Canadian HR Reporter
THE NATIONAL JOURNAL OF HUMAN RESOURCE MANAGEMENT www.hrreporter.com

REPRINT
© Copyright Thomson Reuters Canada Ltd.
Reprint was created with permission on
September 4, 2018 from the September 2018 issue.

# Boards of directors play important role maintaining cyber resilience: Survey

*Cross-organizational training, HR also key components of proper strategy*

BY JOHN DUJAY

**BOARDS** of directors can provide significant aid in helping organizations become more cyber resilient, according to a global survey.

"It's important for companies to understand that achieving cyber resiliency is a company-wide imperative, one that shouldn't be sequestered to certain roles or functions," said Anthony Agostino, global head of cyber risk at Willis Towers Watson in New York, which sponsored the survey.

"Boards should emphasize the need for a strategic framework, and the C-suite should set the tone within their organizations by empowering stakeholders, such as IT, risk, HR, legal and compliance, to drive an integrated risk management and resiliency strategy."

It's critically important — in the past year, about one-third of the organizations experienced a "serious cyber incident" that disrupted operations, found the survey of 452 board members, including 50 in Canada and 100 in the United States, by the Economist Intelligence Unit (EIU). However, only 13 per cent rated themselves as "well above average" in terms of learning from these types of incidents.

## What is cyber resilience?

Most large companies already have extensive cybersecurity in place, but it's the ability to bounce back and continue regular operations that makes all the difference, according to Rachael Bryson, senior research associate in national security and public safety at the Conference Board of Canada in Ottawa, which published the study *Building Cyber Resilience* in July.

"It's an organization's ability to limit the impact of cyber disruption, maintain critical functions and rapidly re-establish normal operations, following cyber incidents," she said.

"There are critical functions that must be maintained. And the difference between just kind of surviving some sort of a cyber incident, and then being able to actually return the business operations, and possibly learn from it and become better, is rapidly re-establishing normal operations; there seems to be a strong correlation between the speed with which normalcy is achieved and the actual success in coming out of the cyber incident."

"The acknowledgement that something could happen because hackers are actively targeting you is merged over to this awareness that everybody has a certain amount of vulnerability because we cannot know all of the system flaws out there until they're exposed in one way or another," said Bryson.

But while a lot more companies are aware of the need for strong resilience, "not everybody is doing it and not everyone understands exactly how you can go about starting," she said.

While awareness could be better, recent events profiled in the media are making a difference, said Rahul Bhardwaj, president and CEO of the Institute of Corporate Directors (ICD) in Toronto.

"Cybersecurity risk has become prominent in the minds of directors more than ever before," he said. "Incidents such as the Cambridge Analytica and Equifax security breaches helped to increase awareness."

In April, an ICD survey found 42 per cent of respondents identified cyber risk or security of information as their number-one concern — double the number who cited changing regulations and disruptive technology, and triple the number who cited global economic instability as their number-one concern.

## The right questions

In executing a cyber-resilience strategy, it behooves boards of directors to not remain high above the fray, but rather ask tough questions of the C-suite, according to Patricia Kosseim, counsel in privacy and data management at Osler in Ottawa.

"A question for the board that is important to ask is 'What level of resources does the organization dedicate to technical security, the physical hardware and software?' But also, it's important for the board to make sure that it asks questions about whether or not management feels it has the necessary technical skills or capacity to deal with the evolving cybersecurity landscape," she said.

"By asking the right questions, a board can certainly help to properly assess the level of risk, they can relativize corporate priorities, they can greatly influence the level and direction of investment. And, from my own experience on boards, they can certainly trigger a whole chain of activity needed to strengthen an organization's cybersecurity posture," said Kosseim.

But before board members can ask those questions, they should know exactly what they are talking about, according to a consultant who educates boards of directors.

"The first thing they should do is actually get educated because if they're not educated about what it means, they will be asking questions that will be counterproductive to the organization's ability to deliver results," said Nadya Bartol, associate director at BCG Platinion North America in Washington.

"Something we find very effective is an educational simulation or tabletop exercise, where we put a board through a series of situations where they role play and discuss any security challenges that come at them, or put them into situations as a board member," she said.

