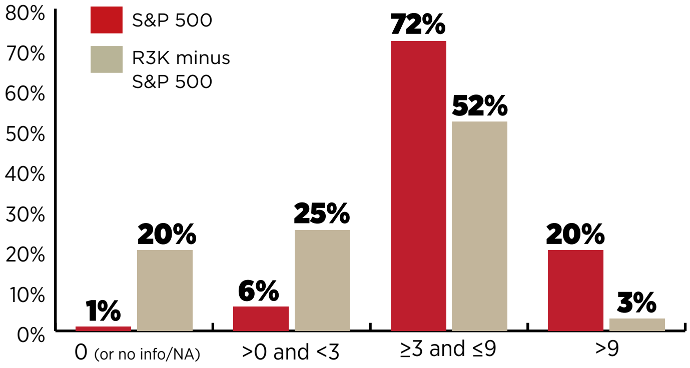
STILL LACKING CLARITY

Most U.S. companies are disclosing general information about information security risk, but few are taking "clear" approaches, which would include a detailed disclosure of risks and strategies to mitigate them.



CYBER EXPERIENCE ON BOARD

Most boards have information security expertise, which ISS defines as either the company disclosing that directors have these skills or that directors' experience suggests skills in this area.



Source: ISS Corporate Solutions Governance QualityScore data for factor Q402-412. Data as of March 2021.

GETTING CYBERSECURITY OVERSIGHT RIGHT

It's complicated, overwhelming and seemingly impossible, but directors can play a critical role in staving off and recovering from cyber events. Here's how.

Melissa Hathaway, President, Hathaway Global Strategies

By now, we're all a little cyber fatigued. The names of cyber attacks and the high-profile companies victimized by them appear in headlines with such regularity that infiltration feels inevitable. At the same time, intensifying regulatory requirements demand that boards remain vigilant about safeguarding data.

The good news? Understanding four types of risks and what can be done about them can help directors vet a company's cyber practices, says Melissa Hathaway, the former head of cyberspace policy review for President Barack Obama and the former leader of President George W. Bush's National Cybersecurity Initiative. Her breakdown:

TECHNOLOGY RISKS

As a board member, you don't need a deep understanding of technology to ask questions that can help your company strengthen its defenses. One area to check is your technology debt, or how much of your hardware and software is outdated and no longer supported by the provider.

"If you've got no way of keeping the systems current—no patching cadence—your systems are 100 percent vulnerable, 100 percent of the time," notes Hathaway. "So, how are you managing that risk, and what is your timetable for a capital refresh? Those are board-level discussions."

OPERATIONAL RISKS

Boards also need an understanding of which assets, services and data that might be compromised in an attack are most critical and how quickly the company will be able to recover them. Topping most lists is the active directory, a frequent target of malware.

"The active directory is essentially the Rosetta Stone for what employees are allowed to do in your company," says Hathaway, who says part of the recent SolarWinds hack involved infiltrating active directories to create new personas, then escalating their privileges to gain data access. "Companies can mitigate that risk by keeping an up-to-date active directory offline."

LEGAL RISKS

Staying on top of a constantly evolving regulatory landscape is also critical, particularly for global companies operating in countries with increasingly strict requirements. "If you operate in Russia or China, for example, you have to allow those governments to put their equipment on your infrastructure," says Hathaway. "And the definition of personal protected data is much broader in certain places—Brazil and California—than others."

Given the penalties running afoul of mandates can incur, directors should be asking for regular briefings about compliance across all jurisdictions in which a company operates in areas like data protection, data privacy and breach reporting requirements. It's important to acknowledge that some requirements, such as accommodating content takedown requests or continuity of service requirements, will apply more to some businesses than others, as well as that meeting them all may not be feasible.

"Then it becomes, what's our risk appetite?" says Hathaway. "Do we want to change the technology, change the way we operate, or maybe even rethink being in that market if the revenue doesn't justify the risk?"

FINANCIAL RISKS

Often intertwined, technical, operational and legal risk all lead to potential costs. Companies may need to devote funds to upgrading cyber insurance policies, invest in replacing outdated systems in order to enable regular security updates or boost liquidity to cover the cost of an inevitable eventual event. Europe's General Data Protection Regulation (GDPR), for example, allows the EU's Data Protection Authorities to issue fines of up to €20 million.

