In collaboration with
the University of Oxford

WORLD ECONOMIC FORUM

Unpacking Cyber Resilience

WHITE PAPER

NOVEMBER 2024

Images: Getty Images

Contents

Foreword

Sadie Creese
Professor of Cybersecurity; Director and Technical Board Chair, Global Cyber Security Capacity Centre, University of Oxford

Akshay Joshi
Head, Centre for Cybersecurity, World Economic Forum

Resilience in the face of cyber risk is a critical objective for any organization dependent on digital technologies and data. This places it on the radar for almost all business leaders in 2024. The globalization of our supply chains, the complexity of technology stacks and the continued appetite to innovate with digital have led to continued aggregation of systemic cyber risk.

Effective cyber resilience is complex. How we achieve it and the controls we use are highly context dependent; what works in the face of one type of threat may not work as well for another. For example, defending against ransomware is very different from defending against denial of service, and defending against accidental failures in a system requires different solutions from defending against a malign threat actor seeking to attack for reasons of sabotage, theft or financial gain.

Business or mission priorities should guide decisions on which response strategies to take in the face of attack. What to address first and how? What can be switched off, and what must stay operational even if services are degraded? Who is allowed to continue accessing the system, and who must be denied further access until the incident is resolved? How much of the business infrastructure is affected?

We practise cyber resilience to achieve business resilience. Numerous international standards and frameworks stand out as examples of good cybersecurity practice that can guide our investments. However, handling an incident and making decisions that best suit the operational context require practical actions. In an era with significant capacity gaps in the workforce's cyber-risk management skills, there is an urgent need to learn the lessons from the front lines and to systematize and share them in order to raise the general baseline.

This white paper unpacks the concept of cyber resilience, an important precursor to understanding effective action. Organizations need to consider their cyber-resilience levels from a holistic perspective, including the processes involved in case of a cyber incident and its impact on the tangible and intangible assets, as well as assessing how different areas of the business are affected and which processes should be in place to reduce panic and facilitate fast decisions in stressful moments. The challenge of building a cyber-resilient ecosystem can seem overwhelming, but learning from cybersecurity experts is the first step in breaking down barriers and taking effective actions towards a cyber-resilient society.

Executive summary

Cyber resilience matters.

Cyber risks are among an organization's highest priorities, and the threat keeps increasing, a fact that has been highlighted by the World Economic Forum's *Global Risks Report* since early 2020.

The challenge is dynamic. The evolution of the digital landscape and infrastructure, driven by the disruption of connectivity and emerging technologies, has vastly complexified the threat landscape and the cyber risks organizations face. Recognizing that individuals and organizations cannot prevent all malicious attacks or cyber failures, while embracing the opportunities that digitalization brings, has led to the rise of cyber resilience.

The digital transformation continuously reshapes and evolves businesses and governments. The primary goals and objectives of organizations are often supported by business processes that are critically reliant on digital technology, commonly without any analogue alternatives. While primary goals and objectives will differ between organizations, they will always include the protection of critical service delivery, stakeholder confidence and the principle assets that underpin value and position in the market. Achieving true cyber resilience is fundamentally a leadership issue, and is paramount to retaining shareholder value.[1]

This paper is the result of collaboration between the World Economic Forum, the University of Oxford Global Cybersecurity Capacity Centre and a working group of industry cyber leaders who came together to unpack cyber resilience and provide a broader strategic definition that considers a wide array of risk scenarios key to an organization's primary goals and objectives. These include risks arising from supply-chain disruptions, attacks on trust and reputation and legal liabilities from data breaches.[2]

It is imperative that organizations prepare for significant cyber incidents. Continuous investment in cyber-resilience capabilities enables organizations to maintain their primary goals and objectives in the face of cyberattacks and other cyber incidents, making sure their growth potential is undamaged. This entails ensuring that operations can be recovered, the impact on internal and external stakeholders ameliorated, financial and trading performance restored, tangible and intangible assets protected and new potential for growth unlocked.

Organizations need to develop adaptable strategies and use shared insights from the practical experience of industry peers to navigate the complexities of the cyber landscape. Proactive collaboration and continuous learning will play a vital role in delivering cyber resilience.

Cyber resilience is an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives.

1 Why cyber resilience matters

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.

Investing in cyber resilience reduces the economic costs of cyber events, while contributing to improvement in an organization's reputation.

The scale, scope and significance of online connectivity is a defining feature of the digital age. Close to 70% of the world's population can access the internet and online services,[3] and digital technologies and processes have become central to everyday life as well as to the work of governments, businesses and societies globally.

Cyber resilience matters and, as this white paper sets out, achieving true cyber resilience is fundamentally a leadership issue.

The very centrality of digital systems and services to the economy and society means that organizations and individuals can experience significant harm or losses should these systems be compromised. What constitutes a significant cyber incident varies for each organization, but is generally one that has the potential to severely affect its operations, finances or reputation.

Damage to integrity – accuracy of information – whether due to sabotage or accidents, can have ramifications for entire business ecosystems and supply chains. Undermining confidentiality – a lack of restrictions on information access and disclosure – can endanger individual privacy and compromise intellectual property restrictions and the government's national security protections. Service instability and lack of availability – unreliable access to and use of information by authorized parties – can result in reduced revenues and in critical environments can cause important functions to fail. What is more, frequent failures of this kind could erode confidence in the role of digital transformation in society.

For these reasons, governments and businesses are becoming increasingly aware of the need to maintain and secure digital systems and to limit the impact of cyber incidents on their primary goals and objectives, whether caused by technical glitches, accidents, unplanned shutdowns or natural disasters.

With socio-technological advances and increasing dependence on cyberspace and the digital technologies that underpin it, the understanding of the practice of cybersecurity has evolved from a focus on basic security controls to prioritizing information security and assurance and increasingly cyber resilience. In today's rapidly shifting technology and threat landscape, organizations need to operate on the basis that significant cyber incidents will occur. Those cyber incidents have the capacity not only to take down a computer or device but also to disrupt an entire organization and significantly affect society. Therefore, keeping a business operating effectively, making it resilient in the face of disruption, must include achieving cyber resilience.

Being cyber resilient enables an organization to minimize the impact of significant cyber incidents on its primary goals and objectives, allowing it to maintain critical services, safeguard stakeholder confidence and protect strategic value.

Thinking about cyber resilience in these terms underlines the point that it is about more than just restoring business-as-usual operations. An organization's primary goals and objectives could include its ability to deliver critical services, to maintain market share, to increase shareholder value, to build confidence in the brand, among other things; in other words, everything that is required to sustain the health of the organization.

