




**Guardians of
digital trust**
Cybersecurity Awareness Month

A hand is shown from the top left, holding a red rectangular block. Below the hand, there is a gap in a wall of light-colored wooden blocks. The background is a gradient of light grey to white, with a dark grey diagonal shape on the left side.

The growing divide between cyber resilient and non-cyber resilient organisations

How can BDO help to
bridge the gap?

BDO

The growing divide between cyber resilient and non-cyber resilient organisations

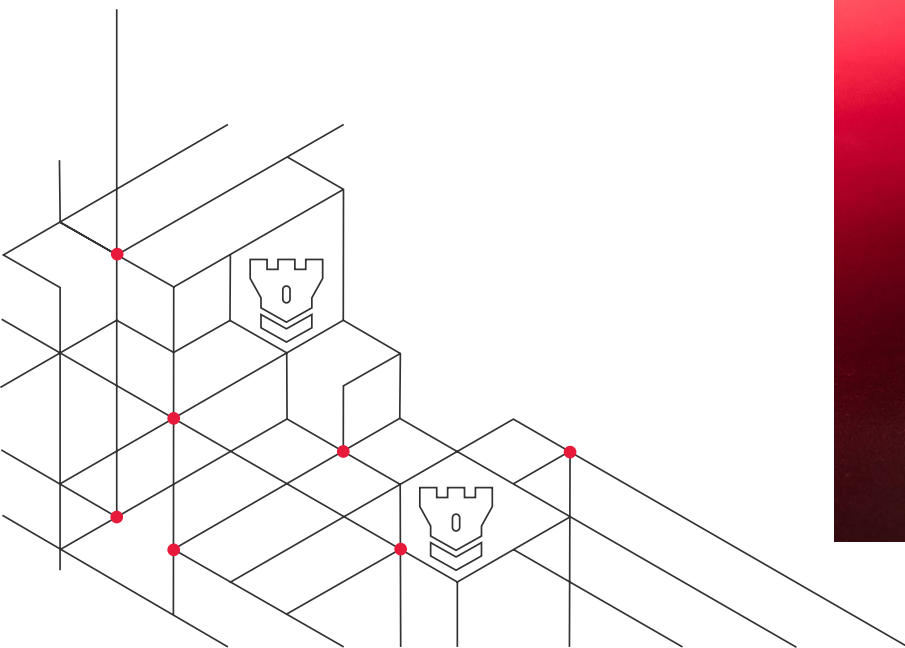
How can BDO help to bridge the gap?

Throughout 2024, cyber events such as ransomware attacks have disrupted organizations across various industries, including Denmark's WS Audiology, Transport for London, MGM and Caesars Casinos in the USA, Seattle's SeaTac Airport, and many others.

In the face of this increasing threat, cyber resilience - the ability to maintain operations despite cyberattacks - has become crucial.

With cyber threats growing more complex and frequent, the gap between organisations who are cyber resilient and organisations who are not resilient is expanding. Recent incidents highlight the significant effects of cyberattacks on reputation, finances, operations, and stakeholders' trust.

The World Economic Forum lists cyberattacks as one of the top global risks, and the COVID-19 pandemic has heightened organisational exposure to these risks.



Understanding Cyber Resilience

Cyber resilience extends beyond traditional cybersecurity, 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 and requires informed risk management, making decisions based on a thorough understanding of the risks. Informed risk management approach involves gathering and analysing all relevant information, learning from incidents and making well-informed decisions that minimise potential negative impacts on the organisation.

Essential elements of informed risk management are:

01

Risk identification - Recognising potential risks that could affect the organisation

02

Risk assessment - Evaluating the likelihood and impact of those risks

03

Risk prioritisation - Determining which risks need immediate attention based on their potential impact

04

Risk mitigation - Implementing a strategy to reduce or manage the identified risks

05

Continuous monitoring, regularly reviewing and updating the chosen risk management strategy to adapt new information or changing circumstances.



