Cybersecurity at MIT Sloan

MITSloan Management Review

Michael Coden
Martin Reeves
Keri Pearlson
Stuart Madnick
Cheryl Berriman

An Action Plan for Cyber Resilience

It's impossible to avoid all cyber risk. Here's how to make your company more resilient in the face of new threats.

The NotPetya malware attack of 2017 encrypted the systems and disrupted the operations of global businesses, starting in Ukraine and spreading rapidly to over 60 countries around the world. Global shipping company Maersk, one of the worst hit, ultimately needed to rebuild its entire IT infrastructure. In the nine days it took to get its systems back online, the company struggled to continue operations using manual workarounds that teams came up with on the fly. In the end, the incident cost Maersk nearly $300 million.

A more recent ransomware attack shut down the operations of JBS USA, the largest U.S. meatpacker, and other attacks have affected hundreds more companies. In late 2021, for instance, the Log4j vulnerability allowed adversaries to embed malware and take control of millions of Java applications developed over the past decade. These widespread incidents have proved that successful cyberattacks are inevitable.

Given that it's impossible to protect against all new cyberattacks, it has become critical for companies to reduce the impact of cyber breaches by focusing on cyber resilience. Cyber resilience requires a systematic, structured, adaptive approach and cannot be relegated to the office of the CIO or chief information security officer. Because it potentially involves all parts of the business, it must be led by the C-suite and board.

Traditional Cybersecurity Is Insufficient

Most organizations evaluate their cyber maturity according to the National Institute of Standards and Technology's Cybersecurity Framework, but it is 80% focused on identification, protection, and detection, and only 20% on an organization's ability to respond to and recover from a breach. Similarly, our research on cybersecurity spending shows that 72% is spent on identification, protection, and detection, with only 18% spent on response, recovery, and business continuity. Not only does this imbalance leave organizations vulnerable, but it leaves companies ill prepared to comply with new rules proposed by the U.S. Securities and Exchange Commission that would require companies' SEC filings to include details on "business continuity, contingency, and recovery plans in the event of a cybersecurity incident." Cybercrime laws have already been enacted in 156 countries, and 250 bills are being considered in 40 U.S. states and Puerto Rico, with additional cyber resilience regulations expected to follow.

...

TO CONTINUE, SCAN QR CODE

***Michael Coden** is a senior adviser at BCG with over 30 years of experience in cybersecurity strategy. **Martin Reeves** (@martinkreeves) is a senior partner at Boston Consulting Group and chairman of the BCG Henderson Institute. **Keri Pearlson** is executive director of the research consortium Cybersecurity at MIT Sloan (CAMS). **Stuart Madnick** is the John Norris Maguire Professor of Information Technologies, Emeritus, at the MIT Sloan School of Management and the founding director of CAMS. **Cheryl Berriman** is global senior director of the CEO Advisory practice at BCG.*

THIS QR CODE WILL DIRECT YOU TO THE CAMS WEBSITE
https://cams.mit.edu
SCAN ME

Cybersecurity at MIT Sloan

THIS QR CODE WILL GIVE YOU ACCESS TO A DIGITAL COPY OF THE ARTICLE
SCAN ME