# BOARDS ON CYBER A!ert

Fear of cyberattacks has corporate directors on edge. CIOs must steer the conversation toward managing business risk.

BY STEPHANIE OVERBY

**When Anthem revealed** in early February that hackers had breached a database containing the personal information on 80 million of its customers and employees, the news hit a little too close to home for Gary Scholten, executive vice president and CIO of Principal Financial Group. His first order of business that day was to gather all the information he could to reassure his board of directors that the financial services provider did not have similar vulnerabilities.

He contacted the industry's Financial Services Information Sharing and Analysis Center to get detailed intelligence on the exact nature of what Anthem publicly called a "very sophisticated external cyber attack" and was able to assure his board members that Principal's customer and employee data was not at risk from the type of attack launched against Anthem.

Anthem is one of the nation's largest health insurers. Because of the size of its breach, the industry in which it occurred and the media attention it received, Scholten wanted to get ahead of the questions that Principal's directors might ask. "Cybersecurity is a huge priority for them because the service we provide is so reputation-based," says Scholten. "It's a top-of-mind board issue."

PHOTO BY BILL NELLANS

**Gary Scholten**, CIO of Principal Financial Group, says cybersecurity is a top-of-mind issue for the company's board of directors "because the service we provide is so reputation-based."

Scott Angelo, CIO of K&L Gates, was in Miami for the annual meeting of the law firm's management committee (a private company's version of a board) when the Anthem news hit. "They wake up, and the first thing they want to know about is Anthem," says Gates, who was hired three years ago specifically to strengthen the firm's cybersecurity stance. "They're inundated with all this information that's out there."

The Anthem breach was just the latest in a string of cybersecurity incidents that have occurred over the past couple of years (you know the litany of contretemps: Target, Home Depot, Sony Pictures, JPMorgan Chase and so on). And corporate boards are on high alert. Cybersecurity is "in the press every day," says Peter Gleason, president of the National Association of Corporate Directors (NACD). "It's the foremost issue on directors' minds right now because it's tied into the risk structure of the organization."

Cybersecurity oversight is the second most important topic for boards in 2015—just behind strategic planning—according to law firm Akin Gump Strauss Hauer & Feld. "It's not just financial services firms or regulated companies—everyone is interested now," says Kimberly Peretti, partner and co-chair of the security incident management and response team at law firm Alston & Bird.

In 2014, 42.8 million security incidents were detected, a 48 percent increase over the previous year, according to PricewaterhouseCoopers. The average size of the financial hits attributed to those incidents was $2.7 million, and the number of organizations reporting incident-related losses of more than $20 million increased 92 percent last year, PwC reports. But the true cost may never be known. As many as 71 percent of compromise victims did not detect the breach themselves, according to a 2014 report by cybersecurity firm Trustwave.

Yet board members complain that they're not getting the right information. More than one-third of them are dissatisfied with the quality of information they get regarding cybersecurity risk, and more than half are unhappy with the quantity of information provided, according to a NACD survey of 1,013 public companies.

There's a positive correlation between how much the board is engaged with cybersecurity issues and the strength of IT security profiles, according to a study by business risk consultancy Protiviti. That's why CIOs like Scholten and Angelo are focused on effective communication with their boards. By providing corporate directors with meaningful intelligence on a regular basis, savvy CIOs and CISOs not only educate their boards about the issues they should focus on as they oversee security-related initiatives; they also garner high-level support for building robust security systems and adopting processes and policies necessary to protect corporate data.

## Defining the **THREAT**

Keith Turpin joined Universal Weather and Aviation as CISO last summer to revamp the security program. Historically, cybersecurity had been all but ignored by the board of the international flight planning and support services provider. "My job was to come in and build a strategy to take to the board and get the support that would allow the program to be successful," says Turpin.

Explaining IT security to a nontechnical audience was going to be a challenge. "I've seen people go into board meetings with a network diagram," says Turpin. "You might as well be showing them a crop circle."

