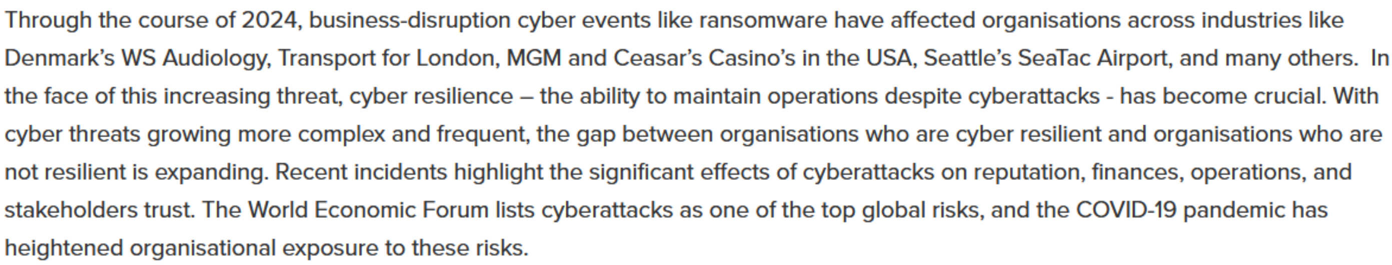
www.bdo.ie /en-gb/insights/2024/the-growing-divide-between-cyber-resilient-versus-non-cyber-resilient-organisations

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

How BDO can help to bridge the gap?

09 October 2024



Through the course of 2024, business-disruption cyber events like ransomware have affected organisations across industries like Denmark's WS Audiology, Transport for London, MGM and Ceasar's Casino's 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:

1. Risk identification – recognising potential risks that could affect the organisation
2. Risk assessment – evaluating the likelihood and impact of those risks
3. Risk prioritisation – determining which risks need immediate attention based on their potential impact
4. Risk mitigation – implementing a strategy to reduce or manage the identified risks
5. 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:

1. **Prevention**: Implementing robust cybersecurity measures to thwart attacks.

2. **Detection**: Rapidly identifying and assessing cyber threats.
3. **Response**: Effectively managing and mitigating the impact of cyber incidents.
4. **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 organisations who are not cyber-resilient?

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 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. 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.

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.

1. **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.
2. **Operational Continuity**: Maintaining business operations during and after a cyberattack is crucial. Cyber resilience ensures critical functions can continue, minimising downtime and disruption.
3. **Reputational Integrity**: Trust is a valuable asset. Organisations who demonstrate cyber resilience are more likely to maintain customer trust and confidence.
4. **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.

1. **Government Initiatives**:
    1. 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.
    2. 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.
    3. EU Cybersecurity Act: The European Union's Cybersecurity Act aims to strengthen the security of digital products and services, promoting a high level of cyber resilience across member states.
    4. 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.
    5. The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) has integrated cybersecurity into its Digital Agenda.
2. **World Economic Forum (WEF)**:
    1. 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.
    2. 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.

Strategies to enhance Cyber Resilience

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

1. **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.
2. **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.
3. **Foster a cyber-aware culture**: Encourage a culture where cybersecurity is a shared responsibility, empowering all levels of the organisation.
4. **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.
5. **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.
6. **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?

At BDO, our Cyber Health Check Service provides a robust security assessment by leveraging the CIS security control framework and scrutinises your system’s compliance configurations. Our goal is to help you assert control over your system’s security, increase visibility into potential issues, and facilitate prompt responses in both on-premises and hybrid environments on a scalable level. Our comprehensive assessment goes beyond merely identifying your risk profile. It also targets flawed processes that might contribute to your risk, offering you a detailed report that doesn’t just highlight vulnerabilities but provides actionable steps to rectify them. Furthermore, our Health Check package includes an external vulnerability assessment. This gives you an immediate overview of potential weaknesses across your web presence, allowing you to identify and address vulnerabilities before they can be exploited. This service is designed to enable and empower you to take proactive steps towards securing your digital assets. Also included in your report:

- Servers running out of date software
- Services that are exposed to the internet and should be behind your firewall
- Compromised credentials for sale.

Key figures:

- $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

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