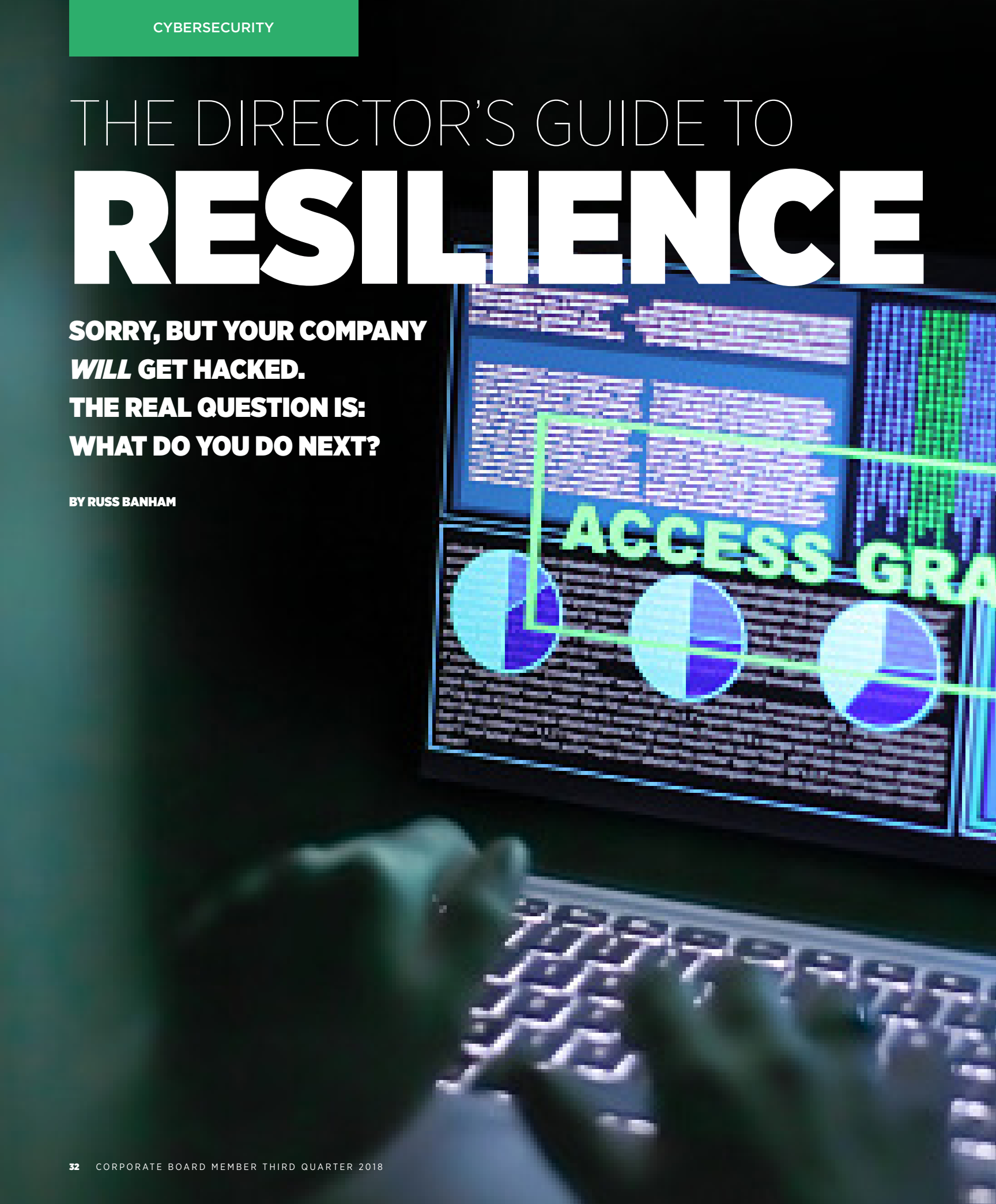
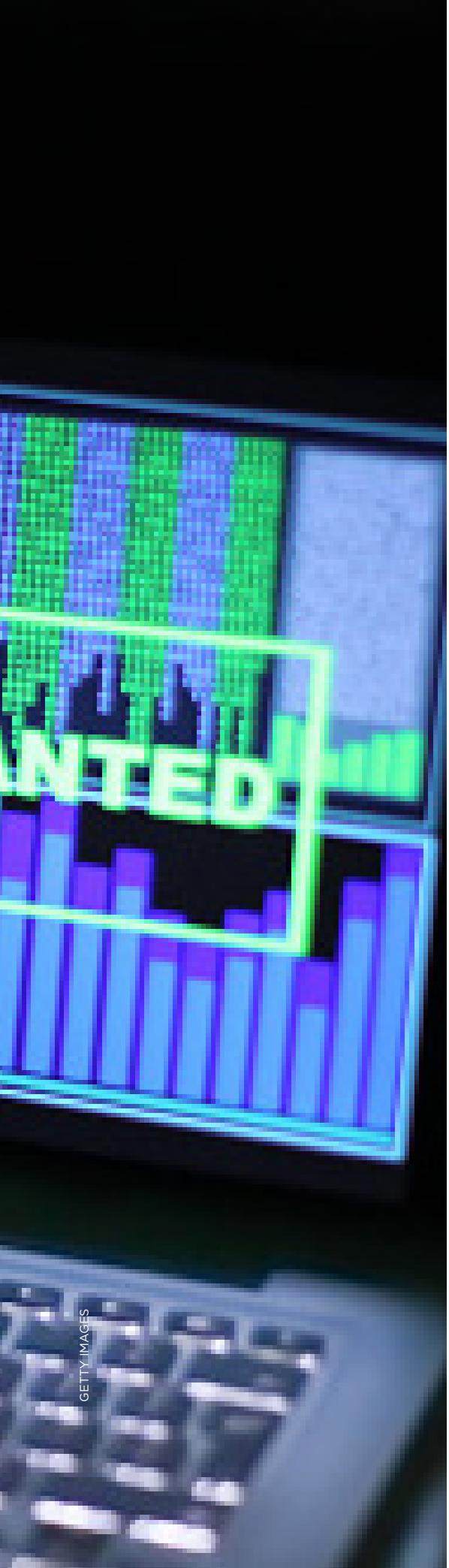
THE DIRECTOR'S GUIDE TO RESILIENCE

