# Cyber resilience

## Creating competitive advantages and promoting trust

Businesses and employees alike are praising the newfound freedom afforded by working from home (also frequently referred to as remote work). The special circumstances surrounding the COVID-19 pandemic have given the economy, society, and not least schools and universities a push toward digitalization that had not been expected to come with such force or speed. Yet as this new digital workplace gains ground, misuse of these data flows and digital interfaces is experiencing an upswing as well. Anybody capable of strengthening their company's resilience against cyber crime while also raising awareness of the concept of cyber resilience at the highest level of management, however, will be able to gain a substantial competitive advantage.



**Trust in uncertain times**

Each and every type of economic activity is built on a foundation of trust, both trust in counterparties as well as trust in products, services, technology, settlement systems and intermediaries. A crisis, however, throws that trust off balance and triggers uncertainty, which in turn becomes a breeding ground for irrational behavior. This is something that cybercriminals cash in on. "Social engineering" is a term that describes sneaky fraud attempts and phishing activities that set a trap to lure in unsuspecting users.

The lightning-fast nature of the digital infrastructure, which was driven by the remote working network, makes it highly vulnerable to cyber attacks. After all: Employees' own personal devices are now suddenly being used for remote work. They hastily started using cloud services, accessing servers via VPN tunnels and conducting video conferences via unsecured data networks.

It goes to follow that the direct consequences of cyber attacks are often dramatic: weeks-long disruptions in operations, unauthorised payments, data leaks, privacy violations and even faulty products and services (which could actually be life threatening in a worst-case scenario).

Not only does this damage a company's reputation and tarnish customer confidence, but it also leads to other damage such as lost sales, legal costs and fines, delayed market entry, administrative costs for replacement and recovery, liability costs, as well as damages and compensation payments. The fact that some companies have been unable to recover and forced to file for bankruptcy is no secret.

**Do the board of directors and senior management know how to leverage cyber resilience as a competitive advantage?**

Yet how do companies and their boards of directors, as the top-most strategic management body, respond to these threats and how do they redirect this negative energy and transform it into a positive force for secure business management?

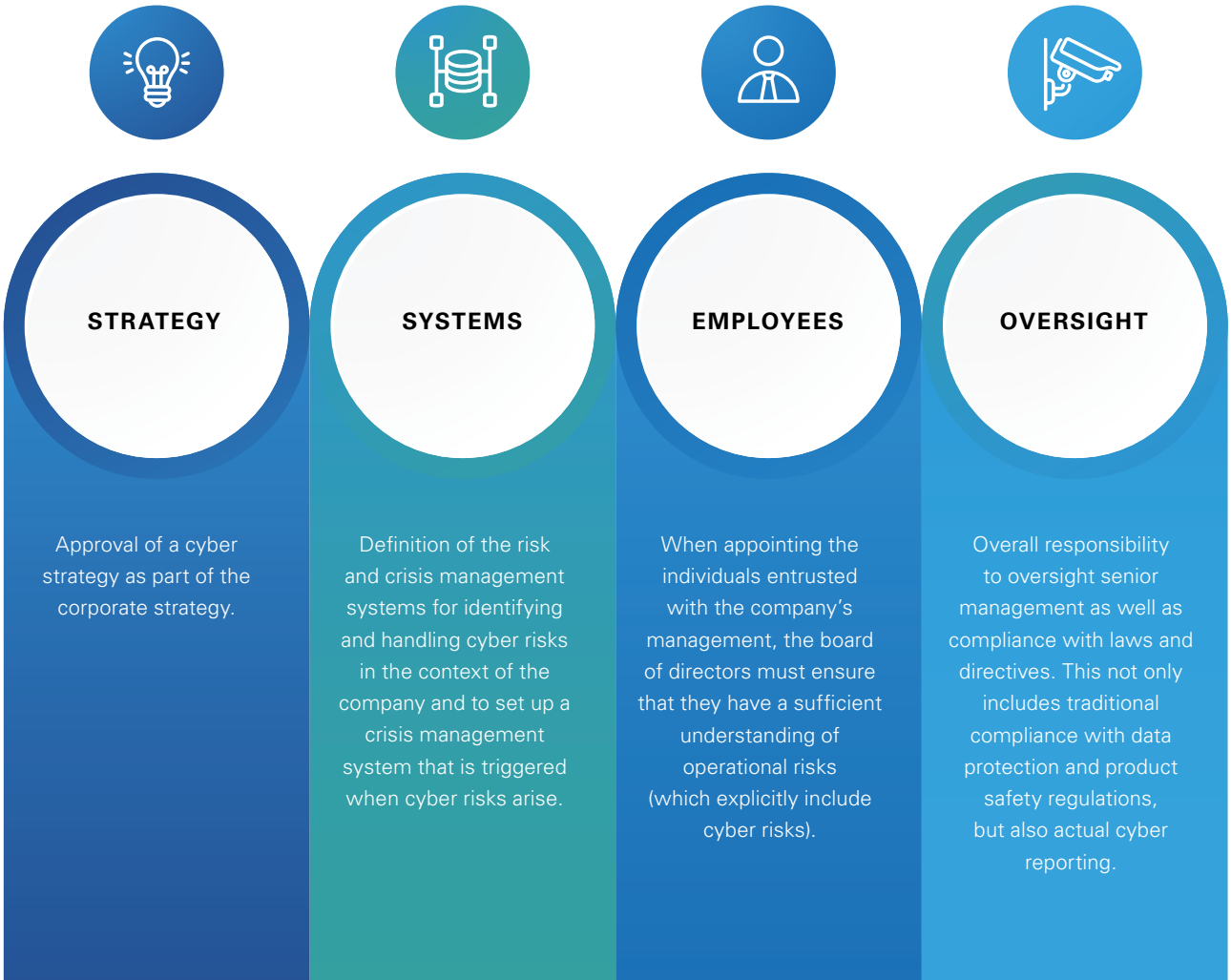
Besides the obvious operational risks, more advanced companies are recognizing that cyber resilience is a strategic opportunity for them to set themselves apart from the competition. The responsible management of cyber risks and even a well-handled cyber incident can boost the confidence of a company's stakeholders, regardless of whether those stakeholders are customers, investors, suppliers or regulatory authorities. What's more, a cyber-resilient company can confidently leverage digital technologies such as data analytics, artificial intelligence and cloud computing over the long term to improve its competitive position.