Using this risk management approach, the mature security programme operates continuously across the entire organisation including:

01

Prevention

Implementing robust cybersecurity 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 this growing divide between organisations who are cyber-resilient and those who are not?

A significant divide is growing between cyber resilient organisations and those that have yet to put adequate measures in place to manage cyber related risks, according to the latest World Economic Forum¹ [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.

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

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

The rise and adoption of new technologies will amplify already existing challenges, as will the widening gap in cyber skills and the talent shortage. Generative AI will undoubtedly advance cyberattacks in the next years; yet at the same time it can be used to help organisations better protect themselves.



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

The importance of cyber resilience

The significance of cyber resilience cannot be overstated in a world where technological advancements are adopted at an accelerated rate and where cyber threats are ubiquitous and increasingly sophisticated. The consequences of cyber incidents can be severe, ranging from financial losses and operational disruption to reputational damage and regulatory penalties.

01

Financial protection

Cyberattacks can lead to substantial financial losses. Cyber resilient organisations are better positioned to mitigate these costs through swift recovery and continued operations.

02

Operational continuity

Maintaining business operations during and after a cyberattack is crucial. Cyber resilience ensures critical functions can continue, minimising downtime and disruption.

03

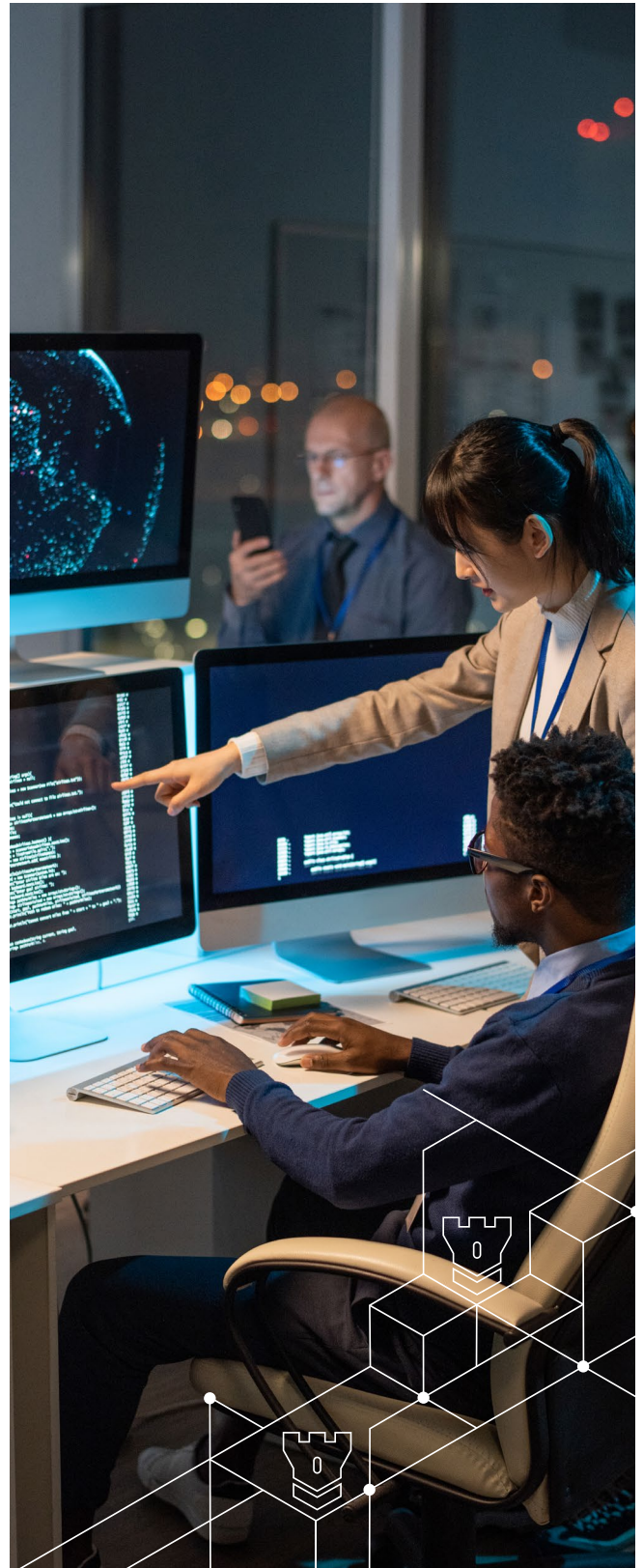
Reputational integrity