SORRY, BUT YOUR COMPANY *WILL* GET HACKED. THE REAL QUESTION IS: WHAT DO YOU DO NEXT?

BY RUSS BANHAM





GETTY IMAGES

IN THE GAME of dodgeball, the objective is to avoid being hit by a ball hurled by an opponent—but at some point, the ball inevitably strikes the mark. Hackers play a far more dangerous version of this game, launching a fusillade of cyber attacks daily. The company on whose board you sit will manage to skirt many attacks but some will succeed.

Nearly every midsized company and large enterprise has been hacked at least once, with no industry spared. Accordingly, board directors must give as much of their attention to what happens after a cyber attack as they do to all of the security measures designed to ward off an incursion.

This responsibility became unnervingly clear following the comedy of errors that ensued in the aftermath of the devastating Equifax data breach last year caused by an unpatched vulnerability. The attack exposed the Social Security numbers, birth dates and addresses of 145 million American consumers.

Chief among the pratfalls was the decision by Equifax's former CEO to wait three weeks before telling the board a massive breach had occurred. By then, directors could do little to stem the damage.

"Board directors have legal and regulatory responsibilities and accountabilities as fiduciaries to protect shareholder value, yet they were intentionally shut out of a disaster that resulted in a 35 percent drop in stock price, wiping out $6 billion in shareholder value," says Jason Hogg, a former special agent with the FBI and currently CEO of Aon Cyber Solutions, a developer of cyber insurance products.

No board wants to feel its views have little import, particularly at a time of extreme corporate duress. Consequently, the onus is on directors to ensure by way of tough, informed and insightful questions that the company they serve can take a hit and recover.

"We live in an era where the world's most important companies can be the victims of a data breach or a complete network collapse, resulting in untold damage to their market value, reputation and brand," says Dottie Schindlinger, governance technology evangelist at Diligent, a provider of enterprise governance management solutions. "If this occurs, you can't wait days to put together a report, and you can't wait weeks to tell the board. The company is on fire."

MALWARE MISERIES MULTIPLY

Woe to any business that falls down the rabbit hole like Equifax. Fortunately, many boards are acutely aware of the existential realities of a major cyber attack. Board director Sheila Hooda sits on two boards—public company Virtus Investment Partners and Fortune 300 insurer Mutual of Omaha, which has publicly traded debt. She says that the risk of a cyber attack is "at the top of the agenda at every board meeting. It's unrealistic for any business to believe their defensive measures will protect them. Cyber criminals are getting smarter by the day."