Cyber risk assessments of target companies should also factor in M&A valuations. "Consider what happened to Marriott, which really should have treated Starwood as a tainted asset when it had a major breach during the deal process," says Hathaway. "They went ahead and integrated anyway, and the second breach ended up incurring one of the largest GDPR fines plus class action lawsuits."

Directors don't need to be technology experts to help companies strengthen their defenses in these three areas. Rather than a deeply technical conversation, the board's approach should be holistic, asking: What do we, as a company, need to do from a technological perspective to mitigate risks of delivering our product or services in the markets we're in?

"Then, for the risks we can't mitigate, the question is, 'What are we going to do to manage through them, whether that's recovery planning, insurance or a reserve on the balance sheet?'" says Hathaway. "Boards just need to tackle it in a comprehensive and intelligent way."

—Jennifer Pellet

MAKING DATA PRIVACY A COMPETITIVE DIFFERENTIATOR

Companies that falter on data privacy practices risk running afoul of regulators—and missing an opportunity.

Myrna Soto, Board Member, CMS Energy, Spirit Airlines and Popular Inc.

David Forman, Vice President of Privacy & International Assurance, Coalfire

Technology permeates every aspect of life today, creating a staggering amount of data on a daily basis. In the course of regular operations, your company is probably collecting vast quantities of information while engaging with stakeholders, from customers and suppliers to employees and shareholders.

The number of risks associated with that new reality are vast and growing. Data misuse or unintended disclosure can bring erosion of customer trust, loss of business opportunities, and reputational harm. Further complicating matters, the concerns over the sheer amount of data being amassed coupled with the frequency of breaches are also prompting a rash of regulatory activity, as states and nations rush to address data privacy concerns through legislation.

BREACH FATIGUE

"For a while there was a little bit of breach fatigue, where people were quasi-numb to the headlines about the data elements out there in the wild that had been breached," Myrna Soto, a board member at CMS Energy, Spirit Airlines and Popular Inc., told directors gathered for a panel discussion sponsored by the cybersecurity advisory firm Coalfire. "But what's happening now is our legislators and regulators are starting to look at not only what corporations are obligated to report, but their obligations regarding managing data protection and data privacy. We're seeing very aggressive regulatory movement."

"It seems like every week we get another news blast that a new data privacy regulation has been proposed at the local, state or country level," agreed David Forman, vice president of privacy & international assurance at Coalfire. "More than 25 states have already proposed or passed legislation around data privacy. Most of our clients are caught in a mode right now where there's an evolving regulatory landscape and the rules are changing on them constantly, while they also have to meet the [data] needs of sales, marketing and other internal interested parties."

In the absence of a federal standard, complying with the pockets of varying data protection and privacy requirements popping up across the U.S. will be challenging. However, there's also an opportunity for companies to stand out from their peers by taking proactive steps toward handling more data responsibly, notes Forman. "It's important for consumers generally to be able to look at a company and say, 'Hey, they're doing things the right way. Whereas, if action is only happening when there's a bad news cycle or an investigation by the FTC or DOJ, then that's going to [generate] distrust toward that company and their products."

Already, corporate leaders on privacy are emerging. Soto, who is also chief strategy and trust officer at Forcepoint, urged board members to take note of Apple's privacy initiative to remove apps that track consumers data without their permission from its app store. "That's important to boards because most companies have a digital presence, some type of app of their own, and we as board members should understand, what are we doing with that data?" she said. "Why are we tracking it? And probably most importantly, are we advising our consumers of what we're doing—and making sure there is an opt in versus just an opt out? Those are brand-protection perspectives you may want to think about in the boardroom. How are we protecting the company's brands from an unfortunate incident or deterioration of confidence?"

Directors should also be aware that data privacy protections call for consumers to be able to change their minds about the permissions they grant. "We have an obligation to make sure that if we collect data on preferences from a particular customer's activities, the customer has the right to say, 'I want you to forget about that,'" said Soto. "You can also put yourself in a liability situation if you don't understand how a third-party processor of your customer data is accessing certain data elements. Those are some of the scenarios you need to think through and address when you look at data analytics."

For many companies, the top challenges are collecting enough data to deliver a tailored experience without overstepping customers' desired level of data privacy, managing that data responsibly and having the ability to adapt when that level changes. On the plus side, as privacy concerns continue to gain momentum, such diligent data privacy practices will pay off.

"As companies get comfortable saying, here are all the things we're doing in security and privacy, you'll see consumers will gravitate toward that," said Forman. "This is a profound opportunity for reputation building going forward." **CBM**

—Jennifer Pellet