Opinion

The Dangerous Disconnect Between IT and Company Leadership

June 4, 2018

New SEC guidance on cyber security is notable for two reasons: First, it underscores the financial impact a successful cyber breach can have on an organization. This includes fixing the intrusion, lost operational revenue, stolen intellectual property, damaged relationships with customers and vendors, and even a reduced stock price. But perhaps more importantly, the SEC has essentially put leaders of publicly traded companies on notice that cyber security must become a strategic priority for their organizations.

Despite a steady stream of global headlines documenting how the cyber threat is growing more sophisticated and aggressive, it still appears that too many boards of directors and senior-level executives aren’t taking the threat seriously. In fact, 66% of respondents believe their organization will suffer a major cyber attack that would seriously diminish shareholder value. Yet 68% had not been asked by their boards of directors for a cyber-security briefing in the past year, according to a survey sponsored by Raytheon Company and conducted by the Ponemon Institute.

The 2018 Study on Global Megatrends in Cybersecurity gathered insights from more than 1,100 senior-level IT security professionals from the United States, United Kingdom, Europe and the Middle East and North Africa region. The respondents work for organizations large and small, in the public and private sectors, and across a spectrum of industries, including finance, industrial, health and pharmaceuticals, energy, services, technology and software.

The survey’s findings underscore the growing cost of cyber crime, which is now estimated to be worth $600 billion. Despite this knowledge, there remains a sizable strategic misalignment between
IT experts and their leadership team. Just 36% of respondents believe that cyber security is a strategic priority for their organization, with only 46% believing their organization’s cyber-security posture is going to improve in the coming years.

The cyber threat is not going away any time soon, and every new cyber attack seems to eclipse the one before it. Last May, the WannaCry ransomware attack took medical records hostage in busy U.K. hospitals, caused production shutdowns at automobile factories in France and infiltrated the Russian central bank. Just a few months later, however, that high-water mark was washed away when cyber criminals exploited a network vulnerability at Equifax and stole personal data belonging to 145 million people.

Factory floors, transportation hubs, power grids, government databases, medical records and consumer goods are all increasingly becoming connected online, providing us with new capabilities to work smarter and faster. But as I discussed with Agenda last June, these new connections, which form the Internet of Things, also increase risk by providing our cyber adversaries with additional opportunities to disrupt our lives.

IT professionals are by far most concerned about the risks posed by unsecured Internet of Things devices, such as HVAC systems, home appliances or wearable tech. Of those surveyed, 82% predict an unsecured IoT device would cause a data breach in their organization. And 80% say the breach would be catastrophic.

The first line of the SEC guidance document sums up the problem succinctly: “Cybersecurity risks pose grave threats to investors, our capital markets, and our country.”

We all have a role to play in fighting the international cyber threat. The cyber-security survey is a tool that businesses can use to initiate a serious internal discussion about cyber security. IT professionals and executives can use it as a starting point to identify potential vulnerabilities, develop an action plan, and make the investments needed to reduce risk and protect the value of their organization.

The cost of protecting your organization will likely be less than the cost of cleaning up after a major breach and loss in market cap.

Boards need to include data assurance in their discussions as well. For some data-driven organizations — GPS-based app developers or hospitals, for example — having their information altered and left in place could be as damaging as having it stolen outright.

A catastrophic cyber attack doesn’t have to happen. To help protect your organization, and remain in good standing with shareholders, give your chief information security officer a seat at your next board meeting.

Copyright 2018, Money-Media Inc. All rights reserved. Redistributed with permission. Unauthorized copying or redistribution prohibited by law.