A case in point is the cyber attack launched against container shipping giant Maersk in mid-2017, which caused $300 million in business interruption costs. Hackers took advantage of the company's security vulnerabilities by using an unknown type of malware dubbed NotPetya that borrowed code from the known Petya ransomware. Hackers demanded a mere $300 in bitcoin as a ransom to restore the ability of employees to access data. "The goal with NotPetya is not necessarily to extract a ransom; rather it appears to be a complete shutdown of a company's network for malicious purposes," says Hogg.

Maersk's information security team applied upgrades and patches to resus-

citate all its systems within 10 days, an extraordinary feat given that it required the reinstallation of 4,000 servers, 45,000 computers and 2,500 applications.

Who were the perpetrators? It's anybody's guess. "The attack surface has gotten radically bigger, with nation-states, terrorists and criminal enterprises all gunning for targets," Hogg says. "Boards are aware of the dangers but generally trust that senior management is on top of the threat."

Is this trust misplaced? "The board must remain objective, which in this case means skeptical," says Wesley McGrew, director of cyber operations at Horne Cyber, a provider of cyber resilience services. "Following an attack, the CEO will back up the chief information security officer (CISO) and the IT team, since he or she hired them. Unfortunately, they have a tendency to downplay the threat."

McGrew is far from alone in this opinion. "I do a lot of presentations for Fortune 500 companies around the topic of cyber resilience, and the assumption among most is that they're already resilient," says Andrew Morrison, principal, cyber risk services, and U.S. leader of cyber risk resilience at consultancy Deloitte Risk and Financial Advisory.

Are they resilient? "Most organizations are prepared for cyber attacks that have occurred before, but they're panicked about this new wave of crippling attacks like NotPetya, a 'scorched Earth' scenario that takes down the entire entity," he says. "Board directors need to be clear and direct in questioning senior management, asking what the plans are to bring back to life the elements of the business that are critical to its continuance and solvency."

Few plans are more crucial, given the possibility of "corporate extinction," says McGrew. "Resilience is about knowing exactly what will be done before the disaster strikes; you can't be figuring out what you'll do while the bombs are falling. You want the business to bend from the onslaught, not break."

NO WALLS ARE IMPENETRABLE

A company's response to a cyber attack is as important, if not more so, than the measures taken to prevent it. "Companies will be judged as harshly for a botched response to a cyber attack as for being vulnerable in the first place," says Schindlinger.

Since many companies experience hundreds of attacks each week, not all incidents require immediate board oversight. "Once a serious attack has been detected, it is no longer a technology and security issue, it becomes a business risk," says Hooda. "At this point, the board needs to be immediately apprised of the situation. The company now is in crisis communications mode."

> "Resilience is about knowing exactly what will be done before the disaster strikes; you can't be figuring out what you'll do while the bombs are falling. You want the business to bend from the onslaught, not break."

McGrew agreed that the circumstances of the incident dictate when to contact the board. "IT security is the responsibility of IT managers, but when a cyber attack poses severe implications on the continuance of the business, the C-Suite and the board are responsible for what happens next," he explains.

External stakeholders like customers, suppliers, vendors and investors will need to be contacted, as will law enforcement, outside legal counsel and the media. Timing is of the essence for regulatory and financial reasons. In some jurisdictions, companies must report a data breach and notify affected parties within a scant 72 hours, the case with the recent implementation of the GDPR (General Data Protection Regulation) in Europe. The penalties for noncompliance are staggering—as much as 2 percent of annual worldwide revenue.

Depending on the nature and scope of the attack, there is an order of priority in these external communications. "This is a giant chessboard with lots of moving pieces; the company has to know when to move the bishop and the queen," says Schindlinger.

Since no two incidents are exactly alike, quick judgment calls are required. "If the network is shut down in a 'scorched Earth' scenario, companies must decide which systems and applications need to come back on line first," says Morrison. "In healthcare, this would be life safety; in investment banking, it could be derivatives trading; in manufacturing, it might be certain machines making certain products in certain locations. Directors will want instant answers to these questions, as they should. If they have been kept in the dark about these communications, it will cause panic and bad decisions."

The loss of the network is not the only existential risk. "In the case of a data breach, directors must assess the threat to intellectual property like a patent or a trade secret, contract bidding criteria for a construction firm or the source code for a software company," he says. "Someone gets a hold of this information, and they can whittle down your market share or launch your biggest competitor."

