CMMI® Institute
AN ISACA ENTERPRISE

Hard Truths About Cybersecurity Failures

Many organizations must contend with gaps that cannot be fixed solely by deploying the latest technologies.

In the face of unrelenting cybersecurity attacks, most organizations respond by collectively spending billions on cutting-edge security technology — more than $93 billion in 2018, Gartner projects. And yet every year the severity and scale of breaches increases.

Unfortunately, there's no volume discount on security breach costs. A break-in takes a toll on organizations both in terms of stolen assets and in damage to reputation and brand. In 2017 the average cost of a corporate breach was $11.7 million, up 23 percent from the previous year, according to a recent Accenture study. The British insurance company Lloyd's estimates that cybercrime costs companies $400 billion annually in direct damages and disruption to business.

What can be done to better manage cyber security risks?

Experts observe that, despite the enormous security spend, gaps are everywhere, presenting attackers with numerous targets for exploits and breaches. And yet fixing gaps is not entirely about applying technology. CMMI believes that the solution starts with thinking of security as part of your business strategy, focusing in important places such as organizational roles and culture. Because these are where gaps most frequently occur.

But closing gaps in security is also about drilling deep to find answers to each of the following organizational issues: operational efficiency of actions taken; resiliency of the people and maturity of processes and technology being used; and fully understanding the total cost of ownership.

Business Drivers and Resilience

Further, a successful security strategy requires three well-coordinated components: program, management and measurement. A security program must be suited to the type of business and tailored to the risks at hand. That includes determining whether the processes and mechanisms that support security goals are mature and resilient enough to withstand employee attrition, budget cuts and emergency situations.

Yet for some organizations conducting a self-assessment of cyber security strategy and capabilities may not be fully embraced by senior management. Is the cyber security strategy to achieve resilience out of alignment with the business?
For many organizations that's a challenge. Fewer than 50 percent of organizations are confident in their security team's ability to handle anything beyond simple incidents, according to the ISACA's State of Cyber Security 2017 report. The survey also identified some of the biggest security gaps in today's businesses: only 25 percent of companies and organizations have security professionals with the necessary technical skills; just 52 percent of companies have the ability to understand security processes; and a scant 17 percent have established internal safe information sharing structures to convey details to employees instead of hiding them out of fear the information will fall into the hands of bad actors.

A resilient organization is one that has achieved the necessary risk-based maturity in those capabilities that address organizational risk. While maturity in and of itself does not automatically ensure resilience, it is a necessary component for strong security measures and a key ingredient in ensuring reliable, consistent outcomes. In this case, resilience refers specifically to the ability of an organization to adapt to changing conditions without compromising their security posture and likewise, to recover from unanticipated events such as an attack or outage.

Security talent is also critical to help close security gaps and improve day-to-day efforts to counter attacks, though it's not easy to find: according to a 2017 ISACA study, just 59 percent of enterprises receive five or more applicants for each open cybersecurity position — and most of the applicants are unqualified. As in other professions, hands-on experience is considered the most important qualification for security professionals.

Looking ahead, many organizations will continue to juggle the risks they face and the specific controls, countermeasures and practices they apply with their one-size-fits-all regulatory-compliance approach. The security situation will only improve when there is a significant refocus on security practices that emphasize business strategy alignment.

Learn more about how you can take a risk-based approach to measuring and managing security risks in the context of your business mission and strategy.