However, cyber resilience is not just a protective control. The cyber-resilient digital transformation of businesses and societies has the potential to drive entrepreneurial innovation, productivity and economic growth. To securely and sustainably capitalize on digital opportunities, organizations must prioritize cyber resilience, not just as an IT matter but as a core strategic issue.

Investing in cyber resilience reduces the economic costs of cyber events (data breaches and intellectual property loss, for example), while contributing to improvement in an organization's reputation (fulfilment of customer requirements and branding secure products, for example).[4] Moreover, by some estimates, more resilient companies generate shareholder returns that are around 50% higher than those of their less resilient peers.[5] Failing to build cyber resilience can disrupt business operations and even lead to the organization's

A cyber-aware boardroom is far better prepared to handle incidents, to minimize losses and to oversee the delivery of an organizational culture of cyber resilience.

collapse.[6] The impact on small and medium-sized enterprises (SMEs) can be particularly severe, with some estimates suggesting that 60% of SMEs falling victim to a cyberattack close down within six months.[7]

Leadership plays a crucial role in driving cyber resilience throughout an organization. It requires more than just a capable cybersecurity team; it demands a culture in which cyber resilience is prioritized in key decisions made at the top. Effective leaders actively engage with cybersecurity strategies, recognizing that it is a core business function just as vital as legal and financial issues, and that managing operational risks will inherently require a component of cyber risk. A cyber-aware boardroom is far better prepared to handle incidents, to minimize losses and to oversee the delivery of an organizational culture of cyber resilience.

Board of director organizations from around the world including the National Association of Corporate Directors in the United States, the European Conference of Directors' Associations, the Japanese Business Federation and others have recently released guidance advocating for a more comprehensive view of cybersecurity that promotes a more resilience-based understanding of the issue.[8]

Moreover, independent research from the World Economic Forum, the Massachusetts Institute of Technology (MIT) and PricewaterhouseCoopers (PwC) has documented that this broader construction of what counts as effective cyber practice at the board level results in significant security outcomes, including better cyber-risk management and closer alignment of cyber issues with business outcomes, enabling the development of a culture of security and potentially reducing cyber events by as much as 85%.[9,10]

By building and exemplifying a cyber-resilience mindset, promoting proactive approaches, staying informed on emerging threats and understanding the broader business impact of cyber risks, top executives can ensure that their organizations remain resilient and well prepared for potential challenges.

The concept of cyber resilience might appear to be common sense, but it has not always been given the priority it requires. Businesses and governments struggle to minimize the impact on their primary objectives and deliver their services in the face of cyber incidents. Resilience is far too important to be left to chance, yet too many organizations have fallen short in their preparations. This highlights the need to fully unpack the concept of cyber resilience and develop a common understanding of its significance.

2 Unpacking cyber resilience

Cyber resilience is an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives.

In today's digital landscape, understanding the concept of cyber resilience and its scope is crucial for organizations aiming to safeguard their operations and reputation. Cyber resilience is defined as an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives. This approach encourages them to consider the many ways in which they are vulnerable and how they can limit the potential impacts – whether these arise from their use of information or operational technology, or from the use of digital technology by others in their supply chain or wider ecosystem.

2.1 The evolution of cyber resilience

Cybersecurity encompasses a wide spectrum of practices, from the protection of data, information and networks to detection and mitigation of cyberattacks, as well as less technical concepts relevant to risk management and the development of policies and legislation. It is now considered fundamental to the development of digitalized economies.[11,12,13]

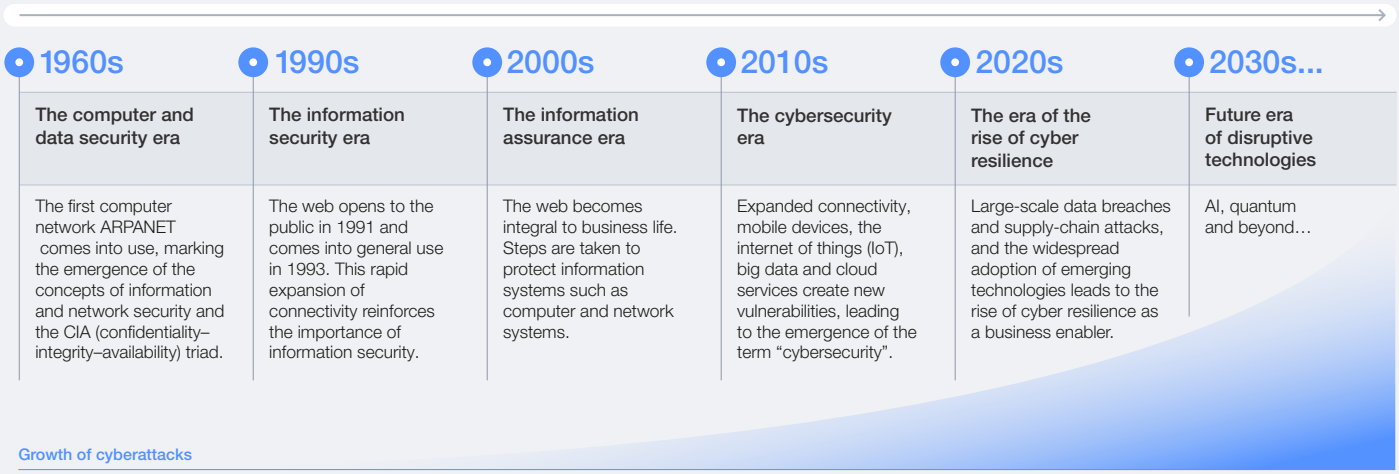
In tandem with the digital revolution, cybersecurity has evolved into a multifaceted field and become a point of attention in various disciplines. In the past 15 years in particular, cybersecurity has been on the front pages of newspapers, in online articles and on social media due to the rising number of material cyber incidents. Of course, the threat itself has existed for much longer than that, with the first experimental development of a computer worm dating back to 1971.[14]

> A shift of focus from cybersecurity to the broader concept of cyber resilience is changing front-line practices in leading organizations.

While cyber resilience has been practised by more sophisticated professionals and more highly regulated sectors since the 2010s, it has emerged as a mainstream concept far more recently. The increasing damage caused by disruptive attacks and data breaches to the core operations of victim organizations, along with substantial harm to their reputations and financial performance, has brought cyber resilience to the attention of boards of directors in most sectors of the economy. This realization has created a shift of focus from cybersecurity to the broader concept of cyber resilience and is changing front-line practices in leading organizations.