PAST IS NOT PROLOGUE

Since the above scenarios are somewhat predictable, they should be addressed in a comprehensive business continuity plan. "Within the organization, roles and responsibilities need to be established beforehand for the crisis communications," says Hooda. "It's up to the board to ask questions, making sure the response is moving forward as planned. The goal is to get the business back to normal at the earliest time possible."

The problem in many companies is that incident response plans collect dust,

failing to evolve dynamically to address newer scourges. "This will sound self-serving, but you need an outside firm to continually revise the plan," says Hogg, who argues that external cybersecurity experts are able to cross-pollinate cyber risk information across multiple clients in diverse industry sectors to get a clearer sense of possible attack vectors.

He urges boards to find external help before a crisis occurs so they can be primed to leap in and apply countermeasures. "When things go wrong, they go wrong fast and big," he says. "You need boots on the ground within a period of hours. You don't pick your players on the day of the Super Bowl."

McGrew agrees. "When the walls are breached, you want full-time security professionals to roll in like a field team to figure out what's going on," he says. "Is it over? What's the exposure—and what needs to be done to regain some semblance of business continuity?"

Companies that rely solely on internal employees also run the risk of being misled. "The CISO and the IT team may be inclined to gloss over the scope of the disaster to deemphasize their potential culpability," McGrew adds.

Morrison agrees that a CISO is likely to say everything is under control. "Say the attack involves stolen passwords from a server," he said. "The CISO might say, 'We did a mass password change, and all is safe now.' Seems all well and good, except it's an insufficient step. The adversary may already be changing the passwords along with you, meaning the problem is not contained."

A BOARD ACTION PLAN

It's also key to designate someone on the board as the incident response liaison with the IT team. One reason is "cyber voyeurism," the board's insistence to know everything that is going on, says Morrison. "In our log of reports from incidents we've handled, a board that asks too many questions is distracting, since the demand for information always outpaces the supply."

Hooda is the director entrusted as the cyber risk liaison on the risk management committees of the boards she serves. To prepare for this responsibility, she has

DATA BREACH CHECKLIST

It's happening: A phone call or text comes in the middle of the night, alerting a board director that the company he or she serves was just hit with a massive data breach. What takes place in the next hours and days can mean the difference between a well-managed incident response and a debacle of Equifaxian proportions.

We asked Diligent, a provider of enterprise governance management solutions to boards, for a checklist of what directors need to do next. Here are some solid questions to pocket on the way to the emergency board meeting.

- **Has the Breach Been Sealed?** Find out if the breach has been stopped. In such cases, engage a trusted third-party cybersecurity firm (hopefully it's on speed dial) to conduct a rapid forensic investigation identifying the scope of the breach and all affected parties. The firm can then work with IT security professionals to remedy affected systems.

- **Have We Launched a Response?** Boards need to make sure that the organizations they serve have a lean and ready-to-roll team composed of representatives from legal, risk and compliance, IT/data security, public relations and investor relations in the wings and ready to coordinate the incident response plan. The directors must ensure that the company is well ahead of the unfolding story to communicate accurately and candidly with customers, investors, shareholders and other stakeholders.

- **Are We Coordinating with Law Enforcement and Regulators?** In some jurisdictions, companies have 72 hours to notify regulators that a breach has occurred. Directors must review the incident response plan on a regular basis to make sure ongoing collaborative relationships are in place with regulators and appropriate law enforcement in preparation to notify victims.

- **What do Insurers Say?** Your cyber risk insurance coverage will absorb specific business losses and expenses (some insurers will pay for a forensics investigation, customer notification and crisis management). Contact your insurer immediately following the detection of a breach to incorporate its assistance in the ongoing drama.

2018 CYBER RISK FORUM

YOU'RE NOT ALONE

Thanks to Facebook and Equifax, getting boardrooms focused on cybersecurity isn't hard. Of course, that doesn't mean directors—or most businesspeople—fully comprehend the threats or their responsibilities. At our Cyber Risk Forum in San Francisco, held in partnership with RSA Conference, CISOs from Aetna, Rockwell Automation and Dell, as well as current and former government officials, shared their best tips for directors and CEOs handling cyber risk:

BE REALISTIC. To start, have realistic expectations, said former U.S. Secretary of Homeland Security Michael Chertoff. "If somebody says, 'Oh, I never want to have an intrusion.' That's like going to the doctor and saying, 'Doctor, I never want to be sick for the rest of my life.' It's not realistic, but if you can reduce the severity and the frequency and the consequences, you are then healthy from the cyber standpoint."