So Turpin turned to his background in physical security. He built a small door and fitted it with several seemingly secure locks. He asked the directors in the room if they thought the door was protected. "They looked at me like I was crazy," Turpin recalls. But he explained to them, as he exploited the critical flaw in each of the locking mechanisms in less than a minute, that while the door looked well protected, it was vulnerable. Cybersecurity, he said, was about having the right controls in place to protect the company's data should an IT vulnerability—of which there are thousands—be exploited. He then presented the board with a risk assessment forecast and a security strategy. "[But] the thing they still remember was that door," he says.

"You can't go in there and tell them about the ISO 27000 standard. That's not an effective message," Turpin says. "You have to boil it down to the core business risks for your com-

## **Educating** the Board

### Tips for doing your homework and then teaching the board of directors about the latest security threats

1 Conduct an enterprise risk analysis and create a baseline cybersecurity profile. Focus on what the company's crown jewels are and the steps you are taking to protect them.

2 Enlist reputable third parties to provide the board with an outside assessment of your company's IT risk profile.

3 Make sure that board members understand IT's incident response plan and their role in it.

4 Use standard frameworks to bolster IT's credibility with the board.

5 Involve other executives—particularly the CEO—in your efforts to discuss cybersecurity with the board.

6 Keep abreast of emerging best practices, regulatory expectations and standards.

7 Offer ongoing education and training for board members and executives on key issues and new threats.

8 Ask board members if they think they're getting the kind of information they need to oversee cybersecurity investments. Make adjustments based on their input.
–S.O.

pany: What could have the most significant impact on our revenue stream?" Once the board understands the fundamentals, it's easier to update them on the impact of security investments and address issues as they arise, he explains. After that first meeting, the board quickly approved Turpin's proposed IT security budget; the COO even asked if he needed more money.

> Cybersecurity is **"the foremost issue on directors' minds right now** because it's tied into the risk structure of the organization."
>
> -Peter Gleason, president,
> National Association of Corporate Directors

"Boards need education first and foremost to get them up to speed on the critical issues: What lexicon they should use, where they need to spend money, when they need to buy insurance," says Gleason of the NACD. "They need fulsome reporting to get their hands around it because it's not something they manage every day."

In 2011, K&L Gates chairman and managing partner Peter Kalis worried that the law firm—which has access to the corporate secrets of thousands of companies—could be the weakest link in his clients' cybersecurity frameworks. "He came to the conclusion that we were as big a target as anyone else," says Angelo, whom Kalis hired for his IT security skills.

The first time he stood before the management committee, Angelo delivered his high-level definition of risk: In order to have a risk, you need to have not only a vulnerability but also a threat that corresponds to that vulnerability. "As an organization, you're going to be managing thousands of vulnerabilities every day. But they're passive," says Angelo. "A vulnerability is like a piece of dynamite. You can kick it around. You can throw it. But without a wick and someone to light it, it's not going to go off. I wanted them to focus on what the true threats are."

That's where Angelo's background in intelligence came in. He started thinking about the types of people who might be interested in the data the law firm had access to, how they might try to get it, and how best to protect against their attempted break-ins. "That's an easier pitch. Then you know where to spend your money," says Angelo. "That there is the secret sauce."

To stay on top of potential threats, Angelo digests a steady stream of third-party research on the changing security landscape. "It used to be difficult to get that kind of information, but it's becoming much more readily available," he says.

## The Business of **RISK**

"Cybersecurity is not an IT issue. It's a business issue," says Lloyd Boyd, CIO of Shale-Inland Holdings, an industrial supplier of pipe, valves and fittings. "In our business, we're not dealing with consumer data or health information, but we know that an attack has the potential to impact business operations. And my board wants to know what that risk is and how we're managing it," he says.

But while the board has become aware of the importance of cybersecurity in recent years, directors don't deal with it every day like Boyd does. "They don't know what they need to know," says Boyd. "It's important for us as CIOs to effectively communicate these issues in practical terms. We're going to be a victim at some point, and we need to be prepared."