Describing the journey from data security to cyber resilience sheds light on the evolution of threats and challenges posed by the digital era and highlights how cybersecurity practices have been shaped to protect society from these threats.

FIGURE 1 | **The evolution from information security to cyber resilience**



Theft by computer (1960), early evidence of criminals exploring vulnerabilities to steal and compromise data from shared resources.

The Creeper virus (1971), the first computer virus, affected all 28 machines running the TENEX operating system.

The Morris worm (1988) caused widespread damage, deleting the resources of 6,000 machines.

The Melissa virus (1999) overloaded the email servers of more than 300 businesses and government agencies, causing $80 million in damage.

The ILOVEYOU virus (2000) caused significant disruption and $15 billion in damage worldwide.

The US Department of Defense (DoD) and NASA hack (2000) placed NASA systems offline for 21 days.

The Slammer worm (2003) caused a denial of service affecting internet hosts and slowing the internet, while infecting more than 75,000 victims in less than 10 minutes.

The Estonia cyberattack (2007) where a series of targeted attacks took down Estonian banks, media outlets and government bodies.

Stuxnet (2010) was the first attack targeting industrial control systems (ICS) to have physical consequences.

The Sony PlayStation hack (2011) stole 77 million account holders' personal information.

Shammon malware (2012) affected several IT machines, disrupting industrial operations for more than two weeks.

BlackEnergy (2015) targeted Ukraine's power grid, causing significant power outages.

Triton (2017) was a malicious code that disabled safety systems to prevent industrial and physical accidents, costing $1 trillion.

NotPetya ransomware (2017) cost multiple large organizations more than $10 billion.

WannaCry ransomware (2017) infected more than 230,000 computers, causing billions of dollars of damage.

The Equifax data breach (2017) affected 143 million customers and cost $1.4 billion in recovery.

Solarwinds (2020) supplied malicious code to 18,000 customers, with 11% of revenue lost.

The Irish Health Service Executive attack (2021) caused disruption for several months, with a total response cost exceeding €100 million.

Colonial Pipeline ransomware (2021) crippled fuel supplies to 50 million Americans for 11 days, costing $4.4 million and brand damage.

Log4J (2021) peaked at 100 attacks every minute, affecting more than 40% of all business networks globally.

The Okta data breach (2022) affected 366 customers in just five days (16–21 January), leading to a $2 billion market cap loss.

The MOVEit transfer data breach (2023) affected 94 million users, more than 2,500 businesses and caused more than $10 billion in damage.

Note: Illustrative view, not exhaustive.

Source: Analysis by the World Economic Forum and the University of Oxford

2.2 The concept of cyber resilience

Cyber resilience is not the same thing as cybersecurity; however, cybersecurity is essential to achieving cyber resilience.

Numerous definitions of cyber resilience exist (see Section A2 of the Appendix). Of these, the most relevant for the purposes of this paper is that provided by the National Institute of Standards and Technology (NIST), namely: "The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."[15] Even here, the use of the term "cyber" as in "cyber resources" and "contested cyber environment" is open to interpretation and could lead organizations to take too narrow an approach to managing their risk exposure.

When considering cyber resilience, it is important to take a broad view of what cyber risk is. Cyber risk can refer to any risk that arises from an organization's use of information services and digital technology or from their use by others in the supply chain or within the wider business environment. The advantage of this definition is that it allows for a wider range of "cyber"-related risk scenarios.

> Ultimately, there is no such thing as 100% cybersecurity. Organizations need to act on the basis that significant cyber incidents will occur.

For example:

- Impacts that might arise from cyber events in an organization's wider supply chain (such as disruption to a critical service on which the organization depends – this need not be a digital service)
- Impacts other than operational business interruptions; for example, legal and financial liabilities arising from data breach or loss of integrity in data for which the organization is accountable
- Risks related to the manipulation of the cyber domain; for example, promotion of disinformation about an organization or misuse of an organization's online platforms to commit financial fraud or incite crime
- Strategic and reputational risks associated with a failure to demonstrate a duty of care to customers, employees or other stakeholders
- Risks relating to operational technology as well as to information technology
- Risks relating to human life (safety- and security-critical systems)

Organizations need to consider the many ways in which they are exposed to cyber risk and how they can limit potential impacts – whether by investing in operational cybersecurity controls, by changing business processes or by taking steps to reduce legal or regulatory liability. This might involve ensuring that business-as-usual operations can continue when system outages occur or limiting the harm that could arise from a compromise to the confidentiality of data. Cyber resilience focuses on limiting the impact, which could be short-term or long-term, operational or strategic, financial or reputational or a combination of these factors.

Organizations also need to assess their exposure to risks within the supply chain. Where it is not possible to achieve the required level of assurance of security and resilience within the supply chain, it may be necessary to consider how dependencies can be designed out or how incidents within the supply chain can otherwise be contained. This assessment will require a continuous monitoring of the threat environment in order to understand the likelihood of the supply chain being compromised. When considering those risks, organizations will also need to turn inwards and assess whether supply-chain compromises could have severe enough consequences to require strengthening safeguards against these propagating risks.

Many organizations have well-developed business continuity plans, which, in theory, should address events such as IT outages or physical damage to IT or operational technology (OT) infrastructure. However, these plans must be thoroughly tested, as cyberattacks can have qualitatively different impacts on technology. The controls that might be effective when handling a benign or accidental failure may not be effective when dealing with incidents caused by malign attacks. In the malign case, the attack will very often include attempts to prevent threat detection and system recovery. For example, targeted attacks may intentionally compromise multiple components and seek to misdirect detection and recovery efforts, causing standard fall-back arrangements (to a previously secure posture) to fail.

Ultimately, there is no such thing as 100% cybersecurity. Organizations need to act on the basis that significant cyber incidents will occur. In order to ensure that they can continue to deliver their primary goals and objectives, organizations need to be able to:

- Anticipate and plan for incidents, based on an understanding of the threats they are exposed to and the potential harms that could arise
- Design processes and establish contingent capabilities that will place the organization in a good position to absorb and recover from events
- Adopt information governance practices that can limit the impact arising from confidentiality breaches and data integrity compromises
- Learn from incidents affecting their own organization and its peers and adapt to strengthen the resilience posture – and perhaps find even better ways to deliver business value
- Take a broad view of cyber risk and the many different ways in which malign actors could exploit cyberspace to cause harm to their operations, profitability or reputation

This process is illustrated in Figure 2. Cyber-resilient organizations are those that know how to "shrink the V" or "shrink the circle".