KNOW YOUR ROLE. You don't have to be a CIO to play a key part. "Your value as a businessman and businesswoman is your understanding of what is important to the company," Adam Hickey, deputy assistant attorney general for National Asset Protection, told the crowd. "What does it need to survive and to grow and to thrive? Is that information? What information? Where is it stored? You can provide strategic guidance to folks in IT, as well as resources that shape the cybersecurity posture."

STAY STRATEGIC. "In my experience," said John Scimone, senior vice president and chief security officer of Dell, "It's generally more beneficial and meaningful to keep [discussion] at a higher level. You can easily get distracted when you start getting into the technical weeds or whatever's on the front page of the *Times* that morning... instead of looking at a company's structure for technology governance, risk governance, roles and responsibilities, lines of accountability."

USE YOUR GEEK. For CISOs, this is essential. "Every single board has a designated board geek (DBG)," said James Routh, chief security officer at Aetna. "And the designated board geek is the person that all board members turn their heads toward when there's a critical decision around IT. And so, all we have to do is discover who that is and then spend about four times the amount of time with him or her preparing [that person] for whatever we're going to cover because nine times out of 10, when the debate and discussion happens about a particular topic in a board meeting, the DBG is going to weigh in. And if you prep the DBG, then that helps the whole board dynamic and starts to demystify the uncertainty."

TALK IT OUT. Above all else, remember—cybersecurity is still an emerging field, especially compared to, say, finance. "I think it's important that board members and CEOs realize that every CISO meeting that we go to, one of the agenda items is how should you report to your board," said Dawn Cappelli, vice president of global security and chief information security officer of Rockwell Automation. "Nobody can figure that out. So I think we need to have conversations and figure this out."

—Dan Bigman

taken multiple cyber risk training courses and completed the NACD Cyber-Risk Oversight Program, earning the CERT Certificate in Cybersecurity Coverage issued by Carnegie Mellon University. She continues to regularly attend cyber risk courses and conferences. "I've made it my responsibility to keep myself educated," she says.

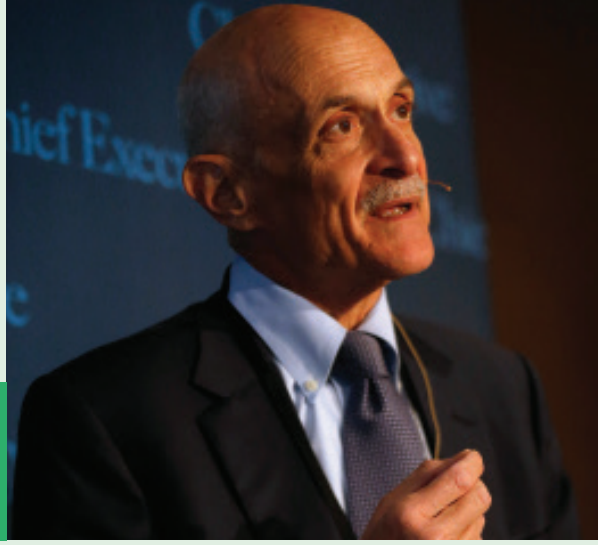
Other directors should do the same, given the grave business risks posed by a major cyber attack. "You need a board director capable of asking the right questions [of the CISO and the IT team]," says Morrison, "but the more important issue is whether or not they have the ability to understand the answers."

Regrettably, boards are only beginning to appreciate this need. Two years ago, Morrison gave a presentation to the board of a manufacturing concern on the potential business impact of a catastrophic cyber attack.

"You need a board director capable of asking the right questions [of the CISO and the IT team], but the more important issue is whether or not they have the ability to understand the answer."

"One of the directors was an older gentleman whose company made sausages, who slammed his fist on the table and said, 'We must invest every dollar we have in a cyber offense, creating an army to attack these guys back,'" he recalled. "The director wanted management to fund an elite attack force to take down hackers. It took some time to get him off the ledge and explain why it wasn't possible."

