For personal, non-commercial use only. Do not edit, alter or reproduce. For commercial reproduction or distribution, contact Dow Jones Reprints & Licensing at (800) 843-0008 or www.djreprints.com

ANDY DAVIS FOR THE WALL STREET JOURNAL (5)

Pete Chronis

Myrna Soto

What Is the Board's Role?

Pete Chronis and Myrna Soto discuss what directors need to do—both when an incident occurs but also in preparation for one

Cybersecurity is a business risk and therefore a board issue, experts say. But cybersecurity oversight can be a challenge for directors, many of whom may not fully understand the issue.

Pete Chronis, chief information security officer at Time Warner's Turner division, and Myrna Soto, the global chief information security officer at Comcast Corp., sat down with Wall Street Journal Business Editor Jamie Heller to discuss the board's role in cybersecurity. Edited excerpts follow.

Should you pay?

MS. HELLER: *Let's say there was a hack on a hypothetical company, and some 57 million accounts were compromised. Someone had the idea to pay $100,000 to make it go away, and it did. That sounds like the deal of the century. What's wrong with that picture?*

MS. SOTO: There are a number of things that are concerning. One is when you think about ransom and you think about extortion, that's what it is. You really have to ask yourself as an organization whether you want to put yourself in the position to pay.

First, are you guaranteed that you're going to get the results that are being promised to you? Second, it sounds like that was a very cheap price for something extremely valuable, so you have to wonder about the too-good-to-be-true scenario. We could probably talk about that topic for hours. But I think it's a big conundrum that many organizations are facing, what to do in a ransom situation. I currently sit on a board, and we've talked about what our crisis-management stance would be. We are electing to say that we would have to review each condition, of course, but the likelihood would be not to pay.

MS. HELLER: *Because?*

MS. SOTO: First, in some instances it's illegal because you are participating in an unlawful activity of extortion of sorts. Second, you aren't really guaranteed that you're going to [get the outcome you want]. And the risks may be just too great.

MS. HELLER: *Pete, what do you think?*

MR. CHRONIS: I echo Myrna's advice. You're dealing with a criminal, and your senior executive leaders, your board, hopefully they aren't used to dealing with people of that ilk.

The big story in this scenario isn't necessarily the ransom. but the choice not to disclose. If you had to go in front of the press, or the public, or your employees, or your customers and say, "Don't worry. The criminal told us they don't have your data anymore," you're going to get a lot of bad press. You'll get a lot of angry customers and a lot of angry employees. So you really have to consider disclosure as a part of your response strategy.

And if you have a chief information security officer reporting to the board, it's important to make sure that he or she has a relationship with those board members so that there can be a free flow of communication and ideas outside of crisis situations.

That way, when the proverbial manure hits the fan, you can have good, constructive conversations and have context around those conversations.

MS. HELLER: *How do you encourage that kind of access?*

MR. CHRONIS: You need an enlightened board that's interested. You need senior leaders who are emotionally mature. You need the right chief information security officer.

MS. SOTO: I couldn't agree more. I think it's extremely important that chief information security officers have a direct line to the board. Being able to communicate status, your opinion of the risk of the organization and being able to have somewhat of an unfiltered conversation with the board and be open to answering questions about readiness, such as, "Are we investing in the right areas? Do we have all the resources that we need?"

The directors' role

MS. HELLER: *How much of a decision-making role should the board play?*

MR. CHRONIS: The role of the board starts way beyond a security incident. Boards are there to make sure that the company has the right strategic plan. Boards need to be prepared to ask chief information security officers and senior leaders questions such as: How good are we at assessing and addressing risk, protecting our assets? How good are we at detecting incidents and containing them? And then how good are we on the compliance side? Do we have any compliance gaps? How good are we at closing those?

That helps promote an open and honest conversation, so that if you have a security incident, they have some context about how it might have happened and what you are planning to do to address it.

MS. SOTO: It is somewhat of a slippery slope because the role of the board isn't to manage the company. The role of the board is to set guidance, provide direction, serve as a governance function over the company but not necessarily manage it.

But the reality is, it comes down to materiality. Are you talking about an event that could be brand tarnishing above and beyond the isolated incident? That is where directors have a fiduciary responsibility to speak their voice and provide guidance.