To garner board support for making the necessary preparations, Boyd applies the "human action model" developed by Austrian economist and philosopher Ludwig von Mises for instigating change: Create uneasiness with the current situation, deliver a clear vision of a better way, and create a safe path forward. "To get the board interested, you have to make it clear why they should be interested," he says.

"Security should be about protecting your current ability to earn and retain revenue, and reducing the risk for new business in the future," says Turpin. "A lot of times, it's seen as a subset of IT, but in reality it's about business risk management."

Gleason agrees. Cybersecurity, he says, "has to be seen by the board as part of the enterprise risk structure the company must address."

At Principal Financial Group, the board knows that incidents are going to happen. "The bottom line is that they want a sense of whether we're taking prudent steps to manage that risk," says Scholten. Is the defense-in-depth approach working? Has monitoring proved effective? Is the company capable of responding to incidents? Scholten doesn't just provide IT's own assessment of Principal's cybersecurity posture; he also brings in third parties to evaluate the state of security.

## Getting Real About **CYBERSECURITY**

Chances are most board members have heard the attention-getting cliché that there are two types of companies: those that have been breached and those that don't yet know they've been breached. "It scares the pants off of them," says Gleason. "But then they're scratching their heads thinking, 'So, all right . . . we're somewhat protected? What does that mean?'"

Scare tactics get old fast. "I don't talk that way to board members. It's a little too Chicken Little," says Boyd of Shale-Inland. "Yes threats are pervasive, and the likelihood of any one company being breached is very high. But there may be things that you flat out don't care about protecting. What's more important is understanding the risk profile of the company. Where are the most critical assets and what are we doing to protect them?"

At Universal Weather and Aviation, Turpin had to break it to his board that it would take awhile to get the company's cybersecurity house in order. "They were like, 'What would it take to do it in half the time?'" he says. Short of fairy dust, he told them, it couldn't be done. "Even if we threw a lot of money at it, there were changes we had to make to the infrastructure and business processes and significant staff training that needed to be done, some of which was very challenging and would take

