Deloitte.

Cyber Point of View:

The role of executive management in cyber security

MAKING AN IMPACT THAT MATTERS since 1845

Leading the charge: As a business leader, you are at the forefront of cyber transformation

Despite significant investments in cyber security, large-scale breaches still occur with far-reaching consequences. There is something missing in the equation to better protect organisations.

What's missing is a fundamental shift in perspective. Cyber security must be seen not just as a technology issue, but as a business imperative. There needs to be a mindset shift whereby executive management steer their organisation's cyber efforts. A "technology dominant" approach has never and will never solve the problem, despite technological advancements.

Our daily lives are intertwined with digitisation, creating a web of technological interdependencies. Coupled with potent cybercrime and an increasingly polarised geopolitical landscape, businesses and governments face escalating risks. Such complexities result in persistent, significant risks, gaps and misunderstandings leading to breaches that erode customer trust and revenue – the foundation for any successful business.

The main consequences of a cyber incident are operational disruption and revenue loss with cybercrime costing an estimated $10.5 trillion in 2025[1]. Real-life examples of widespread IT incidents and outages demonstrate that when things go wrong, it directly impacts the business. Additionally, in many countries around the world, senior executives are being held personally accountable by law for major cyber incidents in their organisations and can face penalties such as criminal convictions. Business leaders have a crucial role in managing cyber security as an operational risk, integrating it into the company's overall resilience strategy.

These aspects show why you, as business leader, are at the forefront of the cyber transformation within your organisations. Business leaders need to take action and steer cyber security beyond technology risks to drive substantial change.

[1] https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/

What can you do?

As a business leader, you are the driving force in enhancing your organisation's overall cyber resilience. By posing the right questions to your security and technology teams, you can shift the focus to achieving full transparency on the organisation's genuine risk exposure and help these teams to find sustainable solutions that go beyond the implementation of tools.

In order to steer cyber beyond technology, there are five key areas where you play a critical role.

Be clear about what matters most to your business

Prioritisation is essential. It is not feasible or resource-efficient to attempt to protect everything at all times. As a business leader, you must lead and drive initiatives to determine which of your business services, products and assets are most vital and require prioritised protection and the ability to recover rapidly.

You are in the lead in defining acceptable levels of risk for cyber incidents, as your security and technology teams might struggle to fully understand the technicalities and priorities of your business operations. It remains therefore your responsibility, as a business leader, to set and establish clear protection priorities. Collaborate with your technology and security teams to explain to them what your business priorities are and what type of information is most critical. This will help you further support these teams in understanding the critical dependencies between business objectives and the underlying supporting architecture.

You should ask:

- What are our most important business services and underlying business processes?
- What are the supporting data assets for these business processes?
- What types of cyber-attacks present the most severe risks to the business?

Focus on reducing complexity

Simplicity is crucial, and the business is the driving force in achieving it. As a business leader you can drive the reduction of complexity by rationalising activities, standardising processes and finding the optimal balance of third-party diversification across the value chain. This enables your teams to streamline business applications, consolidate the technology stack and help standardise the supporting technology.

Simplifying your technology stack, processes, and data not only reduces your attack surface, thereby making it easier to protect, but also improves issue tracking, performance, and recovery from incidents. Here again, collaboration between the business and IT is essential to find the right balance between business requirements and cyber resilience considerations. For instance, consolidating vendors and suppliers can reduce complexity, while diversification can have a positive impact on your overall resilience.

You should ask:

- Are our evolving business demands introducing unnecessary complexity?
- How can we rationalise and standardise our business activities and supporting environment?
- How can we help IT to ensure a high degree of standardisation and automation is achieved at a technological level?

Improve resilience through modernisation

Resilience involves building strong, robust systems and processes that can withstand shocks. Cyber attacks are inevitable, and therefore it is essential to be prepared to effectively navigate them. A modular, self-contained architecture and high degree of automation can help to limit the impact of attacks, and to swiftly detect and contain threats, recover rapidly, and thereby minimise the overall damage. Having a modern architecture in place not only enhances security but also drives broader digital transformation. These principles allow for rapid deployment of digital improvements to meet business needs while ensuring organisational security.

You should ask:

- To what extent do we have an end-to-end overview of our business services and their supporting components so that we can understand their degree of resilience?
- What modernisation efforts have we undertaken in recent years and what investments are still needed to reach our resilience goals?
- Are we pushing the scenarios for stress testing far enough to give us confidence in our ability to withstand major cyber attacks?

Design security controls with the business users in mind

Cyber security is multi-dimensional and must be designed with business users in mind. As a leader, you must strive for a resilient environment where human errors do not lead to disaster. You should encourage your technologists to create a safe environment and ensure security operates seamlessly in the background, balancing security and business performance. Without this balance, employees under pressure may seek to bypass cumbersome controls to meet deadlines as they are inherently motivated to perform a good job.

From a technology perspective zero trust concepts can help significantly to create a more resilient environment. However, before adding further security controls, leaders should question whether existing ways of working could be changed to help increase security – for example by enhancing existing applications to enable data-sharing rather than creating shadow copies of data in spreadsheets that are shared via e-mail and shared network drives.

You should ask:

- What do we need to change to create a safe environment in which employee mistakes do not have catastrophic consequences?
- How are we balancing security measures with operational performance to ensure that security runs smoothly in the background without hindering productivity?
- Are we sufficiently looking into how we could change the way of working before we decide to introduce further security controls?

Support preparedness for cyber incidents

Preparation is key. Major cyber incidents very quickly transcend IT issues and become serious business challenges. An effective response requires a blend of technical cyber skills and experience of leading in times of crisis. As a business leader, you must ensure the response team has the right mix of business and technical skills, is well-trained, and has developed and regularly exercised response procedures and plans. In a cyber crisis, your organisation should be able to rely on its existing crisis management systems, processes, and teams. While the specific response will depend on the nature of the attack, your crisis management decision-making process and communications can guide the organisation effectively.

You should ask:

- What formal planning do we have in place to cope with a major cyber-attack and are we sufficiently staffed to respond effectively?
- Have we identified the relevant cyber crisis scenarios that need support from executives in preparation?
- Are we clear about the decision-making process in the event of a cyber crisis and do we have sufficient detailed protocols in place to accelerate both the response and the recovery?

Conclusion

A mix of technology reliance, geopolitical dynamics, underinvestment, and complexity has created a perfect storm. At Deloitte, we see cyber threats as a business risk that must be addressed with the full backing of business leaders at the executive level. In today's digital world, business success hinges on how well cyber is integrated into organisational initiatives. Cyber security does not have to be daunting, overly technical, or costly. There is also no need to chase the latest technological hypes, but rather to focus on getting the basics right first. As a business leader, you should direct resources towards activities that have the greatest impact on cyber security, including simplifying and modernising your business processes and applications.

Contacts

If you would like to know more about taking a holistic and business focused approach to cyber security contact us:

Sian Batra
Senior Manager
Cyber
smbatra@deloitte.ch

Florian Widmer
Partner
Cyber
fwwidmer@deloitte.ch

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte AG accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte AG is an affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/ch/about to learn more about our global network of member firms.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).