What Cyber Resilience Really Means — And How to Achieve It.

Over the past few years there has finally begun a major shift in how organizations view cybersecurity. The impact of high-profile breaches has propelled growing board awareness, and recognition, that no company is immune from compromise.

Boards are rapidly realizing that cybersecurity is an issue of enterprise risk, not the IT challenge they once thought it was. Enterprise risk management is something boards know well. So, suddenly, it makes perfect sense that – as with any enterprise risk – the key focus is *mitigation not prevention*.

As a result, the corporate view of cybersecurity is transitioning from reliance on technology-based cyber defense – i.e., defend the enterprise by establishing an impregnable perimeter around it – to a broader view: cybersecurity resilience. Cyber resilience is based on the concept that, armed with the understanding that breaches are inevitable, an organization can peer through the lens of enterprise risk management to better focus its resources on meeting the cyber threats and mitigating the cyber risks that matter most.

Companies that achieve cybersecurity resilience are better prepared. Not only do they have excellent perimeter defense to block threats and detect incidents, but they've taken the steps necessary to minimize impact and thus successfully survive the attacks that prove unavoidable.

Building and Sustaining Cybersecurity Resilience

So how can organizations create an effective, sustained approach to building cybersecurity resilience? At CMMI, we believe that cyber resilience is a strategic approach to making security decisions that focus on the company's biggest risks, driven by the board and executive level. It involves a shift in mindset that engages the whole organization: not just security and IT professionals but also senior executives and the entire workforce.

A key starting point for building cybersecurity resilience is the recognition that because each organization faces a unique set of risks, its approach to building resilience must also be unique. Crucially, assessing those risks starts with identifying the organization's most critical assets – the assets that, if compromised, would most dramatically impact the business. With those crown jewels identified, you analyze the potential impact of cyber threats on your critical assets, and how vulnerable the organization is to those threats. Finally, you prioritize enterprise cyber risk mitigation activities around the combination of threats and vulnerabilities with the most potential to disrupt or damage the business.

That analysis translates into a radically different set of risks for each industry. For banks or retailers, some of the biggest cyber risks are breaches of consumers' personal and financial

information. A manufacturing company that depends on an extensive supply chain to maintain production can be highly exposed to cyber-related problems via its partners. A software company faces a broad set of risks related to securing software development and building security into products.

In some cases, the biggest risks to the enterprise may lie outside the cybersecurity realm altogether. For example, one utility company CISO told me that he was much more worried about physical security threats – such as sabotage to power plants – than about cyber-attacks. As he put it, "I've got pipes to protect."

Within each industry, companies naturally share some of the same risks. But there are also important differences based on each company's operational model and business goals.

Building cybersecurity resilience therefore must start by analyzing a company's unique set of cyber risks, or enterprise risk profile. That risk profile provides the foundation for understanding where to focus security investment to mitigate enterprise risk.

The Three-Legged Stool that Supports Cybersecurity Resilience

We designed the ***CMMI Cybermaturity Platform*** to help companies achieve this. It provides a practical, objective method for assessing risk, measuring the organization's level of readiness to meet the risks, and continuously building cyber resilience. In fact, the design of the platform was based largely on input from a broad set of organizations that told us exactly what they needed.

Once your company has a clear view of its enterprise cyber risk profile, the challenge is to prioritize security investment to achieve the greatest risk mitigation. Prioritization is essential, because there is an infinite range of potential cybersecurity protection measures and no organization has the resources to implement all of them.

By highlighting the gaps between the organization's current capabilities and the maturity required to match the risks, our platform generates a roadmap for driving investment to the most critical areas. That roadmap also provides an objective method for demonstrating to the board where security investment is most urgently required.

The investment in building cyber resilience essentially consists of three interlocking elements. Think of it as a three-legged stool: all three elements are essential to build a strong, stable structure.

- **Security capabilities.** Which capabilities are needed to address the most important risks to the enterprise? The answers are likely to be different for a manufacturer, compared to a financial-services company. For example, given the organization's limited resources, is it more important to prioritize investment in securing the supply chain or protecting consumer information? Does the maturity of the organization's capabilities in each area match the importance of the risks to the organization? Do I have the right governance, risk mitigation, and recovery processes in place for those risks?

- **Workforce readiness.** Cybersecurity resilience involves the entire organization, not just IT and security experts. To create a cyber-resilient company, it's essential to build the

right security-aware culture among all employees. Again, the emphasis should be driven by the company's unique set of risks. The culture-building process includes clearly communicating policies across the entire workforce and explaining to all how personal behavior can adversely affect – or advantageously benefit – corporate security resilience.

- **Security and IT operations (SecOps).** The company's risk profile should shape the priorities of the IT security and IT operations teams. Based on that risk profile, which evolving threats are most important to monitor? Is the company leveraging the best technology to address and mitigate these risks?

Resilience is a Never-Ending Challenge

Perhaps most important to understand is that assessing risk and building cybersecurity resilience is a continuous process, not a check-the-box activity to be undertaken once or even annually. That's because the threat landscape is highly dynamic: new threats continually surface and quickly become widespread, creating new risks. Think about the rapid rise of ransomware in the past few years.

To stay ahead of the threats, organizations need to continually evaluate their risks and their capabilities, ensuring they are focusing investment on the things that matter most. Any organization that does this on a continuous basis – assessing enterprise risk; measuring the organization's capabilities, workforce readiness, and security operations from the perspective of the risk; and then prioritizing security investment accordingly – is truly building cybersecurity resilience.