By prioritizing cyber resilience and adopting tools like a scorecard, organizations can not only mitigate the impacts of cyber incidents but also bolster their competitiveness and strategic focus on cybersecurity.

Build your own cyber resilience scorecard

Pearlson and her team at MIT developed a scorecard template based on her experience as a member of several boards. The scorecard idea came from her observation on the boards she's on that companies were looking for a methodology to assess their cybersecurity posture. The multidimensional view of cyber resilience scorecards is pivotal in the shift toward resilience, serving as a comprehensive framework for assessing, monitoring, and enhancing an organization's ability to withstand cyber threats.

Framework development:

Distinguish between transformational and operational aspects, focusing on different threats, allowing organizations to have a plan for recovery when they do.

Assessment and goal-setting:

How exposed your organization really is. Here's how – get a comprehensive risk score in just 5 days.

Malini Rao, CISO, DeepLearnCyber.ai

The proliferation of potential cyber threats, and the sheer volume of breaches, is making it harder for many organizations to keep up with the demand for data security. Cybersecurity is a屹nding at the board level, with a recognized need to understand where its operations can be impacted. Cybersecurity is now a businessnanity, serving as an integrated framework for the governance of cyber incidents.

Regulatory bodies are increasingly looking to organizations to report on cybersecurity risk, policies, and training. This can include boards, directors, and executive leadership. These boards and organizations are now looking to incorporate cybersecurity into their governance processes, with regular reporting to key stakeholders, a vital oversight, and are focusing on implementing cybersecurity policies, investing in new technologies, or enhancing employee training.

Malini Rao, CISO, DeepLearnCyber.ai

Perspective

The cyber resilience strategy that has been around for 20+ years but only now gaining traction, ensuring that cybersecurity is not only a matter of protecting informational assets, but also focuses on mitigating the aftermath, getting back up and running with minimal cost or disruption.

Related

Summer with These Cyber Must-Reads

Forget GPT-4 (For Now) – Kick Off Your Summer with These Cyber Must-Reads

Perspective

A strategy that’s been around for 20+ years but only now gaining traction ensures that cybersecurity is not only a matter of protecting informational assets, but also focuses on mitigating the aftermath, getting back up and running with minimal cost or disruption.