FIGURE 2 | **Organizations resilient to cyber incidents minimize the impact on primary goals and objectives**

Source: Adapted by the World Economic Forum and the University of Oxford from Linkov, I., & Trump, B.D. (2019). *The science and practice of resilience: Risk, systems and decisions*, Chapter 6. Springer. https://doi.org/10.1007/978-3-030-04565-4_6

It is important to define what recovery from an incident means and to understand the range of actions an organization must take to ensure that the recovery is as swift and effective as possible. Restoring systems and recovering data are clearly part of this, as are maintaining critical services and eventually regaining full operational capacity. Recovery, however, also entails rebuilding reputation, market share and customer trust, which can take much longer and may even require the capacity to surpass pre-incident performance levels. Some companies will be able to shrink the circle and come back stronger, while others may never manage to recover fully. Organizations must take all of these factors into account when evaluating what cyber resilience genuinely means for them. Recovering the underlying digital infrastructure may well not be the organization's highest priority when a major incident occurs. Successful recovery will mean that:

- Operations are back up and running
- The impact on internal and external stakeholders has been ameliorated
- Financial and trading performance is restored
- Strategic assets are protected

Only then are the organization's goals and objectives back on track, and opportunities arising from the incident for enhancing the organization's growth potential will have been unlocked. Strategic assets will include tangible assets such as IT and OT infrastructure and other plant, and intangible assets such as staff well-being and public reputation.

Organizations need to consider the range of plausible scenarios that could affect them. It is important to examine how the organization is connected (in both the technical and business sense) to the surrounding business environment. The external environment and the potentially competing interests of stakeholders may well constrain what is possible for the organization. Likewise, some of the key measures to enhance cyber resilience will extend beyond the organization itself. To achieve true cyber resilience, organizations must actively collaborate with external parties, including suppliers, customers and other stakeholders, who have a shared interest in strengthening the resilience of the entire business environment.

The specific actions any organization takes will vary depending on the context and will change over time as the business context, threat and underlying technologies evolve. There are, nonetheless, some paths to success that can be illuminated by the collective experiences and insights of peers – the sharing of good practice on what works and how to overcome barriers to success has motivated this project. These are summarized in Section 3 of this paper.

> To achieve true cyber resilience, organizations must actively collaborate with external parties, who have a shared interest in strengthening the resilience of the entire business environment.

2.3 Cyber resilience includes IT *and* OT

Organizations of all sizes and in many industries encounter remarkably similar resilience capability challenges.

Cyber resilience extends beyond IT resilience, which focuses solely on maintaining IT operations – the functioning of computers and networks that store, process and transmit information – during disruptions. Cyber resilience also encompasses the resilience of OT, industrial control systems (ICS) that operate, control and monitor industrial equipment and processes, fundamental for ensuring the continuation of industrial operations.

Although traditionally managed separately, there has been an increasing convergence of OT and IT environments, driven by the rapid adoption of cutting-edge technologies such as big data, digital twins and the internet of things (IoT). While this convergence offers benefits such as remote control, real-time monitoring and enhanced operational efficiency, it also introduces new vulnerabilities. Historically, many OT environments were "air-gapped" – not connected to the internet or external media; however, as they merge with IT, they become vulnerable to cyberthreats such as malware. An additional layer of complexity is added, as OT environments commonly rely on legacy technologies, which were often designed without cybersecurity in mind and produced by (sometimes now-defunct) manufacturers whose software updates may be infrequent and difficult to implement, ultimately leaving them exposed to security threats.

While IT cyber resilience primarily focuses on protecting data confidentiality, integrity and availability within business networks and systems, OT cyber resilience prioritizes the safety, reliability and availability of industrial control systems and physical processes. The key goals are preventing disruptions to operations, ensuring worker safety and protecting critical infrastructure. It should be noted that risks will propagate across the two environments, and that they will be codependent even if the sole interface is a human being across an air gap. Organizations should look at IT and OT resilience in tandem, enabling them to develop a comprehensive security strategy that addresses vulnerabilities throughout the entire digital infrastructure.

2.4 Influencing factors

An organization's cyber-resilience requirements are shaped by its characteristics – including size, structure, level of digitalization and industry – as well as factors such as the threat actors it faces, their intentions and the potential harm they may cause. Despite those significant differences, organizations of all sizes and in many industries encounter remarkably similar resilience capability challenges.

These shared challenges are formed in a broader context of complex global issues, including a fragmented geopolitical landscape, armed conflicts, misinformation and disinformation, extreme weather events, pollution, societal polarization, forced migration and widespread economic uncertainties.[16] An organization's cyber resilience can be both enabled and limited by the broader geopolitical, technological, societal, economic and environmental context.

Organizations are, of course, responsible for delivering their own cyber resilience within this broader context. The question therefore is how organizations take these external factors into account when developing their cyber-resilience strategies and plans. For more information on each of the factors, please refer to Section A4 of the Appendix.

3 Next steps: Sharing cyber-resilience practices from the front line

Shared insights and lessons learned among peers can serve as a valuable complement to the checklist-based approaches that common cyber frameworks offer.

> The real questions are, what works in practice – and how can this be identified? What can organizations learn from the front-line experience of others?

Various standards, models and frameworks exist to help organizations manage cybersecurity risk and increase their resilience to cybersecurity events. These cover a wide range of actions, from specific technical controls through to board-level governance (NIST CSF 2.0, ISO 27001 and SOC 2, for example)[17] and have become embedded within cybersecurity practice across many sectors and geographical areas. They also form the basis upon which external stakeholders (such as customers, investors, regulators and insurers) can assess how well the organization is managing these risks and therefore how well their interests are being protected. In the same way, there are various standards, models and frameworks designed to help organizations improve their operational resilience to a wide range of threats, of which cyber is only one – albeit usually among the most pressing (for example, in banking and financial services, the Basel Committee and the Digital Operational Resilience Act).[18,19]

These models are valuable, but they have their limitations. Most have been designed to apply broadly across various types of organization, which makes them somewhat static over time – a drawback when addressing the dynamic nature of cyber risks. Typically, they emphasize what actions need to be taken rather than how to effectively implement a control measure within the specific context of an organization at a given moment. Although various sectors have produced specific guidance or regulation to bridge this gap, there remains a wide spectrum of approaches that can be taken, requiring individual judgement in determining the most appropriate measures for the unique circumstances of each organization.

The real questions are, what works in practice – and how can this be identified? What can organizations learn from the front-line experience of others? Are these models and frameworks delivering what their stakeholders need?

