Bespoke Cybersecurity: Tailoring Your Strategy to Different Business Units' Needs

When it comes to socks, knit caps and sunglasses, one size usually fits all customers. But when it comes to cybersecurity, experts agree that even the most comprehensive strategy needs to be adapted to suit the needs of an extended enterprise's different business units.

A recent McKinsey & Co. report on protecting digital assets explains that, "In determining the priority assets to protect, organizations will confront external and internal challenges. Businesses, IT groups, and risk functions often have conflicting agendas and unclear working relationships. As a result, many organizations attempt to apply the same cyber-risk controls everywhere and equally, often wasting time and money."[1]

Doug Grindstaff, SVP of cybersecurity solutions for the CMMI Institute, echoes the McKinsey authors' thinking: "A large enterprise includes multiple business units addressing varied markets and, therefore, with different needs, a far-flung and complex supply chain and an extended network of business partners," he notes. "To be effective, a cybersecurity approach must encompass all of these elements."

Given that most large organizations serve multiple markets and often include consumer, commercial and even research businesses, Grindstaff says that the first step to working out an all-encompassing cybersecurity strategy addressing the entire business's needs is to identify the different types of risk tolerance associated with different parts of the business.

This is in line with the McKinsey report, whose authors begin by stating that "The idea that some assets are extraordinary—of critical importance to a company—must be at the heart of an effective strategy to protect against cyber threats. Because in an increasingly digitized world, protecting everything equally is not an option.

"In any given enterprise," the report continues, "some of the data, systems, and applications are more critical than others. Some are more exposed to risk, and some are more likely to be targeted."

A large enterprise with aerospace and medical units, for example, may need to protect their intellectual property first and foremost in the aerospace business, while for hospitals and medical systems safeguarding patient data is typically the highest priority. "The key point," the McKinsey authors emphasize, "is to start with the business problem, which requires a consideration of the whole enterprise, and then to prioritize critical risks."

Cybersecurity Frameworks: Different Strokes for Different Folks

Cybersecurity frameworks, such as those published by the International Standards Organization (ISO) and the National Institute of Standards and Technology (NIST), can help a company zero in on its most important digital assets and the key risks that it faces. But some frameworks are better suited to this than others.

Frank Kim, founder of security consulting firm ThinkSec and curriculum director at the SANS Institute, groups the different cybersecurity frameworks into three categories:[2]

1. *Control frameworks,* according to Kim, are best-suited for organizations with less developed security protocols that need to improve their overall cybersecurity posture. A control framework helps them assess the state of their technical capabilities and establish a baseline set of security controls. An example would be the NIST 800-53 framework.

2. *Program frameworks,* such as the ISO 27001 guidelines, are used to assess the overall state of a cybersecurity program, measure its maturity and benchmark it against other companies in the same industry.

3. *Risk frameworks,* including NIST 800-39 and ISO 27005, help CISOs and other cybersecurity professionals prioritize their activities. Kim says they can be used to identify, measure and quantify risk, and structure a risk-management program.

CMMI Platform: Consistent But Flexible

The CMMI Cybermaturity Platform developed by Grindstaff represents a fourth category of framework that incorporates elements from all three. Its self-assessment approach requires every group and business unit across an enterprise to consider the same set of potential vulnerabilities, but allows them a considerable degree of latitude for conducting and acting on their assessment.

"An organization's cybersecurity program needs to be consistent across the enterprise in how it reviews and evaluates risks," Grindstaff acknowledges. "But the measures taken will differ from business unit to business unit and geography to geography, based on the business model and the nature of the risks that each one faces."

Grindstaff says cybersecurity leaders should ask three key questions of every business unit across the enterprise:

- Where are you exposed?

- Which of these exposures do you truly care about?
- What's the most capital efficient way for you to address those truly critical exposures?

The answers will vary from group to group and department to department.

Grindstaff likens the situation to a pack of zebras stalked by a lion. The big cat would naturally target any weaker or younger zebras that lag behind the rest of the herd.

"If I had to move this herd across the Serengeti," notes Grindstaff, "my chief concern would be that I don't have an outlier—that none of my zebras stray too far from the pack. In other words, I would need to ensure that I don't have a vulnerability that could serve as a point of entry for a would-be attacker."

At the same time, gathering the herd too closely together won't work either, because then the lion only has a single, target to pursue—one that is both very rich and very slow and cumbersome.

The better solution, Grindstaff says, is to maintain some order to the herd, but also allow each zebra some freedom of movement. That way the pack stays together and no one animal is overly exposed, yet each herd member is able to graze and travel in the way that best suits its nature.

But like the zebra herd, says Grindstaff, this only works "if each unit of the enterprise is situationally aware and fully cognizant of the importance of security."

---

[1] 'Protecting your critical digital assets: Not all systems and data are created equal,' McKinsey & Co., https://www.mckinsey.com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal?cid=reinventing-eml-alt-mip-mck-oth-1701

[2] 'How to choose the right cybersecurity framework,' TechRepublic, https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/