Trust is a valuable asset. Organisations who demonstrate cyber resilience are more likely to maintain customer trust and confidence.

04

Regulatory compliance

Many industries are subject to stringent regulations regarding data protection and cybersecurity. Cyber resilient organisations are better equipped to comply with these regulations and avoid penalties.



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.

01

Government Initiatives

- ▶ **NIST Cybersecurity Framework:** The U.S. National Institute of Standards and Technology (NIST) provides a comprehensive framework for improving cybersecurity practices, which is widely adopted across industries.
- ▶ **EU Directive on Security of Network and Information Systems (NIS2):** Organisations in critical sectors like energy, transport, banking, and health are going to be required to implement appropriate and proportional measures to manage risks to security.
- ▶ **EU Cyber Resilience Act:** The European Union's Cyber Resilience Act aims to strengthen the security of digital products and services, promoting a high level of cyber resilience across member states.
- ▶ **ASEAN** does not have a single, unified cybersecurity act or directive yet. However, it has developed a comprehensive Cybersecurity cooperation strategy for 2021-2025, focusing on advancing cyber readiness, harmonising regional cyber policies, enhancing trust in cyberspace and building regional capacity.
- ▶ The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) has integrated cybersecurity into its Digital Agenda.

02

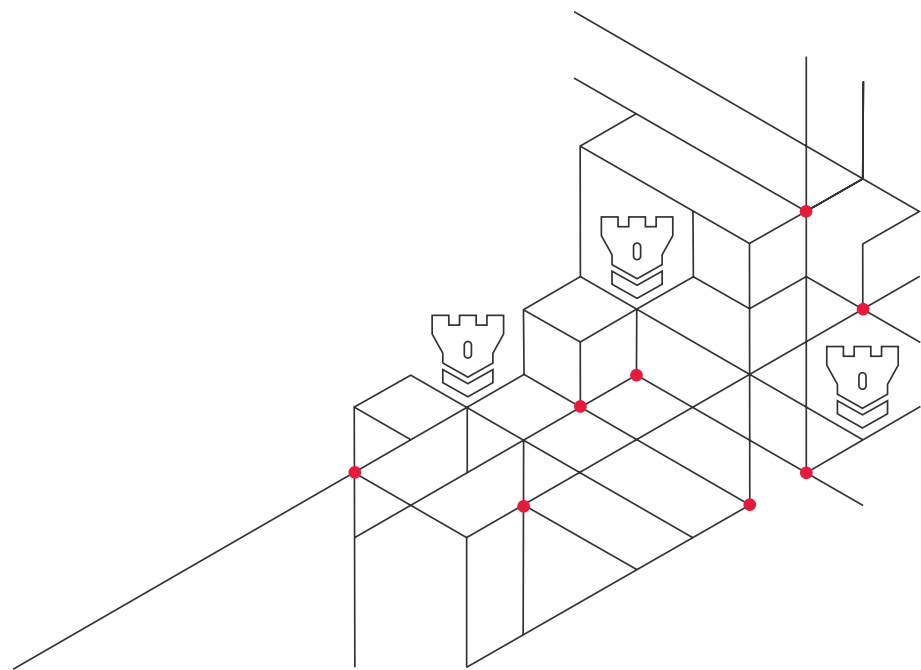
World Economic Forum (WEF)

- ▶ The WEF emphasises the importance of public-private partnerships in enhancing cyber resilience. Their reports highlight the need for a collaborative approach to tackle cyber threats and recommend best practices for building resilience.
- ▶ The WEF's Centre for Cybersecurity advocates for global cooperation and offers resources and forums for organisations to share knowledge and strategies on cyber resilience.

