Security Resilience in the Age of Rising Cyber Breaches

Understanding how to build organizational resilience is vital to deepening board confidence and support.

Ask any executive of a Fortune 500 company and they'll probably nod their head in agreement that cybersecurity threats and risks have cost them plenty of restless nights. They've watched as large public companies' stock value has dropped in the hours after a cyber breach announcement. Think back to some of the big-name recent data breaches: Equifax, Anthem, eBay, JP Morgan Chase and Home Depot. Longer-term, breached companies tend to underperform the NASDAQ, according to one study.[1]

Eight in 10 organizations say their executive leadership supports security, and more organizations than ever now have CISOs in charge of the information security function, according to the 2017 State of Cybersecurity Report.[2] Board executives are also keenly aware that security is intimately tied to a company's brand and customer loyalty, both of which are undermined by a cyber breach.

Yet, Research by ISACA shows that 48 percent of organizations don't feel confident in their team's ability to address complex attacks. Fewer than half are confident in their team's ability to handle anything beyond simple cyber incidents, according to the 2017 State of Cybersecurity Report. Perceived deficiencies are marked by big skills gaps in the know-how of security professionals with only 52 percent able to understand business; 25 percent lacking technical skills; and 17 percent demonstrating adequate communication skills. Those are pretty high numbers considering the amount of money companies now invest in security technologies and operations to combat the cyber threat.

Finding the Same Page

An approach that might instill more board confidence is to take more proactive steps and establish a strategic plan of security practices, policies and priorities for the long term. To do this, companies must build a tightly aligned security mindset that extends from the boardroom to the frontline security operations. This will not only improve security resilience, it will help executives lose fewer hours of sleep.

Adoption of this strategy requires new thinking, however. Executives and board members traditionally have viewed cyber security as a tactical problem, not a strategic issue. This must change. Fixing security vulnerabilities and flaws across

the enterprise requires an ongoing effort to establish a culture of security in the business.

Workforce readiness is also critical, as mentioned above, because insiders carry out an estimated 60 percent of all attacks; consequently, the workforce is the greatest point of vulnerability, according to CMMI. While maturity in and of itself does not automatically ensure resilience, it is a key ingredient in ensuring reliable, consistent outcomes.

Another necessary step in addressing cybersecurity problems is to put in place a program to develop the team's maturity and capabilities. Cyber resilience, not emergency response, should be the focus of IT. Companies that go about business as usual tend to focus on reactive measures that entail ad-hoc security patches, which are neither adequately effective nor durable enough to build strong cybersecurity capabilities.

The overall goal is to build board confidence by aligning strategic objectives with pragmatic insights to security risks. Companies that pursue a path of building security resilience that focuses on the highest risks will benefit from a stronger security cordon and culture across the enterprise. That type of progress should offer some rest for those executives who lie awake at night, listening for the next shoe to drop.

Cybermaturity.cmmiinstitute.com

Sources

1 – Comparitech article. https://www.comparitech.com/blog/information-security/data-breach-share-price/

2 – ISACA State of Cybersecurity Report https://cybersecurity.isaca.org/state-of-cybersecurity