BEYOND blue

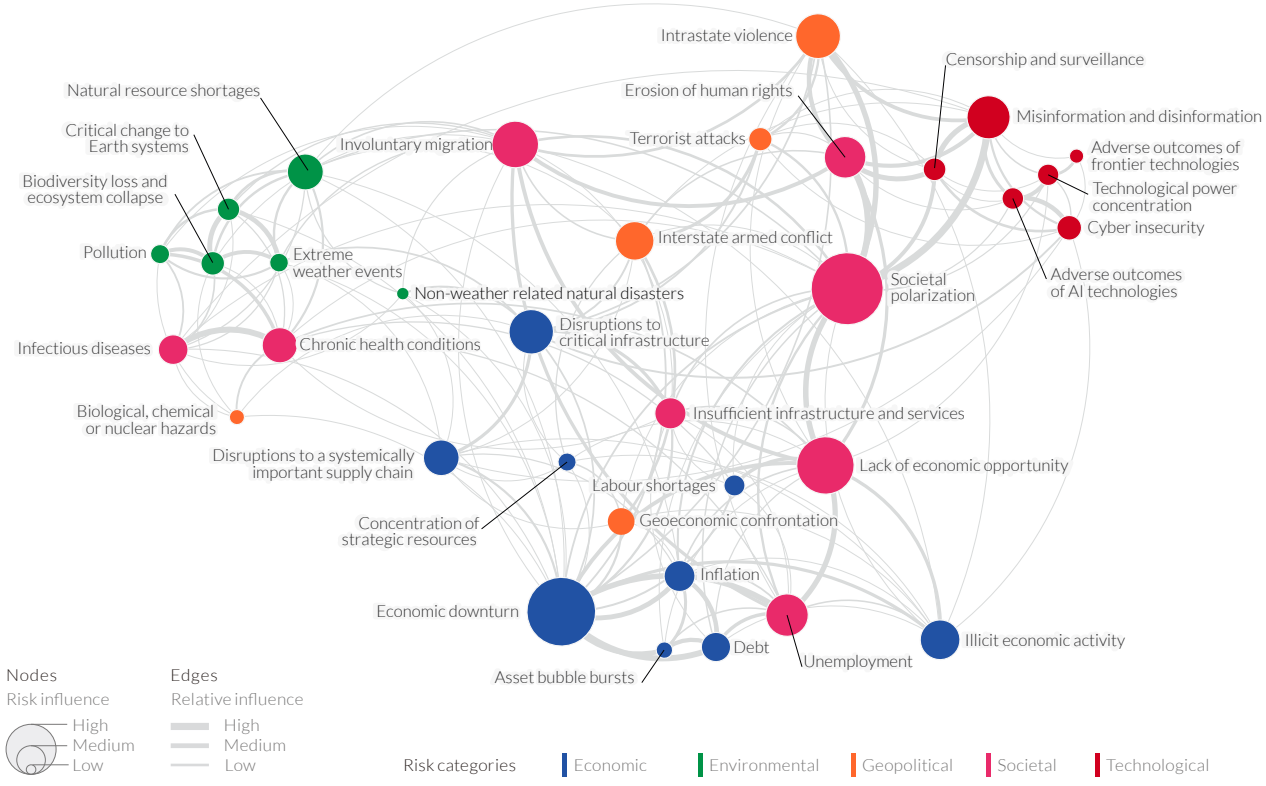
IT'S ALL ABOUT CONTEXT

The world has become increasingly complex, interconnected, and dependent on a diverse ecosystem of suppliers and service providers. The cyber threat landscape is changing rapidly driven by technology advances, global instability and geopolitical risk - as the World Economic Forum's global risk report (Figure 1) shows only too clearly.

The UK Government's Cyber Security Breaches Survey of 2024 reports that half of businesses and around a third of charities have experienced some form of cyber security breach or attack in the last twelve months.

Cyber crises have risen to the forefront of threats facing public and private institutions, with large scale events such as the MOVEit hack, Ticketmaster breach and Crowdstrike's outage, drawing attention to the pervasive and destabilising nature of cyber incidents.

The increase in the frequency and impact of cyber crises mean it is essential for organisations to implement strategies to anticipate, respond, and recover from significant disruptions.



Source
World Economic Forum Global Risks Perception Survey 2023-2024.

Figure 1 (World Economic Forum, 2024, p.9)

This view is also echoed by the National Cyber Security Centre (NCSC), whose CEO recently called for "greater global resilience in the face of increasingly complex and aggressive online security threats". The NCSC support organisations of all sizes in their preparedness and response to a cyber incidents. One of the ways that the NCSC advises organisations to improve their resiliency is through crisis exercising.

The NCSC are not the only organisation emphasising the need for increased resilience. Regulators from many sectors are becoming more vocal in their requirements for organisations to be able to provide evidence of their resiliency - exercising is a key part of that evidence.