The new European directive Network and Information Security Directive 2 (NIS2) is set to become effective as early as October 2024. BDO has developed a clear NIS2 assessment tool that can provide you with insight into your current situation immediately. You can access this tool via the button below.



WWW.NIS2SURE.COM



Strategies to enhance cyber resilience

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

01

Develop a 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

Invest in cyber technology – such as attack surface and posture management, data security controls, security focused AI and machine learning and framework - that is fit for purpose, scalable, resilient, and secure, and that 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 cybersecurity is a shared responsibility, empowering all levels of the organisation.

04

Conduct regular training

Educate employees on cybersecurity 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

Establish cyber governance that defines the roles, responsibilities, and accountabilities of the board, management, and staff, and that provides 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 cybersecurity measures and resilience strategies to identify and address vulnerabilities.



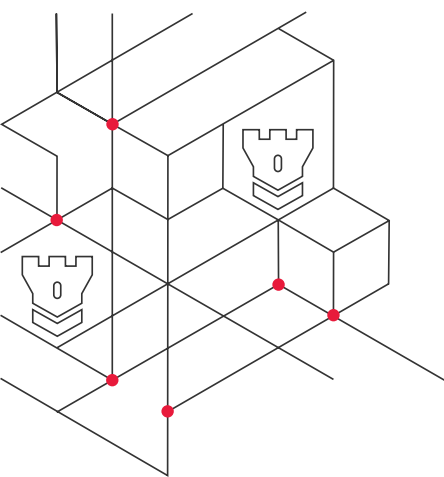
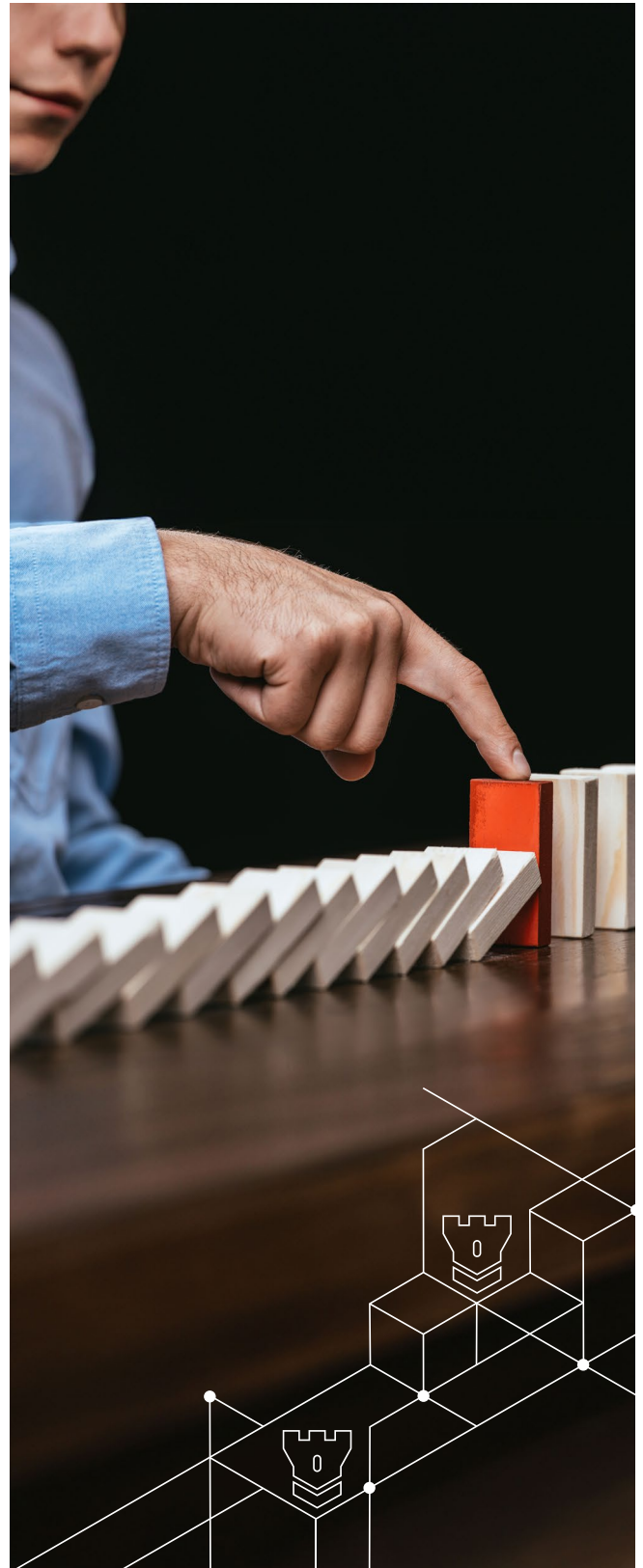
Conclusion

