Guardians of digital trust
Cybersecurity Awareness Month

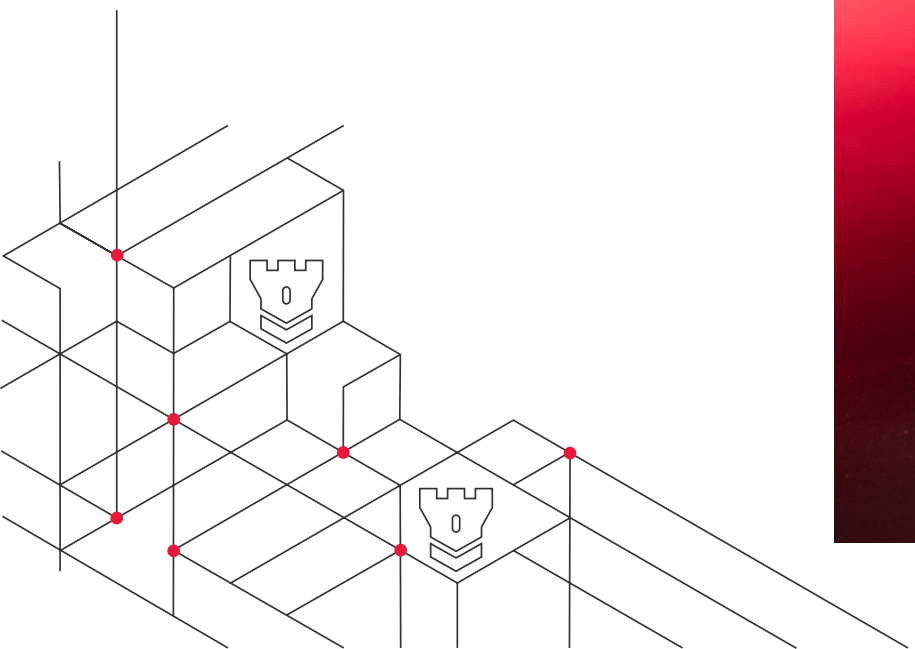
Understanding & enhancing cyber resilience

BDO

The growing divide between cyber resilient and non-cyber resilient organisations and how BDO can help

Through the course of 2024, business disrupting cyber events like ransomware have affected organisations across industries, from Belgium's Duvel Moortgat and Denmark's WS Audiology, to Transport for London, USA's Dicks Sporting Goods and Seattle's SeaTac Airport.

As cyber threats grow in complexity and frequency the gap between resilient and non-resilient organisations is widening. **Cyber resilience — the ability to maintain critical operations despite attacks** — has become essential. Recent incidents highlight the severe consequences on reputation, finances, operations and stakeholders.



Understanding Cyber Resilience

Cyber resilience extends beyond traditional cyber security, which focuses primarily on preventing attacks. Instead, it encompasses a holistic approach that includes **the ability to prepare for, respond to and recover from cyber incidents**. A cyber resilient organisation is not only capable of defending against attacks but also **ensuring continuity and quick recovery** when breaches occur.

Cyber resilience starts well before a potential incident. It demands a strategic approach to risk management, grounded in a comprehensive understanding of the potential threats. This informed risk management approach involves gathering and analysing all relevant information, learning from past incidents and making well-informed decisions that effectively minimise the organisation's exposure to future risks.

By adopting this approach, a mature security program operates seamlessly across the entire organisation, focusing on four critical pillars:

01

Prevention: Implementing robust cyber security measures to thwart attacks.

02

Detection: Rapidly identifying and assessing cyber threats.

03

Response: Effectively managing and mitigating the impact of cyber incidents.

04

Recovery: Restoring normal operations promptly and learning from incidents to improve future resilience.

What is the gap between cyber-resilient and non-cyber-resilient organisations?

A significant divide is growing between cyber resilient organisations and those that have yet to put adequate measures in place, according to the latest World Economic Forum[1] Global Cybersecurity Outlook.