AUDIENCE MEMBER: *How do you discuss with your boards the strategic aspects of what you and your organizations do and the investments you're looking to make?*

MR. CHRONIS: Boards struggle today with how to provide oversight for cybersecurity because they don't feel like experts. My advice to them is to ask open-ended questions. "Do you have everything you need? If you had X number of extra dollars, how would you spend that? And how does that relate back to the business we operate in?"

Then you start to understand whether you have gaps in your program in terms of funding and if the chief information security officer is struggling. Then that becomes a broader conversation with the CFO and CEO. "Are we funding the programs enough?" If boards were asking those fundamental questions, we wouldn't have a lot of the issues we have today.

NICHOLAS ELLIOTT: *Should every board have a cyber specialist, as some governance experts propose?*

MS. SOTO: I don't think that every board needs a cyber expert. I do believe that every board needs a technology leader. It could be a CIO, a chief information security officer, someone with a broad breadth of experience in tech.

For personal, non-commercial use only.

Why We Have to Really Worry About the Banks

George Kurtz, Elena Kvochko and Joe Leonard on the cyberrisks to financial institutions. What's the worst-case scenario?

George Kurtz

Elena Kvochko

Joe Leonard

Financial institutions are prime targets for cyberattacks. How big are the risks, and how can these companies, or any company, best confront the threat?

*The Wall Street Journal's Rachel Ensign discussed these issues with George Kurtz, cofounder and chief executive of cybersecurity firm **CrowdStrike**; Elena Kvochko, chief information officer, Group Security Division, at Barclays; and Joe Leonard, senior vice president for technology and chief information security officer for the Federal Reserve Bank of New York. Edited excerpts of their conversation follow.*

Losing Sleep

MS. ENSIGN: *When bank CEOs are asked, "What's your biggest fear?" they often simply say, "Cybersecurity." What's really the worst-case scenario here?*

MR. KURTZ: If you look over just the last couple of years you've seen a rise in either destructive malware or ransomware that could cripple an organization. Over the last six months attacks have cost literally tens of millions of dollars and a massive loss of confidence by customers.

It's no longer, "My PC's going to be infected and I've got to go clean it up." It's, "My whole company can be taken offline." Combine that with enterprise ransomware. It isn't just, "Hey, we have one computer that is infected for 300 bucks." At some point people are getting phone calls, now or in the future. It's like, "Hey, you've got four hours to wire 10 million bucks."

MS. ENSIGN: *If a bank shuts down, does it lead to a run on the banking system?*

MR. KURTZ: When you can't trade, when you are under attack, there is a loss of confidence in that particular institution. Some of these institutions, if they're out of business or they're not operational, it's a massive ripple.

MR. LEONARD: You have counterparties trading. So you've got two situations where you've got an individual that might be taken offline out of that ecosystem. Or you get a situation where there are concerns about an entity, and do you have other people withdrawing voluntarily?

So the contingent there is not always necessarily the actual threat. It's what happens to the financial transactions. Do people pull back? Does it slow everything down? Does cyber become the impetus for a financial crisis?

MS. ENSIGN: *How likely do you think it is that there is a cyber-driven financial crisis in the next 10 years?*

MR. LEONARD: There are a lot of good private-sector initiatives, there are a lot of public-sector initiatives recognizing this. Something will happen, without question. The question is how big is it going to be, how bad is it going to be, or have we put the right processes in place to sort of contain it and manage it.

A holistic approach

MS. ENSIGN: *What do companies have to do to make cyber an important part of the business that is not siloed off from other places?*

MS. KVOCHKO: No matter how you structure your technology teams, what's important is to be able to have a holistic perspective across your business lines and product lines, to be able to see there is an anomaly or an incident happening in one part of the organization, you're able to connect it to potentially other related events that are happening.

The other advice is that you really have to focus on driving the security culture within your organization. And when you do so, you have to remember that it isn't easy. Studies show that it takes between three months to a year for a certain process to become a habit.

So when you think about establishing a culture, you have to account for that time that it takes for people to learn new ways of doing things, and you have to establish kind of quick wins in between.