The growing divide between organisations who are cyber resilient and organisations who are not cyber resilient underscores the urgent need to prioritise and include cyber resilience as a key business objective. 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.

Cultivating best practices, attracting the right talent and implementing bespoke technology will help build the necessary resilience.

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.

As cyber threats continue to evolve, so too must our approaches to resilience, ensuring that we are always one step ahead in the cybersecurity landscape.



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, including experienced IT, operations, and data privacy consultants, as well as forensic technology, business advisory, and accounting practitioners.

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.



Rocco Galletto
Global Cybersecurity Leader



\$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)



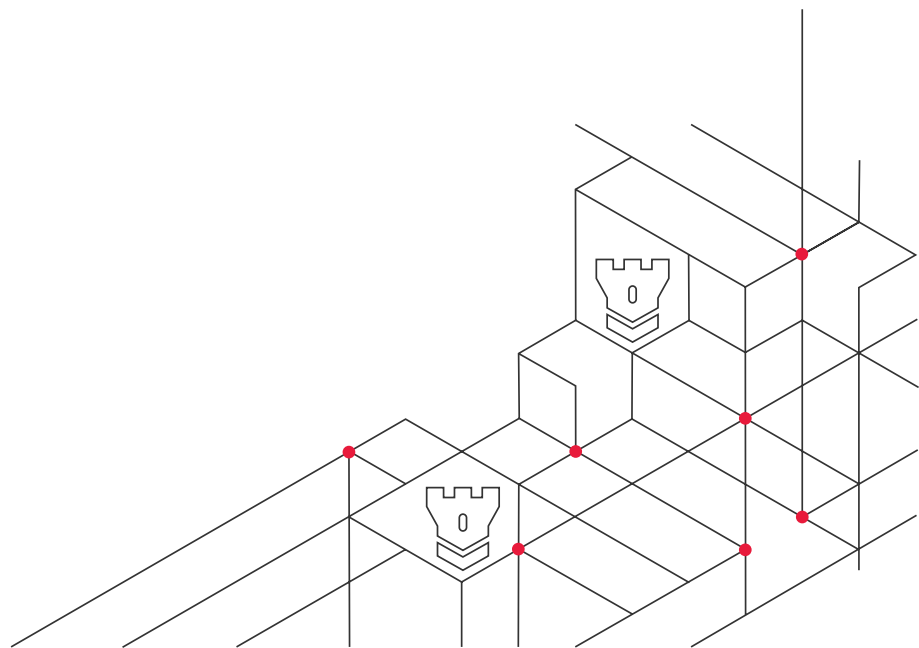
46%

share of organisations that pay ransom after a ransomware attack



1.9 million

global number of unique threats report by end users in 2023



'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

The BDO network is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the

BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV October 2024

