Every port is a storm

listedmag.com/2016/12/every-port-is-a-storm/

These days, whenever a well-known public company suffers a major data breach, bulletins and news alerts circulate quickly among most boards and the governance community. But in October, when a botnet army of hijacked network-connected surveillance cameras, Wi-Fi routers and computers were simultaneously mobilized to carry out a sophisticated distributed denial of service attack that shut down access to sites like Amazon, *The New York Times* and Twitter in much of the U.S., how many directors got similar reports?

If you're answering, "Not me," consider yourself warned. By now, the October attack—directed at networks operated by domain services provider Dyn Inc.—should be on every board's radar. More than any cybersecurity incident before, this one highlighted the massive security risks posed by the exploding proliferation of internet-connected devices, better known as the Internet of Things (IoT).

An EY report, published in 2015, stated the problem plainly: securing the enterprise "will become exponentially more difficult as IoT connects more devices, software, machines, and humans." The time to act is now, as more than half of Canadian companies have already implemented some form of "connected-device solution" according to IDC Canada research. Ranging from things like fleet telematics to the digital oilfield to advanced automation (the so-called fourth industrial revolution), IoT is quickly becoming ubiquitous. To give a sense of the scale, the McKinsey Global Institute forecasts an increase in IoT devices worldwide from 4 billion today to 25 billion by 2020, and puts the economic impact of connected devices at up to US$11.1 trillion by 2025.

That growth in promise also means a rise in exposure.

"The problem with IoT is that there are increasingly more numerous devices attached to the internet being used both inside and outside of the workplace, and many of them are not properly password-protected or capable of being secured," says Andrea Bonime-Blanc, chief executive officer of GEC Risk Advisory in New York.

Indeed, at least one manufacturer of the cameras that bombarded Dyn's networks with malicious requests did not require owners to change the device's factory-default password, offering a layup to hackers who create open source malware to scour the internet for devices with these defaults.

"With the proliferation of IoT devices for enterprise use, companies face two threats," says Dale Drew, chief security officer of U.S.-based internet service provider Level 3 Communications. "First, these devices can be a point of entry for a bad actor. If the devices are not properly configured or monitored, a malicious actor can enter the company through an open port. Second, the devices may be compromised and used for nefarious deeds without the knowledge of the owner. They could be part of a botnet ring."

For consumer-facing companies with connected products, risks exist that make data theft seem mild in comparison. Among the most infamous and dramatic demonstrations of IoT vulnerability was last year's Jeep Cherokee hack, in which two security researchers wirelessly hacked into the vehicle through its entertainment system, gaining control of the steering, brakes and transmission while the vehicle was in motion. The subsequent recall of 1.4 million vehicles by Fiat Chrysler to install a security patch was no doubt a good bargain compared to the alternative: a sudden hijacking on a driver's commute by a hacker who had found the vulnerability first.

For companies adopting IoT solutions, the question is not if, but when, their connected devices will be attacked, no matter how low their profile. This was recently demonstrated in an experiment run by an editor at *The Atlantic*, who disguised a rented server as an unsecured connected toaster to see how long it would take for hackers to attack it. The first attempt came within 45 minutes. The moral: relying on security by obscurity is a mistake management doesn't want to make.

While no one is expecting directors to start running penetration tests or get down into the IT muck, asking questions relating to IoT security and oversight must become part of boardroom conversations. This attention has an impact. According an AT&T report, "the level of board involvement matters, in part, because it impacts the confidence level that a company's decision-makers have in the security of their organization's connected devices. Specifically, there was a 300% increase in the number of organizations showing full confidence in the security of their connected devices when their board was highly involved."

This confidence starts with asking the right questions when introducing connected devices, some of which may sit outside your company's physical domain. The first question: Is there one body overseeing the entire network, of which connected devices are now a part? Bonime-Blanc explained by e-mail: "The most important thing any company (or other type of organization) should do to protect against cyber-threats is to form a management-level committee (preferably chaired by the CEO) that undertakes a focused interdisciplinary review of the type of cyber-governance and management approach that is required for their specific organization."

Richard Wilson, partner of cybersecurity and privacy consulting at PWC in Toronto and coauthor of the firm's "Board Cybersecurity Governance Framework," suggests "it could be a steering committee that's made up of people from IT and operational technology, and if they're market-facing, then consumer technology."

AT LEAST, THAT'S the ideal. Unfortunately, at this stage, interdisciplinary awareness of IoT risk in Canada's C-suites and boardrooms is not very widespread. Instead, oversight still appears to be siloed.

"Our research shows that the majority of IoT-related initiatives are driven by a line-of-business manager or executive," says Nigel Wallis, IDC Canada's vice-president for Internet of Things and Industry Research. That means when it comes to implementing IoT, the IT department isn't there at the beginning talking about security controls. "If you think about the Fiat Chrysler example," Wallis says, "the IT department had nothing to do with that [entertainment system vulnerability]. That was a product-design-engineering-R&D decision."

It behoves senior executives and even directors, then, to see their organizations the way hackers do: as one network, one set of interconnected activities for which any entrance will do. Once they get in and start gathering credentials, they can move laterally across a company's network toward the crown jewels, whether that be customer data or operational control of the physical environment. The role of a steering committee would be to ensure that security is not an afterthought but baked into every process, product and service from the start.

"The IoT question would be, 'Have we used the same protocols, the same level of defence protocols in our IoT environment as we have in our IT environment?'" says Wilson. "For instance, you'd never be allowed to use typically a default password for one of your most important centralized servers. If an IoT device is another potential point of entry, why would we allow it to have a more relaxed protocol?"

IDC's Wallis says that boards should also ask whether cybersecurity guidelines such as the NIST cybersecurity framework, the U.S. government's FedRAMP, and ISO standards are being adhered to when connecting devices.

Ensuring a security mindset permeates the culture is necessary, but not sufficient, for protection. Wilson says that boards also need to start talking with management about so-called "depth in defence," the layering of security controls so that compromise in one area can be contained, ensuring the lateral movement across the network doesn't happen. "We have to assume that various protection points are going to fail, and so what we're looking for are the failsafes, the fall-backs, the redundancy, the multiple layers at the perimeter, on the interior, and ultimately with incident response if they manage to get to that level of success," Wilson says.

Part of that incident response, Wilson explains, is having an explicit cyberattack response plan that considers scenarios involving connected devices that sit both inside and outside your organization’s physical domain. What happens if a device in the field is physically tampered with? What happens if your devices have been co-opted to engage in a DDoS attack? What if operational control of manufacturing or IT equipment has been compromised?

Even if these conversations are happening, management can’t expect to secure the organization if the security team is stretched thin, Wilson says. Directors need to ensure management has assigned the adequate resources to lower the security risk to a level that meets their expectations.

As the wave of IoT adoption builds, enthusiasm about the possibilities must be balanced with respect for consequences and concern for security. “[The enterprise] need[s] to be hyper aware of what it connects to its network and how it is handling the security,” Drew of Level 3 says. “Until IoT vendors are forced to build security into [their] products, it will be incumbent on the owners to take all necessary precautions.”

Photography: Shutterstock