MS. ENSIGN: *Joe, can you share any advice on how to respond to a breach?*

MR. LEONARD: Having that playbook of communications prepared. Because what you'll find in many breaches is what comes out in the beginning turns out not to be accurate or doesn't have all the information or it isn't the full story.

So you've got to be clear and crisp in that messaging when you come out. Make sure it's the message that you want to land in our Twitter, YouTube culture. I can't stress that enough. The preparation side of things is very important.

Selling it

AUDIENCE MEMBER: *Security in general is very expensive. How do you target your message in such a way that you get the money that you need to implement everything that is needed?*

MR. LEONARD: One way to approach that is not to sell it as a technology solution. We're really looking at protecting a business process and profit that is at risk, or a potential cost that is there. Then you could say, "Well, to mitigate that, here are some things we can do." I think that tends to be a more successful conversation than, "Hey, there is a threat out there and we need to spend X dollars on this technology."

MS. KVOCHKO: In addition to the messaging, you can implement security by design or implement security from the beginning. Whenever you're thinking of creating a new product or collecting requirements for that product, also collect requirements for security. Whenever you're thinking about testing the product, also test for the potential vulnerabilities. And when you roll out your product, educate the users on how to use it securely. That would potentially drive the costs down, as opposed to trying to mitigate potential breaches or consequences.

Chertoff

Continued from page R1

2016, the influence campaign on the U.S. election. Was that a cyberattack?

MR. CHERTOFF: This is a very hot area, and we're going to have to be careful about it. If you go to Russia and meet with Russian cyberpeople, they love the idea that we talk about information operations as cyberattacks. Only because their version of cybersecurity is, let's get rid of all the content that we don't like, starting with CNN and The Wall Street Journal. And that's cybersecurity. We obviously as a free society don't equate that with cybersecurity.

Cybersecurity to me means protecting against people who are coming in to manipulate your system, steal your data, destroy your data, corrupt your data. But ideas that we don't like aren't cyberattacks. They're dealt with the way we deal with any speech that we disagree with.

We counteract it with the facts. We make contrary arguments. Maybe we expose the true identity of the person who was purveying the information. It is important to separate information operations from a classic cyberattack, which isn't designed to persuade. It is designed to directly disrupt or destroy.

Possible threats

MR. MCMILLAN: *Is there something on the horizon that keeps you guys up at night?*

MR. CHERTOFF: One would be a significant, destructive attack against critical infrastructure. That would probably be an act of war. Right now, the major players tend to not want to go there. But you look at a country like North Korea, and they seem to operate under a different risk paradigm. The other issue I worry about is fragmentation, everybody pulling the internet into their own borders. There's always been a tension between a borderless internet and state sovereignty. The Chinese are moving somewhat in that direction. It wouldn't result in the loss of human life, but it would deprive us of what is a very significant economic resource.

Schmidt

Continued from page R1

should companies be doing more of to combat this threat?

MR. SMITH: Good cyberhygiene is a must. We're still seeing the majority of compromises are based upon unpatched areas, where vulnerabilities were identified five, 10 years ago.

Something as basic as multifactor authentication, which starts to harden your access points, is one step. Then there is the need for more information sharing and collaboration. As I hear quite often, private industry wants more information from us. They want it faster, and they want more classified data.

I don't know that we'll ever get to a point where [private companies and the government] are completely comfortable exchanging all that information. But quite honestly, I believe that private industry has to come up with the solution to get us to information sharing at machine speed. Because the federal government right now isn't quite agile enough to do that.

Actionable intelligence

MR. DEAN: *Steve, what do you think is the biggest need for enhancement in the area of cooperation?*

MR. SCHMIDT: Scott hit it. Information sharing is all about speed. What we're looking for is actionable intelligence, which is sufficiently specific to allow us to take protective actions that are unique to the threat that we're facing in the time frame the threat is taking place.

Telling us three weeks after something happened, "Hey, a bad thing occurred," isn't especially useful. But when you say, "This tool was just released by this particular group, and they focus on these kinds of customers with it, and we see an uptick in that kind of activity"—that becomes actionable. I can start looking for that signature. I can look for that particular activity and say, "All right, it's targeting this particular part of our organization or our customer base."