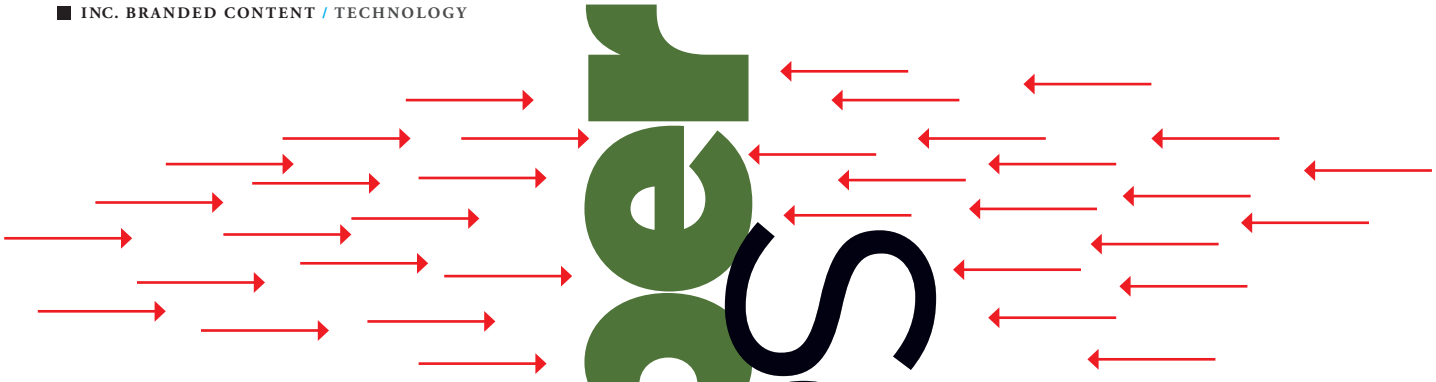

cybersecurity

IS A SHARED RESPONSIBILITY AT THE C-LEVEL

Data breaches can have far-reaching repercussions; protecting against them is a companywide mandate

Attacks by what the cybersecurity industry refers to as "bad actors" have become an everyday issue for companies doing business in the internet age. A 2015 survey of risk managers by Hartford Steam Boiler Inspection and Insurance Company found that nearly 7 in 10 experienced at least one hacking incident over the preceding year. And as the Internet of Things (IoT) creates more potential points of compromise, cyberattacks are on the rise.

"Cyberattacks are pervasive. They do not differentiate between large, medium, and small companies," says Bhavani Thuraisingham, executive director of the Cyber Security Research and Education Institute at the University of Texas at Dallas. Any business that has sensitive information or intellectual property to protect needs to have cybersecurity expertise either in house or through a reliable and reputable third-party provider, she adds.

The evolving cybersecurity landscape also creates new responsibilities for company boards of directors and chief financial officers. "The entire executive staff of an organization must, at the very least, have awareness of this topic and an understanding of how information is being filtered and transported, both internally and externally, and the practices that have been put in place to protect it," says Jeff Ishmael, chief financial officer at Cylance, the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity.

Cylance provides a proactive solution to cybersecurity threats, combining sophisticated math and machine learning with a unique understanding of a hacker's mentality in order to quickly identify what is safe and what is a threat. Rather than simply creating blacklists and whitelists, as most traditional cybersecurity products do, Cylance proactively filters any piece of software that tries to run on a computer, instantly identifying malware and quarantining or killing it. The process takes just milliseconds, uses almost no CPU capacity, and is invisible to end users.

For businesses that have a board of directors, Ishmael recommends adding a member with cybersecurity expertise to strengthen the organization in this area. Boards now have a responsibility to be aware of what cybersecurity measures are in place, how often they are checked and audited, and whether there have been any material or non-financial breaches. In addition, they need to consider any industry-specific cybersecurity issues that might apply, such as HIPAA in the health care space or the myriad regulations governing the financial services industry.

CFOs, too, must now factor cybersecurity into their decision-making processes, Ishmael says. "CFOs have an absolute fiduciary duty around any element of risk with the potential to impact the bottom line, the well-being of employees, or unplanned spend. Those and many other areas are potentially subject to cybersecurity risks."

CFOs need to broaden the approach they take when evaluating cybersecurity spend, Ishmael adds, since the level of risk related to a breach event can be far-reaching, negatively affecting a company's sales earnings, even its ability to conduct business for an extended period of time. "The cost of any action a business might take to proactively prevent such a breach from occurring must be evaluated in light of the much greater costs that could result from failing to take that action," he stresses. "CISOs (chief information security officers) and CTOs (chief technology officers) face job-loss risk tied to breaches; CFOs may soon join them. 'Not my job' is no longer an acceptable response for any executive when it comes to cybersecurity. It's now everyone's job." ■

ARE THE SMARTEST CITIES THE MOST VULNERABLE TO ATTACK?

Smart cities need to become intelligent cities with proactive cybersecurity solutions. Cylance is revolutionizing cybersecurity with artificial intelligence and machine learning—for advanced threat prevention on the endpoint—wherever the endpoint may be. Learn more at cylance.com

CYLANCE™

Silence the Threat