While organizations should be cautious about simply copying practices from others, exchanging insights and lessons learned with peers can greatly enhance the generic approaches that common models offer. In order to stimulate this level of peer interaction, the Cyber Resilience Blueprint initiative, a collaboration between the World Economic Forum and the University of Oxford, convened a community of cyber practitioners, drawn from several sectors and geographical areas, to share good practice and identify how organizations can take collaborative action to address cross-cutting and systemic threats to the resilience of the ecosystem as a whole (see Section A1 of the Appendix for more information about the community). This initiative has identified various practices that are being implemented by organizations today, and perspectives on where the major practical gaps and challenges lie. Together, these findings are helping to build a body of cyber-resilience practices from the front line.

Several themes have been identified:

- Cyber resilience starts at the top. Leaders need to foster the right cyber-resilient mindset centred on their organization's primary goals and objectives.

- Decision-making on cyber resilience needs to be embedded within the established governance structures of the organization, ensuring clear accountability while empowering individual parts of the business to determine what suits their circumstances and strategic priorities.

- Business processes that depend on IT (and OT) need to be designed in a way that recognizes that 100% cybersecurity cannot be achieved. Cyber resilience therefore needs to be built into business processes and information governance practices upfront to ensure that service availability and quality can be maintained and stakeholder interests protected in the event of a major cyber disruption.

> Organizations must collaborate to identify common single points of failure and develop strategies to collectively mitigate the risks associated with them.

- Plans must be established that come into effect when incidents occur, building on a clear and consistent understanding of an organization's core strategic, operational, financial and legal priorities and thereby supporting an organization to safeguard these vital interests during the incident.

- All of the above must be grounded in strong cybersecurity practices to guarantee that the technology infrastructure is designed with the appropriate level of resilience and security corresponding to the organization's reliance on it.

While there is plenty that individual organizations can do to enhance their cyber resilience, this does ultimately also depend on the resilience of the business ecosystem. Improving ecosystem resilience requires collaborative action, in particular:

- Organizations must collaborate to identify common single points of failure and develop strategies to collectively mitigate the risks associated with them.

- Organizations need to explore how best to make use of the limited pool of cyber talent and expertise, particularly to support entities within the ecosystem that lack the internal capabilities necessary to ensure the resilience on which others in the ecosystem depend.

- Organizations should also explore how they can work together to improve the overall talent pool. The World Economic Forum is leading the Bridging the Cyber Skills Gap initiative, which has developed a Strategic Cybersecurity Talent Framework featuring achievable approaches to help organizations build sustainable talent pipelines.[20]

- The policies and processes that have been developed to achieve assurance up and down the supply chain create a significant cost but do not always provide the kind of robust and real-time assurance that organizations need to manage cyber risk. There may be scope for organizations to work together to develop a more streamlined and dynamic approach that provides greater assurance for the ecosystem.

- Organizations, regulators and policy-makers (at international, national and regional levels) should cooperate to develop regulations that support and incentivize cyber resilience. This needs to take into account the requirement to ensure an appropriate level of consistency between regulatory jurisdictions and to recognize that the cyber resilience imperative may sometimes conflict with other regulatory imperatives such as those relating to competition and pricing.

- Organizations should work together, including with public authorities, to proactively address threats and find ways to disrupt those who seek to exploit cyber vulnerabilities. The World Economic Forum's Partnership against Cybercrime was launched in 2020 to promote public–private cooperation to combat cybercrime. It serves as a platform for insight sharing and continuous exploration of approaches to drive successful collaboration against cybercrime.

None of the above negates the fact that organizations are individually responsible for managing the risks to their own primary goals and objectives, but collaborative action may often be the best way to achieve the level of cyber resilience that is required. These reflections are key when organizations are taking action and collaborating on cyber resilience and require further development by the community as next steps.

Appendix

A1 Methodology

This paper is anchored in the thematic analysis of three virtual community workshops, one in-person expert community workshop, five smaller virtual working groups and 40+ semi-structured one-on-one interviews. A total of 76 experts from 71 different organizations participated in the discussions and interviews. While most participants held positions specifically overseeing cybersecurity – such as chief information security officers (CISOs) and chief technology officers (CTOs) – there was a diverse array of profiles, including chief executive officers and consultants. The representation included 16 different industry sectors and participants from Europe, North America, South America, Asia and Africa.

A2 Definitions of cyber resilience

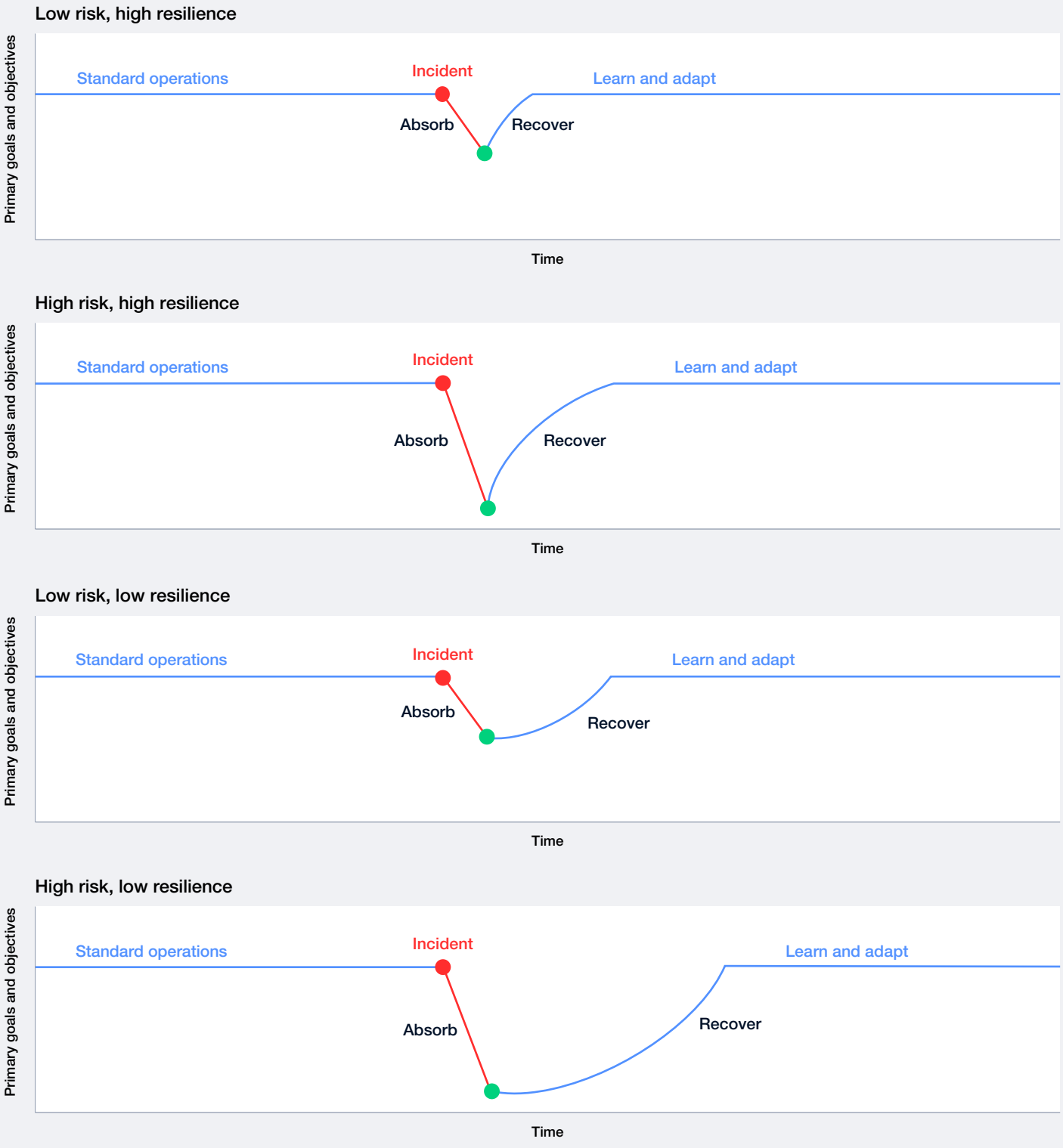
The term "resilience" is widely used and often ambiguous.[21] There are numerous definitions for cyber resilience with a focus on organizational resilience, technical resilience or both. Examples include:

- "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment"[22]
- "The capacity of a system to cope with disruptions while maintaining or rapidly re-establishing the system's functionality"[23]
- "The capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity and feedbacks"[24]
- "The ability to anticipate, prepare for and adapt to changing conditions and withstand, respond to and recover rapidly from disruptions"[25]
- "The ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity"[26]
- "The capacity to withstand, recover from and adapt to the external shocks caused by cyber risks"[27]
- "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources regardless of the source"[28]
- "The ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack"[29]
- "The ability to continuously deliver the intended outcome despite adverse cyber events"[30]

A3 Divergent cyber-resilience profiles

An organization's resilience, as well as their risk context, affect their cyber-resilience profiles. The different cyber resilience profiles are outlined in Figure 3.

FIGURE 3 **Cyber resilience profiles**



Source: Adapted by the World Economic Forum and the University of Oxford from Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience: Risk, systems and decisions*, Chapter 6. Springer. https://doi.org/10.1007/978-3-030-04565-4_6

A4 Broader global context

Organizations have shared challenges shaped by the broader context of complex global issues. Those influencing factors need to be taken into account when designing cyber-resilience strategies.

TABLE 1 **Factors that affect cyber-resilience strategies**

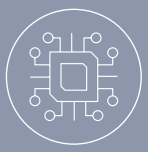
Geopolitics 	Geopolitical instability and armed conflicts are complicating the cyber landscape. They will lead to growing capability among threat actors and the proliferation of innovative offensive cyber capabilities, increased capacity within the threat actor ecosystem and increased potential for organizations to become collateral damage in a state-level cyber incident. For example, ongoing cyberattacks against Ukrainian infrastructure and data, which have been targeting government websites, energy providers and financial institutions since at least 2014, exemplify the growing intersection of geopolitics and cyberthreats.[31] State-sponsored hackers have been increasingly targeting critical infrastructure in Europe and the USA.[32] The growth of state-sponsored disinformation campaigns is also causing concern for governments as well as increasingly for businesses.
Technology 	Technology brings an expanded attack surface, whether from inherent vulnerabilities or through insecure configurations and the accidental introduction of risks when used. The increasingly complex technology environment requires a shift in the approach to cyber resilience, with organizations ensuring that the necessary measures are in place to protect them from cyber risks according to their risk appetite.[33] Setting the appropriate risk appetite for an organization is becoming harder as the complexity of the digital estate grows. For example, in the case of generative AI, its use by malicious actors is a major concern, while it presents opportunities for enhancing the productivity of individuals, business and civil society more generally. According to the World Economic Forum's *Global Cybersecurity Outlook 2024*, fewer than one in 10 business and cyber leaders believe that generative AI will give the advantage to defenders over attackers in the next two years.[34] Organizations need to stay informed on how emerging technologies affect their cyber risks and implement appropriate measures to keep the risks manageable. Achieving the visibility and insight needed to do this remains a significant challenge.[35] Geopolitical tensions are leading to the decoupling of the technology supply chain, creating further uncertainty.
Society 	Societal polarization and the spread of misinformation and disinformation likely pose significant risks to cyber resilience, as mis- and disinformation can be used to influence people in ways that can introduce cyber risk to create new ways to attack an organization or to compromise system defences and other efforts at risk mitigation. Disinformation campaigns are not new, but they are growing in sophistication, personalization and reach, exploiting social divisions, manipulating individuals and creating confusion regarding the credibility of information sources. A striking example of this occurred in 2021 when hackers leaked a manipulated version of confidential documents relating to evaluation processes for COVID-19 vaccines to undermine trust in the Pfizer-BioNTech vaccine.[36] As cyberthreats grow, regulations are adapted to protect citizens and assets. The widespread influence of the European Union (EU) General Data Protection Regulation (GDPR) illustrates how regulations can affect organizations' cybersecurity practices and raise standards.[37,38] Cybersecurity requirements for national critical infrastructure, such as the EU Cyber Resilience Act and mandatory reporting of cybersecurity incidents in the USA,[39] exemplify the increasing need to integrate cyber resilience into all businesses areas to adapt to the changing regulatory landscape.[40]

TABLE 1 | **Factors that affect cyber-resilience strategies** (continued)

