SECURITY INFOWATCH.COM

Cyberattacks often occur during technological change, such as migrating to cloud storage or when factories adopt connected sensors. That means that the board must be attuned to what the company is doing, and what vulnerabilities may be exposed as a result.

SECURITY EXECUTIVES

A cybersecurity handbook for corporate directors

The C-suite should not leave complete control of technology to the techies but assume rigorous oversight from day one

Justin Greis, Daniel Wallance

The risks of cybersecurity lapses are well known, from flight cancellations to ransomware demands to run-of-the-mill ever-present (though still troubling) data breaches. In 2023, known ransomware payments hit a record $1.1 billion. IBM research found a 71% increase in cyberattacks that used stolen or compromised credentials. A survey by McKinsey and the Institute of International Finance found that even among financial service companies, which are well aware that they

are prone to attack, their capabilities are often no match for the skills of well-organized and expert cyber criminals.

Launching a cyberattack is relatively easy, and attackers have the luxury of failure: they only need to succeed occasionally. The implication is that the defenses need to be at least as determined as the assaults. And for that to happen, boards are in a unique position to play an active oversight role. Here are three principles to keep in mind.

Ignorance is not an option

In 2023, the U.S. Securities and Exchange Commission required U.S. public companies and foreign private issuers to promptly report important cybersecurity incidents and describe their cyber-risk management processes. Companies are also required to set out how boards oversee cyber risks.

To meet these regulations, boards should know enough to be able to ask good questions about the maturity of the cybersecurity program, the potential business impact of different scenarios, and the company's level of risk tolerance.

On the latter, there can be a significant difference in cost, strategy, and focus between no tolerance and low tolerance. There can also be some combination, such as zero tolerance for downtime, and limited tolerance for small-scale breaches that affect only a few customers. Making such trade-offs is squarely within the oversight purview of boards.

Cyberattacks often occur during technological change, such as migrating to cloud storage, or when factories adopt connected sensors. That means that the board must be attuned to what the company is doing, and what vulnerabilities may be exposed as a result. Specifically, boards need to know managing is tracking where the company's IT (hardware and software), operational, and digitized factory assets are.

Finally, it can be helpful to engage in activities such as incident response exercises or cyber simulations to understand better how threats can play out and how well the company's cybersecurity program is operating.

See cybersecurity as a competitive differentiator

McKinsey studied 114 companies, ranking their cybersecurity on a scale of 1 to 4. Only 10% were in a position to defend themselves against cyber threats. Why? Major reasons include underfunding, lack of knowledge, and lack of strategy. A board can weigh in on these areas.

It is not only a matter of protection but also of importance. When a company endures a well-publicized data breach or cyber-strike, that shakes the confidence of its customers and suppliers—and often its stock price.

Doing the things that help different stakeholders sleep at night is good in and of itself and for performance. As with all important questions, it is a matter of asking what needs to be done, by whom, and how.

Set priorities

No organization can do everything at once. With that in mind, the question for boards is: what should be done first? We believe the goal should be for management to develop a risk-based, business-backed cybersecurity strategy. That means starting by protecting the things that matter most— data privacy and availability for financial services, for example, or manufacturing processes. Once that is done, it is possible to move on to more sophisticated efforts, such as embedding security into products and systems development. It's important that the controls and processes that are put in place do not stifle internal innovation—something that can give cybersecurity efforts a bad rap. That's why these initiatives should be led by people with a business mindset.

In addition, boards should ensure that their organization is compiling a cyber-risk portfolio, and then review it regularly to ensure that decisions are made consistent with the risks identified. To get a sense of identifying

> *"No organization can do everything at once. With that in mind, the question for boards to ask is: what should be done first?*

priorities, the question is: If we obtained additional resources, how would we allocate them? One area to look at is third- and fourth-party risk, meaning important vendors that, if attacked, could bring devastating consequences to their customers.

The Technology Conundrum

It's a conundrum: the more companies use technology, the more they open themselves to new kinds of cyberattacks. The solution is to build robust and flexible defenses. This will be difficult, given the ever-changing regulatory environment and the ever-faster pace of technological progress.

But boards cannot leave this responsibility to the techies. Rather, they should embrace it through their oversight role. Working with the executive team, the board's role is to negotiate the tricky interplay around usability, security, and cost, and to ensure that the whole senior management team is prepared.

The best outcome, of course, is for nothing of material significance to happen. And the best way to get there is to act as if cybercriminals are always around the corner—because they are.

About the Author

Justin Greis | partner in McKinsey & Company's Chicago office

Justin Greis is a partner in McKinsey & Company's Chicago office. He leads McKinsey's cybersecurity work in North America within the Risk & Resilience Practice, focusing on cybersecurity transformation, the cloud, technology strategy, and digital transformation. Justin designs builds and activates secure and trusted digital transformations to help each organization accelerate its company missions and protect its purpose. Justin brings a wealth of experience across a wide variety of industries.

Before joining McKinsey, he served as a cybersecurity transformation leader both globally and within the Americas for a consulting firm, where he helped clients assess, improve, and

operate world-class cybersecurity programs. Justin was also a consultant in France, and before that, led the technology organization of a not-for-profit consulting group. Justin began his career as an entrepreneur after founding a digital consulting company that designed, built, and implemented dynamic websites, collaboration portals, and interactive digital service solutions.

About the Author

Daniel Wallance | a cybersecurity consultant, senior expert and associate partner with McKinsey & Company.

Daniel Wallance is a cybersecurity consultant, senior expert and associate partner with McKinsey & Company, having worked in the United States, the Middle East, and Europe for global corporations. He graduated from M.I.T. as a Fellow in the System Design & Management Program, jointly operated by the Sloan School of Management and the M.I.T. School of Engineering. Before M.I.T., Daniel was the operations director at a boutique investment firm where he designed the firm's business systems and processes, including redundant and secure enterprise-wide IT systems.