BCG

Weekly Brief

April 24, 2023

Cybersecurity and the C-Suite

To BCG's network around the world,

Cyber threats are becoming more frequent, with 85% of cybersecurity leaders worried about the rise in attacks. Nation-states and their surrogates are increasingly attacking corporate assets, while new technologies like generative AI create more opportunities for malicious actors to threaten private and public infrastructure and networks.

Chief information security officers (CISOs) and cyber teams work tirelessly to prevent attacks and minimize disruption. This work is never over, though, and the CEO and C-suite should play active roles in securing their organizations.

BCG recently surveyed 600 senior cybersecurity leaders across industries and geographies to understand best practices and approaches. Several important insights and three important recommended actions emerged from the firms that identified their cyber capabilities as advanced.

Treat cybersecurity as a business. Cybersecurity should be organized, managed, and evaluated as a business. Most of the advanced cyber organizations are already doing that. More than half of them, 56%, measure the ROI of cyber investments, compared with 39% of average cyber organizations.

When cybersecurity is treated as a business, boards, CEOs, and the C-suite ask how cybersecurity programs fit into broader strategies. They want to understand the business impact of cyber events and insist on fast and targeted responses to attacks. They view cybersecurity as a strategic capability that they adequately fund even in tight economic times. Advanced cyber organizations spend more than double that of average organizations on cybersecurity, our survey found.

Build a cybersecurity culture. Cybersecurity is a human activity, not just a technology play. After all, most cyber breaches are caused by human rather than technological failure. Only 18% of surveyed companies report having a strong security culture. However, a culture of awareness, responsibility, and consequence reduces the odds and the impact of an attack.

When the C-suite makes cybersecurity a priority, the rest of the organization responds by making it a priority, too. For example, one large retailer decided to implement business information security officers, essentially CISOs for each business line, to help foster a security culture and understand risks. Employee training and a disciplined approach to avoid, manage, and recover from attacks also help. Leading organizations have begun to embed security processes and experts into development teams so that security acts as an enabler rather than a blocker further down the road.

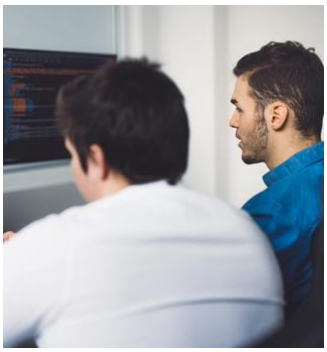
Expand your view of risks. Organizations should search expansively for today's risks and anticipate future ones. Advanced cyber organizations, for example, probe their supply chains and vendors as well as their customer base for external cyber-risks that may infiltrate their organizations. They also engage in scenario planning and tabletop exercises to understand new and emerging risk, create cross-functional responses to attack, and evaluate cybersecurity investments. Nearly three-quarters of advanced cyber organizations, 72%, identify AI-enabled attacks as a priority, compared with 53% of the average organizations.

With the cost of cyber crimes exceeding $2 trillion annually, these three actions are sensible and cost-effective measures that can make your organization and the world a safer place.

Until next time,

Christoph Schweizer
Chief Executive Officer

Further Reading



As Budgets Get Tighter, Cybersecurity Must Get Smarter

A survey of CISOs reveals how advanced companies gain cyber maturity and what best practices they use to prepare for emerging threats in economically uncertain times.

READ MORE →

Prepare for Cyberattacks by Overprotecting Your Crown Jewels

BCG managing director and partner Paul O'Rourke talks about the inevitability of breaches, the increasing focus on safeguarding personal data, and the cyber skills every company needs.

READ MORE →

The CEO's Guide to Cybersecurity

Cybersecurity is often viewed as a purely technical issue. But CEOs, boards, and the C-suite need to be part of the solution, strengthening cybersecurity programs and integrating them into broader strategies.

READ MORE →