PHOTO BY ROBERT SEALE

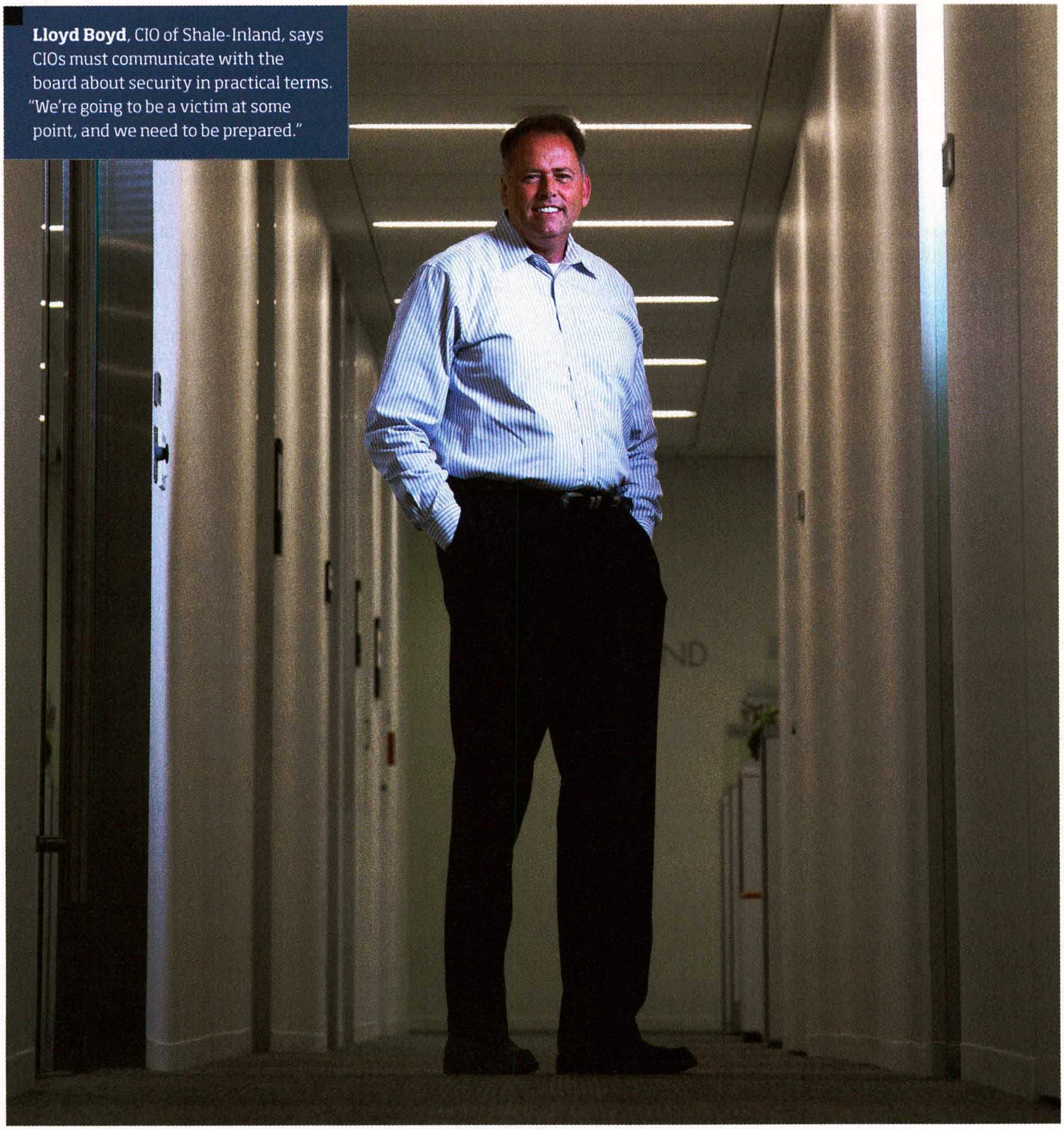
time," he says. "I told them that as we proceeded, I would let them know if there were opportunities to move more quickly. When I walked out of the meeting, I had their full support."

## Going Beyond the HEADLINES

While extensive media coverage of high-profile breaches has spurred board members to care more about IT risk than ever before, a daily diet of such headlines can sow panic. "You would think it would help, but it also hinders," says Boyd. "It can even desensitize the board because they know that the press can sometimes overhype things. They need a fair and balanced perspective of what is real."

Some news has value. "When [a breach] occurs in your industry or meets some threshold that allows you to reinforce the message that what you're doing is good or enables you to make a request that hasn't been approved yet, it might be a good use of the news of the day," says Cal Slemp, managing director and head of the IT security and privacy practice at Protiviti. "But we don't recommend a steady stream of [such news]."

Angelo also worries about overplaying the scary headlines. "If you're going to talk about Anthem or Home Depot or Target, you'd better make sure it's relevant," he says. "I keep that stuff out of my presentations. Everyone can read it on their own, and that's what got us before the board in the first place."



**Lloyd Boyd**, CIO of Shale-Inland, says CIOs must communicate with the board about security in practical terms. "We're going to be a victim at some point, and we need to be prepared."

PHOTO BY ROBERT SEALE

Turpin scoured various reports of security incidents and unearthed an attack outside his industry that illustrated an issue that Universal Weather and Aviation was facing internally. "I found an example that clearly showed something that could happen to us and what the impact would be if it happened," he says. "It was the best example of a worst-case scenario. It was clear to [the board] how devastating it would be to the business." When major vulnerabilities are exposed—a Shellshock vulnerability or a Heartbleed bug—Turpin sends out a companywide message to let everyone know that his office is aware of the issue and has plans in place to handle it.

## Keeping the Board on **BOARD**

If giant banks and government agencies can get hacked, how can the average business protect itself? That's a question Jerry Irvine, CIO of IT services firm Prescient Solutions and a member of the National Cyber Security Partnership, gets a lot. "Everyone would like to get that magic cape to throw over their systems to protect them from the rest of the world," he says.

