CMMI® Institute
AN ISACA ENTERPRISE

Cyber-Resilience: A More Potent Approach to Cybersecurity

Is your business cyber-resilient?

For the CEOs, CIOs, CISOs and others charged with protecting their enterprises from cyber attack, this question becomes more pressing by the day. Fifty-eight percent of global enterprises admit to having experienced at least one data breach during the past 24 months and, per a recent McKinsey & Co. survey[1], the impact of one high-visibility breach after another is making cybersecurity a top concern for business leaders worldwide.

This stark reality depicted by McKinsey is leading companies to view their cybersecurity strategy in a different light. Armed with the understanding that data breaches are inevitable and can put the entire enterprise at risk, corporate boards and senior managers have begun focusing cyber resources on the highest-priority threats they face and mitigating those, rather than trying to prevent cyber attacks entirely.

Thus, boards and senior managers are demanding their organizations become *cyber-resilient,* which in simplest terms is a reflection of how well a company can continue to carry on its business when a system failure or adverse cyber event occurs.

"Companies that achieve cybersecurity resilience not only have excellent perimeter defense that blocks threats and detects intrusions, but they're also taking the steps necessary to minimize cyber impact and successfully survive those attacks that prove unavoidable," observes Doug Grindstaff, SVP of cybersecurity solutions for the CMMI Institute. CMMI's best practices models help businesses identify performance gaps and increase performance results.

McKinsey's survey responses depict a wide range of activities that enterprises are rolling out to counter their cyber risk – along with some concerning shortcomings. The plus side includes investments in new security systems and personnel, external advisors and control systems. "What they lack, however," write the authors of the consulting firm's report, "is an effective, integrated approach to cyber risk management and reporting."[2]

The authors go on to identify three specific shortcomings:

1. Lack of *structure.* While corporate boards and committees are swamped with reports, they're often inconsistent and cluttered with too much detail. Unsurprisingly, many boards are dissatisfied with the degree of insight that this provides.

2. Lack of *clarity.* From a board member's point of view, the most glaring problem is that these reports fail to capture the degree of risk faced by the business, leaving leadership without a clear sense of their biggest vulnerabilities. The McKinsey consultants quote one top executive as

saying, “I wish I had a handheld translator, the kind they use in Star Trek, to translate what CIOs and CISOs tell me into understandable English.”

3. Lack of *consistent data.* This compounds the problems from numbers one and two. One quoted executive describes receiving a report indicating that an important corporate asset was sufficiently protected, only to be given a second report the following day that insisted the same asset was under threat. The executive asked: “Which should I believe? And what should I do?”

Shifting from a ‘Culture of Compliance’ to Cyber-Resilience

Underlying these deficiencies are two competing views of cyber security.

On the one hand, there are CISOs and others who are reactive in their approach, caught up in what might be termed a “culture of compliance,” and sometimes find themselves “fighting the last war.” Grindstaff, who is chief architect of the CMMI Cybermaturity Platform and has spent years meeting with enterprise cyber professionals, describes these cybersecurity execs as concentrating on the *last* breach to impact their industry. They demand their teams prevent a similar sort of occurrence within their own organizations, and focus on compliance with regulatory requirements. But this type of reactive “check-the-box” mentality leaves them open to any number of “Day One” risks – the continuously emerging new threats that have yet to occur.

A culture of cyber-resilience, on the other hand, analyzes the most critical risks facing the company at any given time and then seeks to mitigate those risks. Instead of trying to defend against each and every possible threat, the cybersecurity team zeroes in on those dangers that pose the gravest risk to the business, constantly re-evaluating which ones are paramount and how capable they are to respond to them. While steps are taken to detect and prevent an attack, the true measure of success is no longer “Can we dodge the bullet?” but “Are we capable to continue to function if a breach occurs?”

This approach helps address the communications problem identified by McKinsey, since it frames the security data that’s presented to board members and senior executives in terms of the business risks that are posed and the counter-measures that have been taken.

Because every enterprise faces a unique set of risks, every company’s cyber-resilience program must also be unique. The biggest danger for banks and retailers, for instance, may be the theft of their customers’ personal and financial information, while threats to a manufacturer’s supply chain may be its chief cyber-related risk. It follows, then, that what each type of enterprise does to safeguard against these risks will also be different.

Moreover, because new threats are constantly emerging, no enterprise can afford to sit on its laurels. Managing cyber risk is an ongoing process, and resilience-driven thinking reflects that. It isn’t based on crossing some imaginary goal line (whew! *Now* we’re finally safe!), but on a continuous reassessment of the enterprise’s critical capabilities given the current threat landscape. That’s a disconcerting prospect for many cyber-security executives, leading Grindstaff to say that when it comes to cybersecurity, “The key to being successful is getting comfortable with being uncomfortable.”

A major cyber attack can be devastating to any organization, and unfortunately there is no silver bullet to prevent them; breaches will occur despite the most heroic efforts to ward them off. To stay ahead of the threat, companies need to constantly reevaluate their risks and plans to respond. By undertaking an ongoing program of priority-based preparation, prevention, response and recovery, a business can achieve true cyber-resilience and minimize the consequences of any attack.

[1] ‘A time for boards to act,’ McKinsey & Co., https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/a-time-for-boards-to-act

[2] ‘Cyber risk measurement and the holistic cybersecurity approach,’ McKinsey & Co., https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/a-time-for-boards-to-act