Economics 	A business's cyber resilience is closely tied to its broader economic context. Businesses continue to pivot in the face of geopolitical and technological change: new business models are being developed; some markets are consolidating, while others are fragmenting; and new markets are opening while others are closing. All of these can affect an organization's cyber-risk exposure and the options it has to address them. Internally, cybersecurity spending tends to be more protected than other IT budgets during economic downturns,[41] among other reasons because cybercrime tends to surge during economic recessions.[42] However, cyber leaders are not immune to budgetary pressures,[43] and this economic context strains cyber-resilience capacities and their ability to ensure business resilience. There is a shortage of cyber skills and talent, fostered by wider societal issues such as a lack of diversity in science, technology, engineering and mathematics (STEM) education and the slow adaptation of traditional educational systems to meet industry needs. In addition to not being able to recruit an adequate workforce, the stress and demands of the threat environment are driving trained personnel out of the profession. Gartner has predicted that as much as 25% of the current CISO workforce may leave the profession entirely.[44] According to the World Economic Forum's *Global Cybersecurity Outlook 2024*, this skills gap is particularly pronounced in smaller organizations, where half say they do not have or are unsure whether they have the skills needed to meet their cyber objectives. Similarly, 52% of public-sector organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience.[45] While this shortage of cyber talent becomes increasingly well understood, there is a gap regarding the broader appreciation of cyber risk and what capabilities are needed within the rest of the workforce to build cyber resilience.
Environment 	Organizations cannot simply focus on human-caused disruptions, as the natural world may bring events that damage digital infrastructure or cause significant changes in societies that will create new cyber-resilience requirements. For example, as climate change increases the frequency, intensity and impact of extreme weather events, businesses need to prepare for scenarios such as power outages caused by extreme weather, which can compromise digital infrastructure and business continuity.[46]

Source: Analysis by the World Economic Forum and the University of Oxford

Contributors

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Luna Rohland
Specialist, Cyber Resilience

University of Oxford

Ioannis Agrafiotis
Senior Researcher, Global Cyber Security Capacity Centre

Sadie Creese
Professor of Cybersecurity; Director and Technical Board Chair, Global Cyber Security Capacity Centre

William H. Dutton
Oxford Martin Fellow and Technical Board Member, Global Cyber Security Capacity Centre

Patricia Esteve-Gonzalez
Research Fellow, Global Cyber Security Capacity Centre

Jamie Saunders
Oxford Martin Fellow; Technical Board Member, Global Cyber Security Capacity Centre

Acknowledgements

This white paper was co-created by cyber leaders, experts and diverse stakeholders as part of the World Economic Forum's Cyber Resilience in Industries initiative, who shared insights and lessons learned through interviews, design workshops and consultation sessions. The World Economic Forum would like to thank the following individuals for their leadership, engagement and feedback.

Elie AbenMoha
Publicis Groupe

Mansur Abilkasimov
Schneider Electric

Tamim Ahmed
Bangladesh National CERT

Bushra AlBlooshi
Dubai Electronic Security Center (DESC)

Hoda Al Khzaimi
New York University Abu Dhabi

Hessah Almajhad
Saudi Information Technology Company (SITE)

Fahad Alqahtani
NEOM Company

Yasser N. Alswailem
Saudi Telecom Company (STC)

Romain Aviolat
Kudelski Group

Nik Bartholomew
Occidental Petroleum Corporation

Mauricio Benavides
Metabase Q

Janus Friis Bindslev
PensionDanmark

Jalal Bouhdada
DNV

Grant Bourzikas
Cloudflare

Duncan Bradley
Kyndryl

Marijus Briedis
Nord Security

Ian Buffey
AtkinsRéalis

Tony Buffomante
Wipro

Ronald Charron
Canadian Centre for Cyber Security

Piotr Ciepiela
EY

Larry Clinton
Internet Security Alliance

Steve Cobb
SecurityScorecard

Stefan Deutscher
Boston Consulting Group

Hazel Diez Castaño
Santander

Donna Dodson
evolutionQ

Ali El Kaafarani
PQShield

Mohammed Elofi
Gulf International Bank BSC (GIB)

Gregory Eskins
Marsh McLennan

Peter Evans
New South Wales Police Force

Jeff Farinich
New American Funding

Sabrina Feng
London Stock Exchange Group

Shannan Fort
Marsh McLennan

John Frazzini
X-Analytics

Javier Garcia Quintela
Repsol

Jonathan Gill
Panaseer

Tracie Grella
AIG

Jassim Happa
Royal Holloway, University of London

Ronald Heil
KPMG International Services

Randy Herold
ManpowerGroup

Paul Hopkins
Vodafone

Lawrence Jarvis
Iron Mountain Information Management

Laura Jiménez Orgaz
Santander

Santeri Kangas
Cujo

Rosa Kariger
Iberdrola

Andreas Kind
Siemens

Ryan Lasmaili
Vaultree

Simon Leech
Hewlett Packard Enterprise (HPE)

Shawn Lonergan
PricewaterhouseCoopers

Kris Lovejoy
Kyndryl

Michael Meli
Julius Baer

Thomas Millar
Cybersecurity and Infrastructure Security Agency

Deryck Mitchelson
Check Point Software Technologies

Paulo Moniz
EDP

Sean Morton
Trellix

Michele Mosca
evolutionQ

Emmanuel Mugabi
Centenary Technology Services

Tejas Mulay
Bajaj Financial Services

Natalia Oropeza
Siemens

Mark Orsi
Global Resilience Federation

Tom Parker
Hubble Technology

Pankaj Paul
Burjeel Holdings

Rahayu Ramli
Petronas

Cyril Reol
Mercuria

Jesús Sánchez
Naturgy

Miguel Sánchez
Telefónica

Ralf Schneider
Allianz

Arno Sevinga
Royal Vopak

Vikram Sharma
QuintessenceLabs

Leo Simonovich
Siemens Energy

Colin Soutar
Deloitte

Mark Stamford
OccamSec

Ian Tien
Mattermost

Phil Tonkin
Dragos

Prashant Verma
Bajaj Finance

Alexander Ward
Thales

Swantje Westpfahl
Institute for Security and Safety (ISS)

Ollie Whitehouse
UK National Cyber Security Centre (NCSC)

Wendi Whitmore
Palo Alto Networks

David Wilson
UBS

Kate Yamashita
Accenture

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Alison Moore
Editor, Astra Content

