BCG

Weekly Brief

August 27, 2024

Becoming a Cybersecure CEO

Not long ago, CEOs left cybersecurity to their chief information or security officers. Those days are over.

Cyber attacks are becoming more frequent and more damaging. The Cyentia Institute estimates the cost of a single high-impact breach to be $52 million. In aggregate, cyber attacks will cost the global economy nearly $10 trillion in 2024, according to *Cybercrime* magazine.

In response, regulators in the US and Europe are imposing new obligations on CEOs and on boards. In the US, for example, CEOs are responsible for ensuring that their companies promptly disclose material cybersecurity incidents and have strong processes to identify, assess, and manage these risks.

In recent years, partners in BCG's Risk and Compliance practice have worked with hundreds of clients on cybersecurity and digital risk, helping to elevate the topic from the tactical to the strategic, from siloed in IT to embedded in the business, from reactive to a source of competitive differentiation. They recently published The Cybersecure CEO, a primer on how leaders should think about and prepare for these new risks.

This rising scrutiny for CEOs is occurring while they are under pressure to digitally transform and to integrate AI and GenAI into their businesses—exposing their organizations to additional cyber risks and bad actors.

Human and organizational error are responsible for most cybersecurity breaches. In addition, increasingly sophisticated yet easy-to-use tools are making the criminal's job much simpler. GenAI is allowing infiltrators to quickly create realistic deepfake text messages, photos, websites, company documents, videos, and even real-time conversations.

It’s no longer a question of if a cyber attack will happen—but when. How can CEOs prepare themselves for this riskier, more regulated world? “The Cybersecure CEO” lays out questions that address the steps a CEO should take:

- **Are you having strategic discussions with your board?** You should at least be able to explain your company’s greatest cybersecurity threats and the key vulnerabilities of your most critical systems. You should also have a clear sense of what would happen to the organization in the event of a major attack.

- **Is your mix of cybersecurity spending right?** Companies have three goals in cybersecurity: prevention, responding to a crisis, and recovering from one. Most cybersecurity spending goes toward prevention. BCG estimates that only 20% is devoted to response and recovery once an attack happens. By focusing more on response and recovery, CEOs can help their companies minimize the impact of attacks—which are likely to be successful at some point in time—and improve their ROI.

- **How secure is your digital transformation?** As organizations race to digitize, CEOs should ensure that new IT solutions and cloud platforms are sufficiently secure—but not at the expense of postponing new digital solutions.

- **Do you have the capabilities, culture, and talent to be cybersecure?** You need to ensure that all business functions—not just IT and risk management—are actively involved in cybersecurity. CEOs can help elevate cybersecurity as a critical capability that all employees are responsible for.

As the job of the hacker gets easier, the demands on corporate leaders grow larger. By investing in recovery and protection, embedding security early in digital transformations, and creating a culture of vigilance, CEOs can manage cyber risk rather than fall victim to it.

Until next time,

Christoph

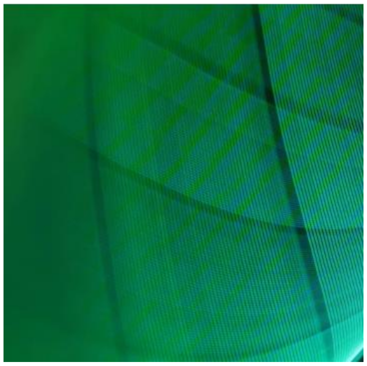
Christoph Schweizer
Chief Executive Officer

Further Insights

The Cybersecure CEO

Tougher regulatory oversight and the soaring costs of major data breaches are elevating cybersecurity to a higher strategic priority for corporate leaders and boards.

READ MORE



Cybersecurity and Digital Risk

BCG's cybersecurity consulting combines business expertise, a strategic mindset, use of proprietary tools, and deep knowledge of cyber technologies.

READ MORE

Is Your Supply Chain Cyber-Secure?

Resilient companies prioritize cybersecurity. And those that rely on a smooth-functioning supply chain are increasingly giving precedence to managing the cybersecurity risks of their suppliers, not just their own.

READ MORE