JUNE 21, 2016

Legaltech® news

ONLINE

An ALM Publication

Cyber for the C-Suite: 3 Tips for Closing the Information Gap

BDO's Shahryar Shaghaghi gives advice for pushing cyberattack readiness to the top of the board's list.

BY IAN LOPEZ

It's no secret that there's a language barrier between technologists and executives, but on the modern cyberthreat landscape, misunderstandings can cost businesses money, reputation and jobs. This begs the question: How can companies bridge this information gap?

Cybersecurity is "similar to other risk management sets of issues that the board has to be on top of from an overall oversight" perspective, explained Shahryar Shaghaghi, head of BDO's international cybersecurity group. "Traditional information security has evolved to an extent to where it now has to be an integral part of any management risk profile, and it has to be translated in a meaningful way that the management and board can fully understand."

For board members, the idea of managing risk is "not a foreign concept," CyberVista CEO Amjed Saffarini previously told Legaltech News. "What is foreign is the form that this risk takes—the digital risk, the internet risk, the cyber risk—and so, that's where you need to fill the gap."

A survey from CyberVista and Zogby Analytics quantifies this lack of understanding, finding that while over 60 percent of participants reported at least one cyberattack attempted on their organization, 35 percent were unsure of what in their state legally constituted a breach. Yet the notion that organizations are falling behind in cyberwarfare is not lost on CEOs, as an IBM survey found that a little over half of CEOs polled reported their organization's cybersecurity strategy as "well-established."

Misunderstandings around cyberthreats are not surprising to Shaghaghi. Traditionally, boards have had audit committees providing them with metrics around cyber risks, but "in general they have operational metrics, and painting the picture in terms of the number of attacks and the types of impacts." Therefore, they give "very little" information for management "to really understand from a standpoint of risk profile and overall cybersecurity risks" and what they mean to the organization.

Here are three tips from Shaghaghi to overcome the information gap standing between organizations and an effective risk management strategy:

1. Begin the great migration from a reactive to proactive cyber strategy

The digital revolution is well underway, and along with it, "our lives are becoming more and more digitized," Shaghaghi said. "There's no question that [cyberattacks] will not slow down. What we need to focus on is to really contain them and minimize their impact."

In a "reactive situation," companies don't have "much time to be able to follow a set of logic and patterns" that would have a "higher impact in terms of mitigation," he added.

For a proactive plan, Shaghaghi advises to employ "predictive threat intelligence data" as it allows you to plan and test strategies so cyberattacks aren't "a surprise" or "first-time event for you to react to." Doing so, he explained, would be "more proactive than reactive in terms of" understanding potential scenarios that could destroy or impact an organization.

2. Incorporate Predictive Threat Intelligence Data into your 'Risk Profiling'

With cyberattacks continuously proliferating, there's much information available on who may be attacked next and why. Shaghaghi noted that threat intelligence data is available from "various sources," including the government, and it "can be correlated to your inherent risks" and attributes of your company to provide "more meaningful" information.

With this information, the board "can start to look at, 'Why would the bad guys want to potentially attack my organization,'" he said. "And once you start looking at those incentives and start looking at probabilities," you can categorize and evaluate your assets.

"Very few companies do that right now. I think it's very important, like any other risk profiling. Organizations need to go through valuation of their assets, and by doing that they can apply the right level of decision-making process for their management and board to understand truly in a quantified way what a risk is," he added.

Shaghaghi also advised that when source data isn't available, organizations "can start the journey" by looking at the "most important set of information" as it applies to "the business level." Doing so will get the attention of the board, as "the tech level is not really the right level" to help executives understand the risk. Instead, he advised to link risks to such things as the supply chain and data privacy.

3. Develop a Risk Management Profile with a 'Cybersecurity Baseline'

Shaghaghi noted that while there's guidance from shareholders and regulators for having at least one board member with cyber knowledge, this is "not practical" because of a shortage of cyber resources. It's not "about having that expertise. It's about translating the data in a meaningful way," he said.

In an effort to fight risk and help the board understand the importance of doing so, Shaghaghi suggested developing a risk management profile in relation to a "cybersecurity baseline" for decision-making. Additionally, a company will want to get direct reports aligned with this baseline, and in doing so, the reports will become "more mature" regarding cyberthreats.

"Once you have the right level of information associated with some sort of benchmark, you can definitely provide this benchmark" in a way that shows its importance as it relates to an industry, he added.

From there, an organization can measure and report against the baseline, making its risk management valuable and "measurable as opposed to getting a report full of technical jargon that doesn't mean anything to the board or management."

Shahryar Shaghaghi
National Leader, BDO Technology Advisory Services Practice and Head of International BDO Cybersecurity
(212) 885-8453 / sshaghaghi@bdo.com