Irvine doesn't have a magic cape, but he suggests something better. "Give [the board] something to touch and read and understand that shows you are making progress and getting things done," he says. "What the board wants are metrics to keep on top of what's happening." Some key metrics include an inventory of known and authenticated devices and software, vulnerability scans, and the business continuity measures "that would be necessary in case of a security breach or incident," Irvine says.

CIOs and CISOs can partner with board members to figure out what information would be most useful. "What we see work most effectively as boards are pushing into this area is working collaboratively with executives in the organization to work through what's important and settle on series of communications and metrics on governance for cybersecurity," Irvine says.

There are no rules about how often to communicate with the board about IT risk. "You don't want to over alert. But, then again, you don't want to paint too rosy a picture," says Peretti at Alston & Bird. "The goals should be to create meaningful and consistent reporting that establishes credibility and paints an honest and accurate picture."

Boards don't need daily—or even weekly—updates, but they do need to see the big picture. "The board should be focusing on managing risks, not detailed operations," Turpin says. "They need to be informed enough to support strategy."

Most CIOs and CISOs talk directly to the board about cybersecurity every quarter.

"It has to be frequent communication. It can't be once a year. That's not going to give a sense of what's occurring and how well positioned we are," says Scholten. He meets with this board five times a year and also provides a cybersecurity report at each monthly executive team meeting. "Things change so much, it has to be frequent," he explains. "From that report, we can choose what should go on to the board." Scholten also has ongoing interactions with Principal's audit committee, with whom he conducts a "deep dive" into IT risk every year.

Just as important as Scholten's board updates are the active education and awareness programs he conducts. "We're really aggressive with respect to training and keeping people abreast of new trends. Questions from the board become better as result."

Ideally, you should institutionalize a process for providing updates on threats and corporate risk assessments, whether to the audit committee specifically or the board as a whole, says Boyd.

Such updates could be presented via risk scorecards, heat maps, IT security dashboards or some other format, says Gleason. "There are a variety of ways to present it, but the goal is to communicate what the risk looks like holistically, and how it's changed since the last update," he explains.

## Building Trust Amid **UNCERTAINTY**

Since Angelo gave his first cybersecurity presentation to the board in 2011, his interactions with directors have evolved. There were two zero-day exploits in the press in those early days. "It generated a ton of questions. My email would light up," he recalls. He found himself having to schedule meetings with board members and executives to discuss the incidents. "But that was fine," he explains. "Once I was able to explain that it had no impact on our architecture, the issue went away."

Fast-forward to this February's management committee meeting and the huge Anthem breach, and the difference is clear: He no longer gets sidelined by the latest headlines that ultimately have little to do with the state of security risk at K&L Gates. Committee members were certainly aware of the big breach, but they trusted that Angelo was on top of it and didn't interrupt his regular cybersecurity update at the meeting with questions or concerns. "A year ago, it would have dominated the discussion," Angelo says. But this time, he says, "I was able to stick to the facts."

Still, CIOs must have a realistic message because of the ever-evolving threats. "One thing I always close with—and they're probably tired of hearing me say this—is 'Things can change overnight.' You can go to bed feeling secure and wake up to an exploit that we're vulnerable to," Angelo says. "The bad guy only has to be right [once]. We have to be right all the time." The committee understands that, but members are confident in the company's security posture because of the transparent way he discusses security strategy with them.

"There is a growing persistent threat. Whether it's from state-sponsored attacks or organized crime, there are so many easy ways to monetize data to make it a profitable venture," says Boyd. "At the same time, the sky is not falling. We don't have major issues every day. The threat is more sophisticated, but so are our protection mechanisms."

Boyd says his regular communication with the Shale-Inland board makes that clear. "It works very well. And it's a mature way to present the issues and enable the board to become a partner in guiding what we want to do," he says. "Every IT person would like to say, 'Just trust me to put in place what we need.' We can't do it all, and we can't do it fast enough. We don't want to create a false sense of security." CIO

Stephanie Overby is a freelance writer based in Massachusetts.