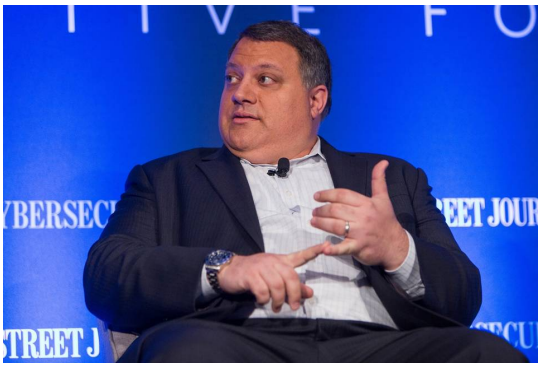
JOURNAL REPORTS: CONFERENCES

The Corporate Board's Role When It Comes to Cybersecurity

Turner Broadcasting's Pete Chronis and Comcast's Myrna Soto on why cybersecurity oversight remains a challenge for directors



PETE CHRONIS | 'The role of the board starts way beyond a security incident.' PHOTO: ANDY DAVIS FOR THE WALL STREET JOURNAL

Dec. 18, 2017 10:09 p.m. ET

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.

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.

MYRNA SOTO | 'I do believe that every board needs a technology leader.' PHOTO: ANDY DAVIS FOR THE WALL STREET JOURNAL

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

JOURNAL REPORT

- Read more at WSJ Conferences

MORE IN CYBERSECURITY

- How to Fight the Threat From Nation-States
- What Companies Should Be Most Concerned About
- The Risk to the Financial System
- What Happened When Verizon Learned of the Yahoo Breach

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.

Write to reports@wsj.com

Appeared in the December 19, 2017, print edition as 'What Is the Board's Role?.'

- **College Rankings**
- **College Rankings Highlights**
- **Conferences**
- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Tech Companies to Watch**
- **Wealth Management**