The report states **a rise of cyber inequity**. 90% of executives surveyed at the World Economic Forum's Annual Meeting of Cybersecurity end 2023, stated urgent action was needed to address the divide.

Some organisations are more prepared and proactive than others in addressing cyber risks and building cyber resilience. According to the report, **only 17% of organisations are considered cyber resilient leaders, while 74% are still cyber resilient novices**. These leaders have the following dimensions in order:

- a clear and comprehensive cyber strategy
- a strong and supportive cyber culture
- the ability to attract talent
- a robust and agile cyber technology capability
- an effective and accountable cyber governance programme.

The novices, on the other hand, lack one or more of these dimensions and are more likely to suffer from cyber breaches, disruptions and losses.

[1] The cybersecurity trends leaders will need to navigate in 2024 | World Economic Forum (weforum.org)

Strategies to enhance your Cyber Resilience

To bridge the growing gap, there are several proactive steps organisations can take, such as:

01

Develop a cyber resilience plan:

Create a comprehensive plan that outlines preventive measures, incident response protocols, and recovery strategies. Ensure the plan aligns with the business strategy and objectives. Review and update it regularly to reflect the changing cyber landscape and business needs..

02

Invest in cyber technology:

For example, in attack surface and posture management, data security controls, security focused AI and machine learning. Technology that is fit for purpose, scalable, resilient, and secure. It also enables the organisation to detect, respond, and recover from cyber threats and incidents, while providing valuable resources the ability to offload and automate certain tasks.

03

Foster a cyber-aware culture:

Encourage a culture where cyber security is a shared responsibility, empowering all levels of the organisation.

04

Conduct regular training:

Educate employees on cyber security best practices and the importance of their role in maintaining cyber resilience. 95% of cyberattacks are due to human error, emphasising the tremendous need for in-house learning & development, at all levels.

05

Establish cyber governance:

Define the roles, responsibilities, and accountabilities of the board, management, and staff, and provide clear and consistent policies, standards, and procedures for cyber risk management and compliance monitoring, reporting and acting.

06

Perform regular audits and assessments:

Continuously assess cyber security measures and resilience strategies to identify and address vulnerabilities.

Global perspectives on cyber resilience

Global institutions such as governments and the World Economic Forum (WEF) recognise the critical need for cyber resilience and provide guidance to help organisations bolster their defences.

- **EU Directive on Security of Network and Information Systems (NIS2)**: Requires organisations in critical sectors like energy, transport, banking, and health to implement appropriate and proportional measures to manage risks to security.
- **EU Cybersecurity Act:** Aims to strengthen the security of digital products and services, promoting a high level of cyber resilience across member states.

Conclusion

The urgent need to prioritise cyber resilience is clear. By understanding its importance, leveraging global insights and implementing strategic measures, organisations can **safeguard their assets, maintain operational continuity and build trust** in an increasingly digital world.

It is no longer a question of if, but rather when your organisation will be at risk. No country or organisation will be spared from cybercrime, so it is crucial that global stakeholders work together to help close the gap.

How BDO can help

The fundamentals that cyber professionals have put in place are working. BDO's Global Cybersecurity practice is comprised of professionals from a diverse range of backgrounds. We are built to provide comprehensive, customised services for each client, focusing on your specific operating model, technical demands, regulatory environment and industry dynamics.

Whether it's financial services, healthcare, retail, natural resources, or any other industry – we understand your needs. Our global footprint extends to every corner of the globe and so does cybercrime. Let us help your organisation, wherever you are, to mitigate the cyber risks you're facing.

Sam Nelen
Senior Manager - BDO Advisory

$9.22 trillion
cost of cybercrime worldwide in 2023

The global cost of cybercrime is forecast to jump to
$23.84 trillion
by 2027,
up from $8.44 trillion in 2022 (Statista)

46%
share of organisations that pay ransom after a ransomware attack

1.9 million
global number of unique threats report by end users in 2023