"And it achieves dynamic learning, instead of just saying, 'Here's a PowerPoint presentation.'"

The risk to companies from cyber incidents can be so profound that board members should proactively educate themselves in "understanding the level of risk, because they also have to actively inquire into the mitigation strategy and measures that the organization has in place to be able to assess the residual risk that the organization faces," said Kosseim.

"It's one thing to understand the external risks, but with the right mitigation strategies in place, the level of residual risk is really what is operative in terms of decision-making at the board level," she said.

"The first part of the board's responsibility is to insist on being properly educated about the business and having access to the information it needs to discharge its oversight responsibility."

As well, providing the leadership to help companies move on after a serious incident is one of the most crucial roles for a board, said Kosseim.

"And, most importantly of all, the board can drive organizational culture towards greater awareness and protection."

## Who's responsible?

What is clear, according to Bryson, is not just one department in the organization is responsible to foster cyber resilience.

"The big difference really tends to be in ownership and responsibility," she said. "Whereas cybersecurity can be owned by one department, or we tend to see a very delineated centre responsibility, cyber resilience really stretches across the whole organization and brings together key functions to ensure business continuity."

"That's more than just IT or your security department writ large," said Bryson. "Wherever an organization kind of slots into cybersecurity, it's a much bigger role."

Companies would do well to spread out the responsibility in an effort to boost cyber resilience, said Kosseim.

"A typical and flawed assumption is that it rests entirely on the shoulders of the chief information security officer (CISO)," she said.

"But, in fact, a healthy governance structure will promote a shared responsibility between the CISO… and the chief privacy officer. And in some organizations that have really put some thought into this, both those senior positions may co-chair a cross-functional team that draws on communication, on finance, on audit, and particularly on HR."

"More and more is the recognition that a healthy governance process for dealing and addressing a cybersecurity threat is one that positions itself horizontally across the organization but is headed up by both the privacy and security heads."

And by properly discharging the traditional role of governance, boards can facilitate a better method of sharing information throughout the organization, said Kosseim.

"Another is to ensure that there's the appropriate governance process in place in the organization to elevate regular reporting on cybersecurity to the board. That can be either directly to the full board or, more typically, it could be to one of its standing committees," she said. "Its audit committee, for instance, is particularly well-suited to receive reports from management on cybersecurity."

"A board should probably be asking senior management about where cybersecurity responsibilities sit within the organization."

## Role of HR

Rolling out the organization's overall cyber strategy is a key component for HR, particularly in influencing behaviour and ensuring a strong and positive work culture, according to Bhardwaj.

"For effective management on security-related issues, all employees need to understand this to be a priority," he said.

"No one wants to believe that security was breached based on an action that he or she unknowingly performed. Understanding this potential risk at the individual level is a behavioural change that is within the purview of the HR department."

"By being a part of the management process, HR then becomes a strategic partner for the IT/CISO teams in relation to cybersecurity and the organization," said Bhardwaj.

Post-incident, HR holds "a lot of policies around return to work; they'll hold a lot of information about how to contact employees in case of emergency. They would be an important part of that kind of crisis playbook," according to Bryson.

"By spreading information, spreading awareness, training, ongoing training, cybersecurity, all kinds of different training against insider threats, against phishing, against whatever kind of issues facing your organization, HR should be an important part of ensuring that that is rolled into professional development and learning plans," she said.

"As members of that crisis playbook, they'd be invaluable in terms of communication, in terms of normalcy, in terms of training people to work."

Many companies are still not putting in place "seemingly basic cyber-related HR policies, such as ongoing security awareness training, identification of at-risk employees and internal communications after a security incident," according to the Willis Towers Watson/EIU report.

Only 44 per cent of organizations reported they participated in ongoing security awareness training or were able to identify talent deficits in their IT departments.

Once management of the risks has been put in place, a best practice is for companies to undertake exercises that best illustrate weak points in the overall strategy, said Bryson.

"This risk tolerance and mapping exercise is step one, and that has to be undertaken by the board," she said.

"Then, really, (it's about) putting the finances and the resources behind a project like this."