However, the sausage-maker cannot be faulted for perceiving the threat in



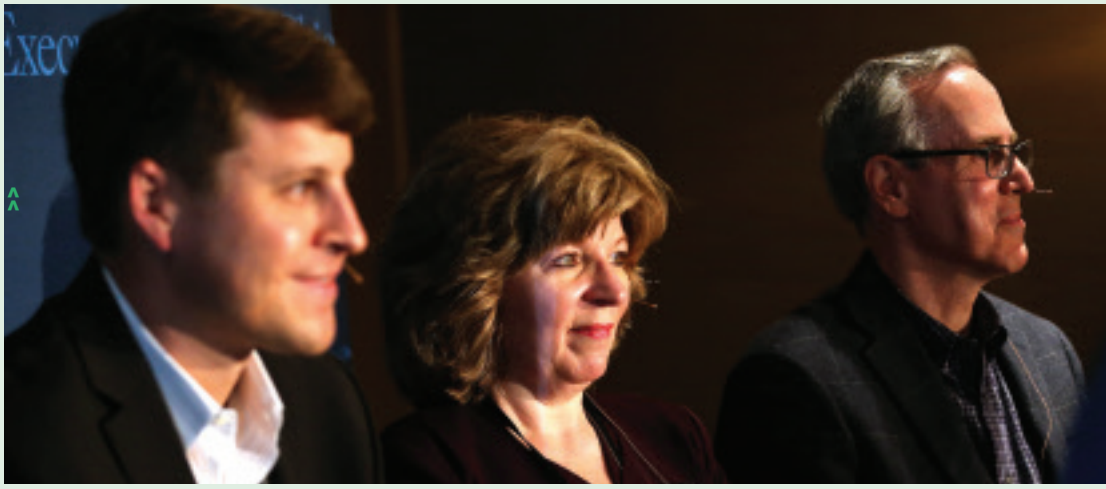
>> Former U.S. Secretary of Homeland Security Michael Chertoff

Key Takeaways

Grant Thornton led forum attendees in a cybersecurity simulation to provide participants with a better understanding of potential impacts of a cyber event and how leaders should engage to ensure that both organizational and customer expectations are met. Key learnings included:

- ✓ How a business decides to address cyber risk awareness and accountability can determine its susceptibility and resiliency for cyber threats
- ✓ Integrate cyber risk planning early in business decisions; it will pay off during periods of crisis
- ✓ Consider how your ability to respond to cyber incidents may be impacted by new technology constructs, such as IoT
- ✓ Set the tone "from the top"—leaders that position cyber risk as a key business risk made more informed decisions to protect their business

BLP members get full access to videos and transcripts of the Cyber Risk Forum: visit BoardLeadershipProgram.com



John Scimone, senior vice president and chief security officer of Dell; Dawn Cappelli, vice president of Global Security and chief iInformation security officer of Rockwell Automation; James Routh, chief security officer at Aetna

war-like terms. In both tabletop and actual incident response simulations, victim companies take action in what they call "war rooms."

FORENSIC FIRE DRILLS

"We'll pretend there is a data breach, running through the different steps of the client company's disaster response plan to evaluate their respective effectiveness," says Schindlinger. "If a particular step falters, we discuss the reasons why and how to mitigate this possibility in future. It's a learning exercise."

These steps include the forensic investigation into the cause and extent of the incident, the notification of affected parties like investors, customers, suppliers and other partners, collaboration with law enforcement and the board's response to media outlets. "Public relations personnel need to brief the board about appropriate messaging, and board members should select a single director to represent them in all media interactions," McGrew advises. "A director who innocently gets the terminology wrong will be roasted on a spit on Twitter. The court of public opinion is harsh."

Morrison has led exercises for clients that simulate actual interactions with members of law enforcement and the media. "We've performed a Wolf Blitzer–like scenario where someone designated as a CNN representative asks the board for live comments," he says. "The director has to know whether to comment or not. We've even simulated an FBI-type investigation, where an FBI agent calls the director out of the blue. In such cases, we rely upon former FBI agents to ask the questions."

Hooda offered one final piece of advice for boards as cyber risks increasingly consume their attention. "Sophisticated companies are realizing the value of using artificial intelligence to gain a clearer picture of their vulnerabilities to both existing and evolving forms of malware," she said. The tools do something that most current approaches cannot: They read the minds of attackers. In the ongoing war on cyber risks, a prescient offense may yet be the best defensive measure. **CBM**

Russ Banham is a Pulitzer-nominated business journalist and author who writes frequently about cyber financial risks and security.