In financial services, the UK's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) have released Operational Resilience regulations, with a deadline of March 2025 for implementation. The FCA and PRA both require that firms use severe but plausible scenarios to test their response capabilities. Financial services with entities operating in the EU are also faced with The Digital Operational Resilience Act (DORA), mandating that firms ensure robust testing of ICT systems to ensure the effectiveness of the controls in place.

The interdependence of sectors, and of the public and private organisations in each sector, has resulted in an environment in which a disruption to a single service can ripple across industries. Disruptions have the potential to affect operations, economies, and essential services on a global scale.

In recognition of this, those who play a critical role in financial services supply chains, who traditionally have fallen outside of the regulatory ringfence, are being pulled into it by the UK regulators. The FCA and PRA have recently published a joint regulation requiring 'critical third parties' to the UK financial sector to demonstrate resiliency in the event they are impacted by a severe but plausible scenario. It is likely that the forthcoming Cyber Security and Resilience bill will extend this coverage to third parties supporting other critical infrastructure sectors.

For critical infrastructure in the EU, the Critical Entities Resilience Directive (CER) is also in place, requiring essential service providers to strengthen their resilience against all hazards and stress test themselves to test their preparedness. Additionally, critical entities are also considered essential entities for the purposes of the Network & Information Security Directive (NIS2). NIS 2 focuses on cybersecurity resilience encompassing requirements for audit and testing.

As we move forward, regulation will grow demanding that an increasing number of third parties demonstrate their resiliency to critical infrastructure clients and regulators alike.

FAIL TO PREPARE, PREPARE TO FAIL

Crisis or incident plans can provide a level of comfort to stakeholders and leaders that their organisation is resilient. However, without adequately exercising their plans, organisations have little assurance that they will work in practice. Crisis exercises allow organisations to respond to a crisis or disruptive event in a way that enables board level, managerial and operational level colleagues to apply their crisis management plans in a safe learning environment. Effective crisis management is underpinned by culture and a consistent, open-minded approach to continuous improvement through training and exercising. Having a crisis management team that is dynamic, and fully aware of their individual and overall responsibilities as a cohesive function could be the difference between an organisation staying afloat and ceasing to exist.

Choosing which scenarios to exercise should be informed by threat intelligence to reflect the organisations current threat landscape. Scenarios can be exercised in several ways, from tabletop, live real-time simulation, or a hybrid approach. No matter the approach, one of the objectives should be to educate participants on the unique attributes of a cyber crisis and make the exercise as realistic as possible. There is a fine balance between applying enough pressure for teams to experience the stress of crisis response, whilst fostering an environment that allows participants to ask questions, make mistakes and learn from the experience.

One of the biggest misses following actual crises is to conduct a thorough debrief to help better prepare the organisation to deal with future incident and crises. The debrief and subsequent reported recommendations are vital to turning ‘lessons identified’ into ‘lessons learned’. The implementation of these requires investment and buy-in from stakeholders and executives to provide the resources required.

FORWARD LOOK

The World Economic Forum's (WEF) recently published a report on the importance of cyber resilience stated that "to thrive in the digital age, organizations must prioritize cyber resilience as a strategic leadership issue, enabling them to protect core business objectives and promote long-term growth". With AI-generated misinformation and disinformation and cyber-attacks sitting at number two and four of WEF's Global Risks of 2024 respectively, it is clear that cyber related risks will remain a significant concern for years to come. Moreover, central to the future of cyber risk and resilience is the recognition of cyber as a compounding force that intensifies risks across the broader landscape. As such, while cyber is a significant risk on its own, it also acts as a risk multiplier, amplifying the impact of other threats such as geopolitical conflict, economic instability, and natural disasters.

The cyber threat could therefore be a key feature of many disruptions that organisations must anticipate. In preparation for this, the resulting risks cannot be treated in isolation or within organisational silos as they are intrinsically linked and have the capability to disrupt every part of the organisation. Cyber is not just a problem for the IT team to address.

Whilst this vast and often unknown cyber risk landscape may seem daunting for organisations to navigate, David Ferbrache OBE, Managing Director of Beyond Blue highlights that "Exercising is a vital tool for combatting this uncertainty. Organisations may not be able to predict how they will be hit or by whom, but they can hone their responses and better prepare for the hard choices they will face in a major incident".

WHY

BEYOND blue

If you are seeking to future-proof your organisation against evolving cyber risks, Beyond Blue has over 250 years of combined experience in all thing's cyber and resilience. We are one of the NCSC's 33 UK Assured Service Providers for Cyber Incident Exercising (CIE), crisis exercising and resilience services to ensure your organisation can respond effectively, recover quickly, and adapt confidently to cyber challenges. To find out more about Beyond Blue's boutique consultancy, take a look at our website or get in touch at enquiries@beyondblue.tech.