Endnotes

1. Hatami, H., & Segel, L. (2023, April 6). *Six CEO priorities for 2023.* McKinsey & Co. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/six-ceo-priorities-for-2023.
2. Ibid.
3. World Bank. (n.d.). *Individuals using the internet (% of population)*. Retrieved 2024, October 4, from https://data.worldbank.org/indicator/IT.NET.USER.ZS.
4. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15): 1–20. https://doi.org/10.3390/s23156666.
5. Hatami, H., & Segel, L. (2023, April 6). *Six CEO priorities for 2023.* McKinsey & Co. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/six-ceo-priorities-for-2023.
6. Ibid.
7. Leigh, D. (2023, March 14). *60% of SMEs that suffer a cyber attack go out of business within six months*. TechRound. https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/.
8. National Association of Corporate Boards. (2023, March 24). *NACD directors' handbook on cyber-risk oversight*. https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/.
9. World Economic Forum. (2022, November 15). *As cyber attacks increase, here's how CEOs can improve cyber resilience*. https://www.weforum.org/agenda/2022/11/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience/.
10. PricewaterhouseCoopers. (2016). *Turnaround and transformation in cybersecurity: Key findings from the Global State of Information Security Survey*. pwc-global-state-of-information-security-survey-2016.pdf.
11. Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security, 27*(5): 781–799. https://doi.org/10.1080/02684527.2012.708530.
12. IBM. (2024, July). *Cost of a data breach report 2024*. https://www.ibm.com/reports/data-breach.
13. University of Oxford, Oxford Martin School. (n.d.). *Global cybersecurity capacity centre*. Retrieved 2024, October 4, from https://gcscc.ox.ac.uk/the-cmm.
14. Chen, T. M., & Robert, J.-M. (2004, December). *The evolution of viruses and worms*. Researchgate. https://www.researchgate.net/publication/228869267_The_Evolution_of_Viruses_and_Worms.
15. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021, December). Developing cyber-resilient systems: A systems security engineering approach. *NIST Special Publication 800–160*, *2*(1). https://doi.org/10.6028/NIST.SP.800-160v2r1.
16. World Economic Forum. (2024, January 10). *Global risks report 2024*. https://www.weforum.org/publications/global-risks-report-2024/.
17. Cisternelli, E. (2024, February 27). *7 cybersecurity frameworks that help reduce cyber risk*. BitSight. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk.
18. Bank for International Settlements. (n.d.). *The Basel Committee – overview*. Retrieved 2024, October 4, from https://www.bis.org/bcbs/index.htm.
19. Digital Operational Resilience Act (DORA). (n.d.). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009*, *(EU) No 648/2012, (EU) No 600/2014*, *(EU) No 909/2014* and *(EU) 2016/1011*. Retrieved 2024, October 4, from https://www.digital-operational-resilience-act.com/Preamble_1_to_10.html.
20. World Economic Forum. (2024, April 28). *Strategic Cybersecurity Talent Framework*. https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/.
21. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x.
22. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021, December). Developing cyber-resilient systems: A systems security engineering approach. *NIST Special Publication 800–160*, *2*(1). https://doi.org/10.6028/NIST.SP.800-160v2r1.
23. Sikula, N. R., Mancillas, J. W., Linkov, I., & McDonagh, J. A. (2015). Risk management is not enough: A conceptual model for resilience and adaptation-based vulnerability assessments. *Environment Systems and Decisions*, *35*(2), 219–228. https://doi.org/10.1007/s10669-015-9552-7.
24. Pimm, S. L. (1991). *The balance of nature? Ecological issues in the conservation of species and communities*. University of Chicago Press.
25. U.S. Department of Defense. (2016, January 14). *DoD Directive 4715.21: Climate change adaptation and resilience*. DoDD 4715.21, January 14, 2016, Implementing Change 1, August 31, 2018 (whs.mil).

26. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 1–9. https://doi.org/10.1016/j.iot.2020.100204.

27. Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), 1–17. https://doi.org/10.1093/cybsec/tyz013.

28. Ross, R., Graubart, R., Bodeau, D., & McQuaid, R. (2018). Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems. *Draft NIST Special Publication 800–160*, *2*(1). https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

29. European Central Bank. (n.d.). *What is cyber resilience?* Retrieved 2024, October 4, from https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html.

30. Bjorck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis, editors, New contributions in information systems and technologies. Advances in Intelligent Systems and Computing, 353. Springer. https://doi.org/10.1007/978-3-319-16486-1_31.

31. Lewis, J. A. (2022, June 16). *Cyber war and Ukraine*. Center for Strategic & International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine.

32. United States National Security Agency/Central Security Service. (2024, May 1). *Defending OT operations against pro-Russia hactivist activity* [Press release]. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3761830/urgent-warning-from-multiple-cybersecurity-organizations-on-current-threat-to-o/.

33. World Economic Forum and University of Oxford. (2020, November). *Future Series: Cybersecurity, emerging technology and systematic risk*. https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.

34. World Economic Forum. (2024, January). *Global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

35. World Economic Forum and University of Oxford. (2020, November). *Future Series: Cybersecurity, emerging technology and systematic risk*. https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf.

36. European Medicines Agency. (2021, January 15). *Cyberattack on EMA – update 5*. https://www.ema.europa.eu/en/news/cyberattack-ema-update-5.

37. Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338–1347. https://doi.org/10.30574/ijsra.2024.11.1.0220.

38. Machado, P., Vilela, J., Peixoto, M., & Silva, C. (2023). *A systematic study on the impact of GDPR compliance on organizations*. SBSI '23: Proceedings of the XIX Brazilian Symposium on Information Systems. https://doi.org/10.1145/3592813.3592935.

39. Cybersecurity & Infrastructure Security Agency. (2022, March). *Cyber incident reporting for Critical Infrastructure Act of 2022 (CIRCIA)*. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

40. Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science and IT Research Journal*, *5*(1), 120–140. https://doi.org/10.51594/csitrj.v5i1.709.

41. Gleeson, J. (2023, October 16). *Cybersecurity: A potentially vast investment opportunity as technology evolves*. AXA Investment Managers. https://www.axa-im.ch/en/research-and-insights/investment-institute/future-trends/technology/cybersecurity-potentially-vast-investment-opportunity-technology-evolves.

42. Swinhoe, D. (2020, May 21). *Cybercrime in a recession: 10 things every CISO needs to know*. CSO. https://www.csoonline.com/article/569341/cybercrime-in-a-recession-10-things-every-ciso-needs-to-know.html.

43. IANS and ARTICO Search. (2023, October 2). *2023 security budget: Benchmark summary report*. https://cdn.iansresearch.com/Files/Marketing/2023SurveyContent/IANS+ArticoSearch-2023SecurityBudgetBenchmarkSummaryReport.pdf.

44. Gartner. (2023, February). *Gartner predicts nearly half of cybersecurity leaders will change jobs by 2025*. https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025.

45. World Economic Forum. (2024, January). *Global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

46. Rutherford. (n.d.). *Climate change and cyber security: What to expect in financial services*. Retrieved 2024, October 4, from https://www.rutherfordsearch.com/blog/2021/09/climate-change-and-cyber-security-what-to-expect-in-financial-services.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org