Holistic Cyber Resilience Key to Building Board-Level Confidence in Enterprise Preparedness

With cyberattacks rising – and corporate fear of an attack rising along with them – how should an enterprise respond? McKinsey & Co. posed precisely this question in a recent survey. It found that an overwhelming majority of corporate board members now consider cybersecurity a top concern – but fear their companies are not adequately prepared to manage the threat.[1]

Typical of many comments included in the report, one respondent told McKinsey's researchers that, "So far, we have not taken a big hit. But I can't help feeling that we have been lucky. We really need to ramp up our defenses." Similarly, another executive noted that, "Digital resilience is one of our top priorities. But we haven't agreed on what to do to achieve it."

Why are these board members so insecure about their businesses' ability to guard against cyber risk?

Survey Reveals Need for Holistic Cybersecurity Approach

The survey responses reveal that these board members' organizations are already taking numerous steps to counter online hazards, including investments in new personnel, new skill sets and new technology. What their organizations lack, however, according to the McKinsey study authors, is an overriding holistic approach to cybersecurity.

As defined by veteran IT author Margaret Rouse, such an approach "seeks to integrate all the elements designed to safeguard an organization, considering them as a complex and interconnected system. The ultimate purpose of holistic security is continuous protection across all attack surfaces: the totality of all physical, software, network and human exposure. The integration of different levels and types of security enables a more comprehensive understanding of vulnerabilities and more comprehensive protection against a variety of threats."[2]

While the elements of Rouse's definition are all necessary to holistic cybersecurity, they aren't necessarily sufficient. So the McKinsey report goes further, putting it this way: "A holistic approach proceeds from an accurate overview of the risk landscape." The goal, the authors

state, “is to empower organizations to focus their defenses on the most likely and most threatening cyber risk scenarios, achieving a balance between effective resilience and efficient operations. Tight controls,” they add, “are applied only to the most crucial assets.”

Building Board Confidence with CMMI Cybermaturity

One such holistic framework is the CMMI Cybermaturity Platform, developed by Doug Grindstaff, SVP of Cybersecurity Solutions for the CMMI Institute. Grindstaff says a key benefit of the platform is that it instills confidence at the board level in the organization’s preparedness to cope with a variety of cyber dangers.

In discussions with enterprise leaders, Grindstaff also has observed McKinsey’s findings – all too often. He notes that corporate boards “often lack confidence in their organization’s ability to fend off or recover from a devastating cyberattack.” Yet many CIOs and CISOs mistakenly blame those board member doubts on a low level of technical expertise.

“’They just don’t get it,’ is a common refrain that you hear from CISOs and other security professionals,” says Grindstaff. “But that’s wrong and completely misses the point. It isn’t about being technically savvy,” he insists, “but about putting cybersecurity into a business context.”

Such a context is necessarily holistic, taking into account all of the risks that the organization faces, prioritizing them and then requiring each group and business unit across the enterprise to consider taking protective measures against the same set of potential vulnerabilities. But, Grindstaff points out, it is also about presenting security-related data in the manner of a business report – a format with which virtually all board members are intimately familiar.

Needed: Data about Cyber Risks

The McKinsey report echoes this sentiment when it concludes that holistic cybersecurity “is not, or at least not primarily, about coding. It is more the result of engaged conversations across roles in which acceptable risks are identified, the data needed to understand the organization’s true resilience are marshalled, and the focal points for risk-reducing investment are established, along with the most effective ways to monitor progress.”

“Without data about the company’s inherent security risks and what’s required to mitigate those risks,” Grindstaff says, “it is impossible for the board to make informed decisions about the company’s cybersecurity posture. And if the data provided is irrelevant from a business standpoint, or if the metrics change from quarter to quarter, it undermines the board’s ability to make data-informed, risk-prioritized decisions and then track the outcomes of those decisions over time.”

Holistic Approach & Steady Data Flow Instill Board Confidence

Since it’s the board that has the best overview of the business’ risk tolerances, no holistic security program can succeed without the board’s steadfast support. But no board can be truly confident in their organization’s cybersecurity without a steady flow of quality information on the risks facing the company and their potential impact on the business.

It's the combination of the holistic, risk-prioritized cybersecurity approach and steady flow of supporting information that leads to the kind of confidence that enables board members to sleep soundly at night.

---

[1] 'Cyber risk measurement and the holistic cybersecurity approach,' McKinsey & Co., https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

[2] 'Holistic security,' TechTarget, https://whatis.techtarget.com/definition/holistic-security