Businesses frequently view cyber risks as being an intangible, nearly unreal threat, in part because attacks such as these often exploit technical vulnerabilities that are enormously complex. It would be a fallacy, however, to conclude on this basis that cyber risks are inevitably technical risks that have to be managed by the IT organization. Considering the potential repercussions of a cyber attack, it becomes obvious that these attacks constitute operational risks and that board members and senior management must be well-versed with them.

A board of directors' main tasks can be broken down into the following four domains: strategy, systems, employees and monitoring. Its tasks with respect to the company's cyber resilience can also be extrapolated from those:

Establishing a system of governance within the company that





takes a risk-based approach to implementing cyber security measures is one vital step toward ensuring that these cyber resilience tasks are carried out effectively.

### Boosting a company's resilience

While efforts in the past have focused on technical measures designed to prevent attackers from penetrating the company's systems (key word here: firewall), much like the fortifications around a medieval city, modern cyber strategies are more broadly based. The reason for this is the automatic assumption that increased networking and integration between companies, suppliers and customers means that an attacker can and eventually will penetrate protected areas. Consequently, a modern cyber strategy is designed to identify intruders swiftly and prevent them from causing major damage, thus boosting a company's resilience against cyber attacks.

### Questions for the board of directors

One crucial aspect is the board of directors' understanding not only of cyber threats and their corresponding strategic opportunities and risks but also of how it influences the definition and implementation of strategic and operational measures, and this holds true both with respect to the board of directors' role as a corporate strategist and its supervisory function. Here, the board of directors should strive to paint a clear picture of the following:

1. Which new cyber threats or risks have arisen and how do they affect our organization?
2. Can our cyber resilience program adequately tackle the challenges that arise as a result of the current and future cyber risk situation?
3. Do we understand our current vulnerabilities (also with respect to our suppliers and service providers) and which processes do we have in place to address the identified cyber risks?
4. Is our organization sufficiently prepared to respond appropriately to an attack?
5. Which key risk and performance indicators should we monitor at the board of directors' level in order to perform our supervisory function?
6. Does our organization comply with legal and regulatory data storage requirements, such as data privacy?
7. Is cyber resilience one of the strategic issues discussed by the board of directors and when was the topic of cyber threats addressed most recently?
8. How do we transform our organization's reactive approach to cyber threats to one that is anticipatory?
9. Is our competition a step ahead of us? If so, does this give them a competitive advantage?



## Conclusion

Cyber risks are operational risks that could jeopardize a company's continued existence and a matter the board of directors has to focus on within the scope of the duties conferred to it by law. The board of directors should ensure that the company has a resilience-based cyber strategy, which also necessitates the rigorous implementation of basic measures to protect against cyber crime. This calls for a cyber reporting system geared toward the target audience that can create clarity regarding the status of a company's cyber risks and resilience. Not only does the board of directors have to manage the company's cyber risks, but also work together with senior management to assess how cyber resilience can be leveraged as a distinguishing characteristic and competitive advantage.

## Read more

Cyber resilience – The role of the board of directors in dealing with cyber risks (in German).
kpmg.ch/blc

**Dr. Matthias Bossardt**
Partner, Head of Cyber Security and Technology Risk
KPMG Switzerland

+41 58 249 36 98
mbossardt@kpmg.com



This article is part of the KPMG Board Leadership News. To receive this newsletter for board members three times a year, you can register here.

### About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc