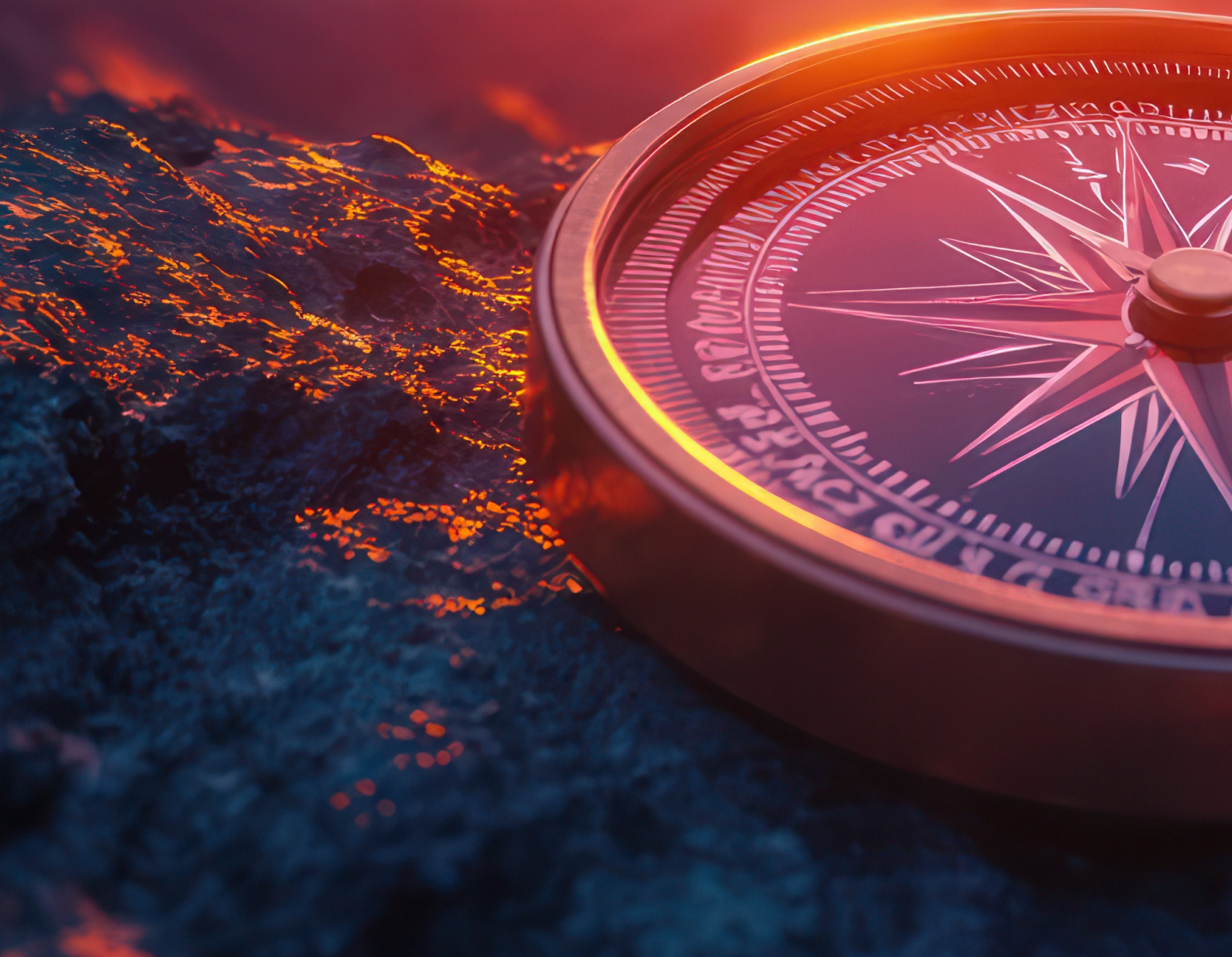
In collaboration with
the University of Oxford

WORLD ECONOMIC FORUM

The Cyber Resilience Compass: Journeys Towards Resilience

WHITE PAPER

APRIL 2025



Images: Getty Images

Contents

Foreword

Akshay Joshi
Head, Centre for Cybersecurity, World Economic Forum

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

Cyber resilience matters. As businesses and governments continue to evolve their use of digital technologies and data, global dependence on cyberspace continues to grow. This increasing reliance exposes organizations and individuals to heightened cyber risks at a time when threat actors are becoming more sophisticated, well-resourced and innovative.

Cyber resilience acknowledges that no system is entirely secure. Traditional cybersecurity efforts have evolved from merely implementing technical security controls to a broader strategy focused on safeguarding core business objectives. The goal is not just to prevent cyber incidents but to minimize their impact on an organization's primary goals and objectives, such as maintaining critical services, safeguarding stakeholder confidence and protecting strategic value, while promoting long-term growth.

Building on our previous white paper *Unpacking Cyber Resilience*, this publication delves into the practical aspects of cyber resilience, offering insights drawn from the front-line practices of leading organizations globally. It emphasizes the need to move beyond technical solutions and develop comprehensive strategies that align with business objectives. Through consultations and workshops with cybersecurity practitioners, this work distils real-world lessons on what works – and what does not – when confronting cyber risks.

Ultimately, cyber resilience is a practice, not a theory, and sharing learnings about "what works" is key to building collective knowledge in the field. The Cyber Resilience Compass should not be seen as a static tool but as a vehicle for organizations to exchange experiences and identify front-line practices as they seek to make progress along their cyber resilience journey. We invite you to access additional insights and contribute to the Cyber Resilience Compass here.

Executive summary

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

The specific actions any organization takes to strengthen its cyber resilience will vary depending on the context and will change over time as the business, threat landscape and underlying technologies evolve. There are, nonetheless, some paths to success that can be illuminated by the collective experiences and insights of peers. Sharing good practice, what works and how to overcome barriers to success has motivated this endeavour (see *Unpacking Cyber Resilience*).

To gather insights on leading practices, the World Economic Forum, in collaboration with the University of Oxford, conducted a series of consultations and workshops with cyber leaders across geographies and industries, addressing the following questions:

- What have they done to cope with threats posed to their organization?
- What worked for them?
- What failed?

Those discussions identified numerous concrete front-line practices that, while not exhaustive, provide a rich source of inspiration and direction. For accessibility and actionability, the Cyber Resilience Compass systemizes them into seven interrelated categories:


Leadership


Governance, risk and compliance


People and culture


Business processes


Technical systems

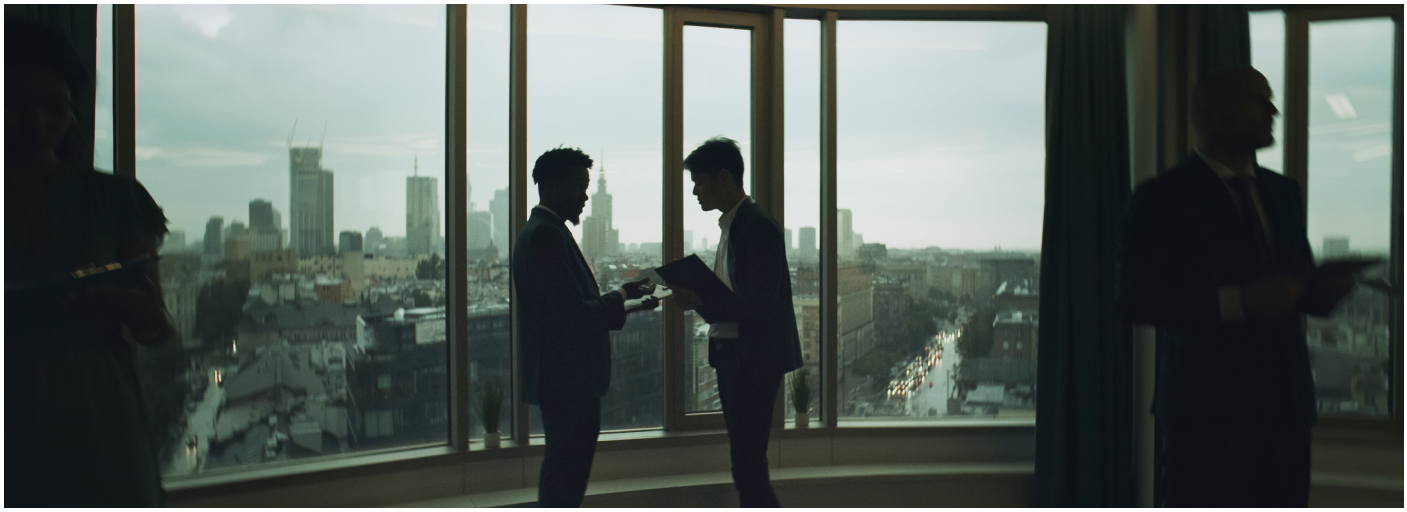

Crisis management


Ecosystem engagement

This white paper highlights the critical role of collaboration, knowledge-sharing and adaptive learning in strengthening cyber resilience. There is no universal blueprint for success – each organization must tailor and scope its approach based on its specific context, strategy and external factors. However, by drawing on the experiences of others, organizations can identify effective strategies and shape their own resilience roadmaps to navigate an increasingly complex cyber landscape. As a vehicle for the sharing of front-line practices and experiences, the Cyber Resilience Compass seeks to provide the valuable insights that help organizations develop and refine their cyber resilience journey.

1 Unpacking cyber resilience

Cyber resilience goes beyond traditional cybersecurity; it is an organization's ability to minimize the impact of significant cyber incidents on its primary business goals and objectives.



The term "cyber resilience" does not diminish the importance of cybersecurity but recognizes that where 100% cybersecurity cannot be achieved, further measures are required (both pre- and post-incident) to protect the organization from the impacts of severe cyber events.

When considering cyber resilience, it is important to take a broad view of what cyber risk encompasses. 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. Organizations need to consider the many ways in which they are exposed to cyber risks and how they can limit potential impacts – whether by investing in operational cybersecurity controls, by adapting 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, legal or reputational – or a combination of these factors.

Preparing for cyber incidents

Organizations advise acting on the assumption that significant cyber incidents will occur. To ensure that they can continue to achieve their primary goals and objectives, organizations need to be able to:

- Anticipate and plan for incidents, based on an understanding of the threats to which they are exposed 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 peers and adapt to strengthen their resilience posture – and perhaps find even better ways to deliver business value.
- Take a broad view of cyber risk and the many ways in which malign actors could exploit cyberspace to cause harm to their operations, profitability or reputation.

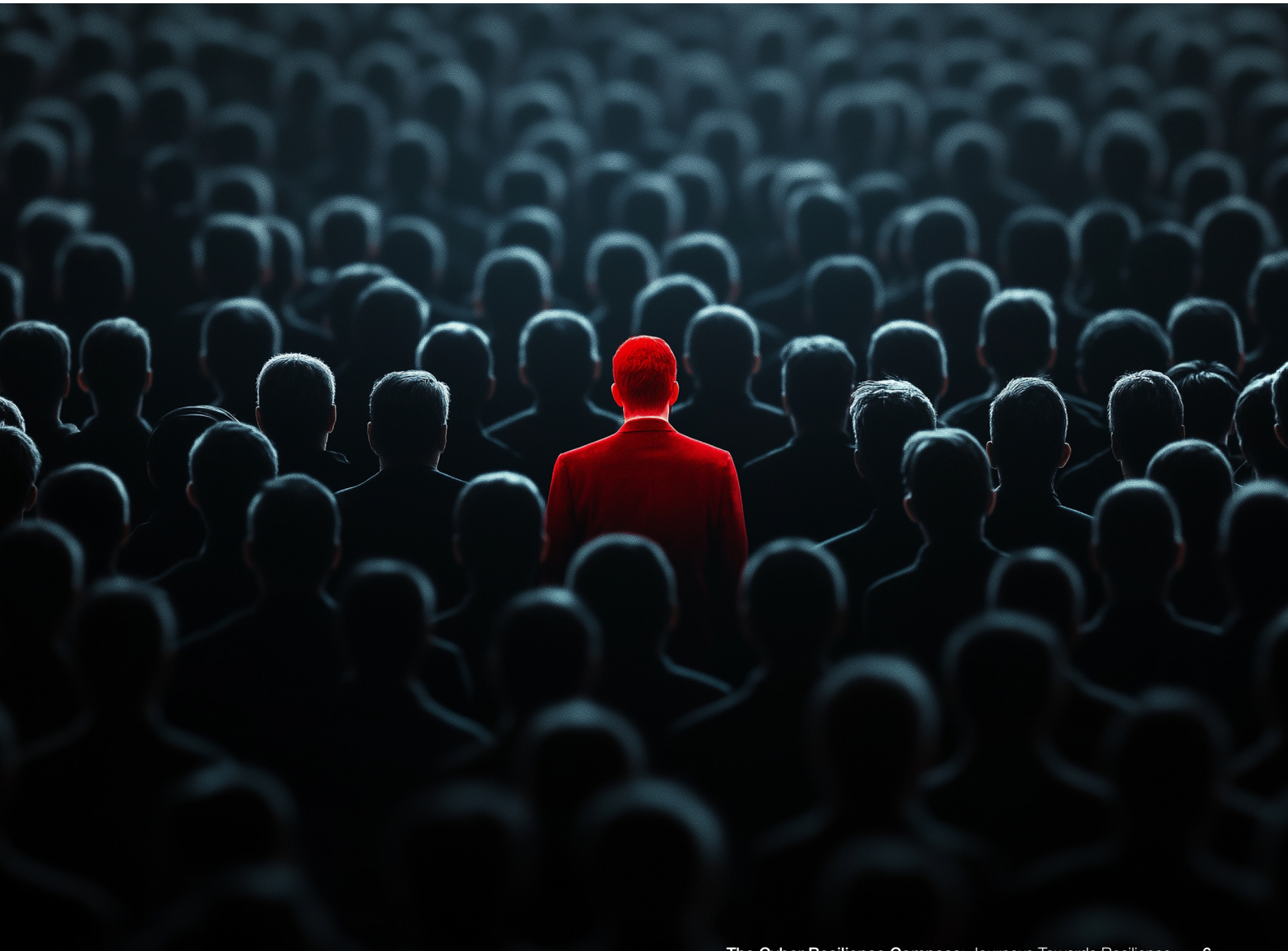
The cyber resilience context

The risks and challenges in building cyber resilience are not uniform but unique to each organization as it faces its specific threats in context. Therefore, as the following sections explore systematized categories of practices and issues drawn from the cyber front line, it is important to emphasize again that an organization's cyber resilience is tied to the particular nature of the organization's technological and business processes. These processes are influenced by its preparations for and actions in response to incidents and other factors including the broader ecosystem, its industry and whether it operates in a local or global context.

The cyber resilience strategies and practices of organizations are likely to differ not only in the nature of the threats they face but also according to the characteristics of each organization. These may include the:

- Size and the scope of its operations
- Grade of digitalization and centrality of technological systems, including information technology (IT), operational technology (OT) and internet of things (IoT)
- Whether it is categorized as critical national infrastructure (CNI) or otherwise subject to regulatory obligations
- Degree of decentralization and independence among the organization's units
- Volume, speed and degree of reliance on its supply-chain ecosystem
- Diversity of cybersecurity capacities within and across the organization
- Workforce allocated to the most critical processes
- Availability of skilled cybersecurity professionals in its labour market
- Sector- and industry-specific challenges

These and other circumstances influence how any given organization can become more resilient to cyberthreats. Ultimately, there is no universal solution or single approach that fits all organizations; instead, numerous front-line practices exist, which vary by applicability, depending on these contextual factors.



2 The Cyber Resilience Compass

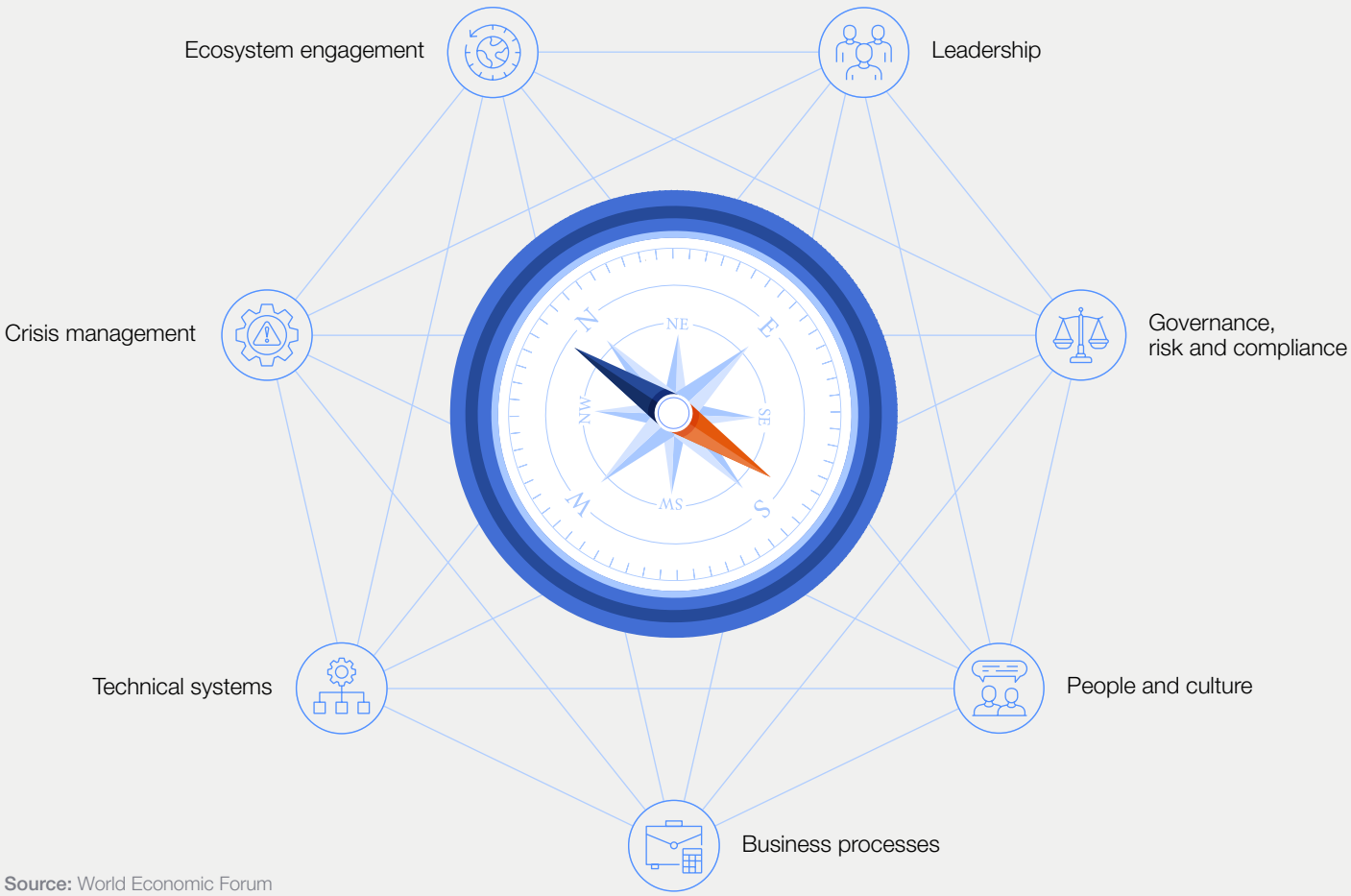
Organizations can use the Cyber Resilience Compass to share cyber resilience approaches that work best in practice.

Achieving cyber resilience is a complex, dynamic and ongoing process that requires more than just a single action or tool. Instead, it involves a combination of practices and efforts cultivated over time by an organization, its leadership and its technical teams. Through experience and continuous improvement, organizations can develop a more robust approach to cyber resilience. In this process, exchanging insights and lessons learned with peers can significantly help organizations to leverage effective practices and strategies.

Recognizing that collaborative sharing is essential for improving practices, the Cyber Resilience Compass facilitates this collaboration by collecting what works in practice – that is, what organizations can learn from the front-line experiences of others. The Cyber Resilience Compass outlines a range of concrete and detailed practices, which aggregate to seven general interrelated categories to help organizations define their cyber resilience journey.

The Cyber Resilience Compass is not a static tool; rather, it serves as a dynamic resource for leaders and organizations to identify front-line practices, share experiences and exchange insights to enhance their cyber resilience journey.

FIGURE 1 **The Cyber Resilience Compass**



Source: World Economic Forum

3 Learnings from front-line practice

What lessons can be learned from speaking with cyber experts about their front-line practices? What are they advising their peers to do?

Through workshops and consultations with cyber experts, a list of front-line practices was gathered and systemized into a manageable set of seven categories. The following sections provide a brief description of what each category entails and examples of front-line practices that the world's leading practitioners take in each area. The list of front-line practices is not exhaustive, but the examples are intended to inspire action and provide direction. Reflecting the complex reality of cyber resilience, many of the practices relate to more than one of the overlapping and interrelated categories.

3.1 Leadership

Leadership describes the approach to setting goals, making decisions and providing direction for the organization. This involves leaders:

- Identifying the "crown jewels" and **prioritizing** their resilience
- Defining and owning the organization's **risk tolerance**
- Embedding a cyber resilience **culture**
- Empowering local **decision-making** within the overall parameters set by top leadership
- Promoting cross-organizational **collaboration**

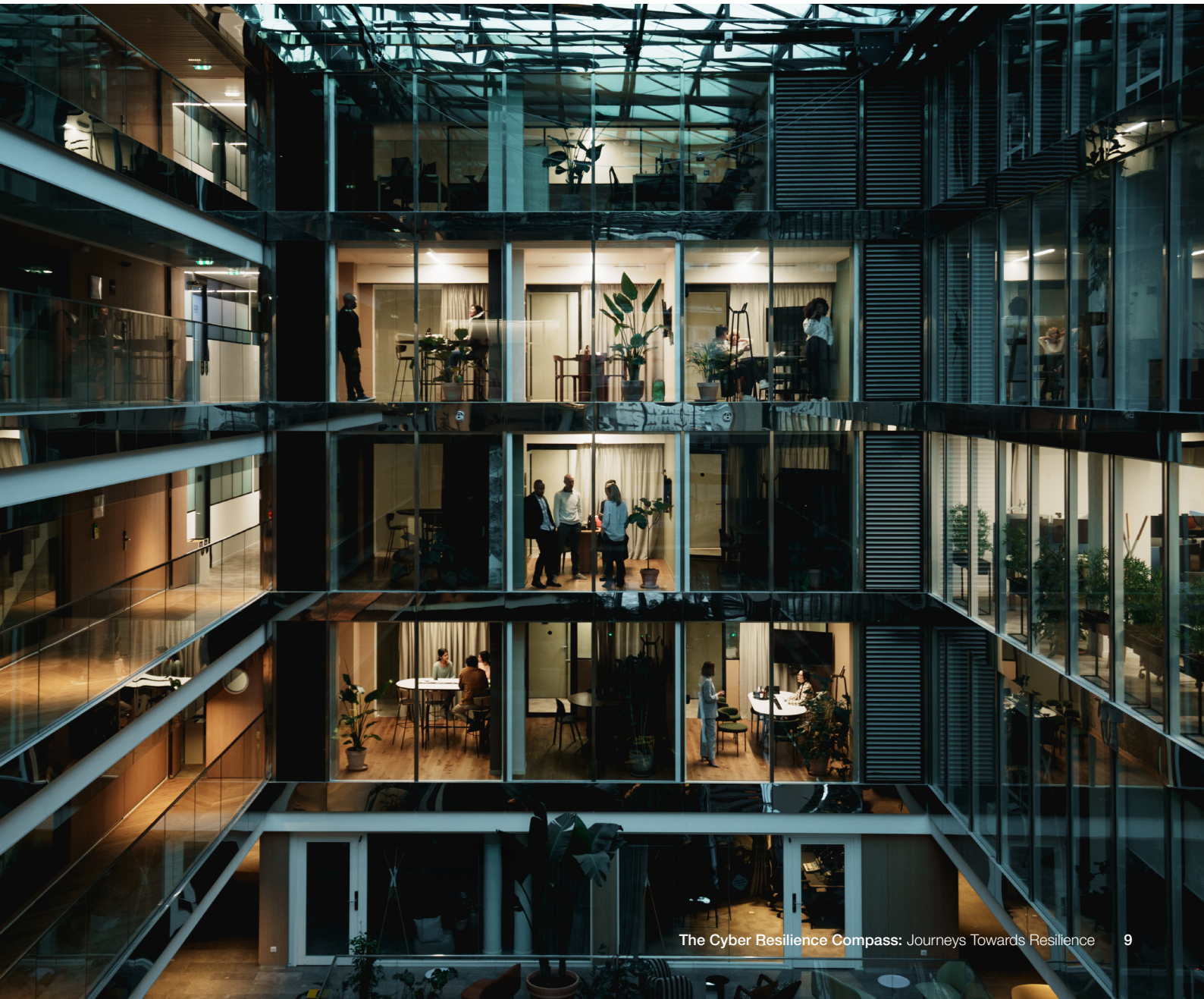
Examples of front-line practices that organizations are applying:

- Top leadership identifies the organization's most valuable assets, business processes and products (its "crown jewels") to ensure adequate prioritization and resource allocation. Technical leadership develops an understanding of how technology supports these assets and quantifies risks, including financial, operational and reputational impacts.
- Top leadership validates the organization's risk tolerance to balance the strategic imperative to drive growth with the need to maintain operational stability. By setting clear parameters for risk assessments, establishing the organization's risk profile and communicating it, leaders steer decision-making and ensure that any risks that are taken align with the company's overarching objectives.
- Top leadership embeds cyber resilience as a core organizational value to ensure that everyone, from top leadership to entry-level employees, embraces awareness, proactivity and adaptability. Chief information security officers (CISOs) actively communicate the importance of cyber resilience and enforce clear cyber resilience policies, encouraging employees to take responsibility for protecting data and systems.
- Risk-owners and CISOs engage with leadership to enable informed decisions and active management of their organization's cyber risks. CISOs' engagement with top leadership includes the provision of context-specific cyberthreat briefings for top leadership, personalized cybersecurity and awareness training, scenario-based tabletop exercises and expert briefings.
- Top leadership builds trust and open communication with CISOs and technical teams to cultivate effective cross-organizational collaboration. Top leadership engages with the CISO, asks critical questions and helps prioritize cybersecurity investments to enable swift responses in crises and alignment of resources with the organization's risk appetite and strategic goals.

Experts highlighted the practical challenge of securing the level of top leadership engagement described in the examples above. The primary reasons cited were the limited time leaders have to address cyber risks and the difficulty of translating complex technical issues into terms that relate to business leaders' main goals and objectives. Scenario planning and executive tabletop exercises were recommended as effective methods to engage leadership and increase awareness of the connection between critical business processes and the supporting capabilities, including both internal technologies and external services. In organizations that had experienced significant cyber incidents, the dynamic was very different – these events often resulted in a dramatic increase in leadership awareness and concern for the issue.

> **In organizations that are best in class, you can ask business leaders, 'What are the most pressing cybersecurity issues?' And they will be able to name the top three because they are working on those issues.**
>
> Natalia Oropeza, Global Chief Cybersecurity Officer; Chief Diversity and Inclusion Officer, Siemens

> **We started with making sure that everybody understands the challenges associated with security broadly. The messages come from the CEO as well, not just from the CIO or IT. This constant feedback and dialogue is important and, if it comes from the C-suite, it makes an impact for the entire organization.**
>
> Pankaj Paul, Director, Strategy and Innovation, Burjeel Holdings



CASE STUDY 1

Mærsk – Informed decision-making: Establishing a risk-based approach

The NotPetya cyberattack in 2017 significantly affected Mærsk's short-term operational capabilities and customer service. More importantly, it marked a turning point in the company's transition to a risk-based approach for cybersecurity investments and enhancements. Before initiating this transition, top leadership, in collaboration with stakeholders across the organization, assessed the business criticality of its applications and their roles in key business operations. This assessment provided the foundation for prioritizing investment areas effectively.

Consequently, Mærsk adopted a quantified risk reduction strategy, translating risk into a "dollars-lost" equivalent, which facilitated meaningful discussions with the board and chief financial officer (CFO), ultimately securing essential funding for its cyber transformation programme. This strategy also guided decisions on where to invest in developing, operationalizing and embedding cyber capabilities.

By using Monte Carlo simulations and other risk-modelling techniques, Mærsk enabled data-driven, risk-based decision-making. This methodology has also significantly improved due diligence and purchasing decisions. The steps taken since 2017 have resulted in better investment prioritization, reduced cyber risk exposure and enhanced resilience across Mærsk's operations.

CASE STUDY 2

PETRONAS – Leading organizational change: A cyber resilience transformation

When PETRONAS embarked on its digital transformation journey in 2017, leadership made cyber resilience a top priority from the outset. Following PETRONAS' shift towards a more strategic and extensive use of data, technological solutions and new ways of working – as well as its role as the operator of national critical infrastructure – the need to operate securely became a non-negotiable prerequisite. However, an initial assessment of the organization's cybersecurity posture indicated that substantial improvements were needed to keep pace with its increasingly complex operations and digital initiatives.

Driven by a clear leadership mandate, PETRONAS began building its cyber resilience capabilities in 2018, focusing on five major pillars:

- **Enterprise cybersecurity governance:** Establishing a holistic framework for managing and enabling cybersecurity consistently across the group
- **Cyber defensive operations:** Ensuring effective identification, detection and response to cyber threats
- **Identity and access:** Enhancing clarity and control over who has access to what and when
- **Real-time operational technology (OT):** Enabling better visibility of and response to threats in the OT environment
- **Extensive enterprise-wide education and awareness programme:** Supporting all pillars by ensuring employees understand their role in protecting both themselves and the organization against cyber threats.

Ultimately, executive leadership ensured that cybersecurity was not just viewed as an IT concern but as a business imperative, providing the necessary support and advocacy for the intensive three-year programme while integrating it into corporate decision-making. As a result, PETRONAS elevated its security posture from reactive to proactive, establishing cyber resilience as an actionable agenda at every level of the organization.

3.2 Governance, risk and compliance

Governance, risk and compliance concerns an organization's approach and governance mechanisms put in place to manage risk and meet compliance requirements. This involves:

- Defining the organization's **risk profile**
- Establishing clear **ownership and accountability** structures
- Ensuring **compliance** with legislative and regulatory requirements
- Implementing **risk mitigation** measures

Examples of front-line practices that organizations are applying:

- Risk-owners across the organization develop risk profiles to provide a structured approach to managing cyber risk within their local purviews, identifying vulnerabilities and impacts and implementing proactive measures. These are combined within the enterprise risk management process to provide an organization-wide view of cyber risk. Such methodical risk assessments include identifying critical assets, evaluating their supporting digital infrastructure, assessing potential threats, analysing existing controls and reviewing past incidents within the organization, sector or broader ecosystem.

- Top leadership establishes transparent ownership and accountability structures and a clear chain of command to empower decision-makers. Individual risk-owners establish roles and responsibilities for key processes, decisions and risk management and communicate these structures, with regular reviews and assessments to ensure that roles adapt to address emerging risks.

- Legal, compliance and cybersecurity teams periodically evaluate legislative and regulatory developments to mitigate legal and financial risks while strengthening the cyber resilience posture. To create robust compliance strategies, they use incident notification requirements, cybersecurity standards, certification frameworks and regulatory fragmentation.

- CISOs and chief revenue officers (CROs) assess cyber insurance as a strategic tool to limit financial losses, legal liabilities, business disruptions and reputational damage caused by cyber incidents. They work closely with insurers and legal teams to meet policy requirements and to maximize coverage benefits.

Experts emphasized the need to ensure that relevant risk-owners across the organization fully understand their exposure to cyber risks, as well as the limitations of what the cybersecurity team can guarantee in terms of system availability, data confidentiality and data integrity. Many highlighted the challenge of embedding responsibility and accountability for managing residual risk within the organization's governance, risk and compliance systems.

A common issue raised was the tendency to treat cyber risk as "the CISO's problem" rather than understanding that cyber risk is business risk. The lack of cyber awareness and a shortage of specialized staff were identified as key factors contributing to this challenge, making it difficult for some risk-owners to grasp the extent of their cyber risk exposures. Additionally, immature regulations and the lack of qualified external advice were cited as barriers in certain regions.

> **It is imperative to get multiple stakeholders in the room – front-line operators, legal, compliance, marketing, risk management, security practitioners and HR – and ask each of them to identify the top three critical scenarios they believe could cause us the greatest financial harm or the most devastating impact on the business connected to other KPIs.**
>
> Gregory Eskins, Head, Global Cyber Insurance Center, Marsh McLennan

CASE STUDY 3

Schneider Electric – Key internal controls in action

Trust is at the core of Schneider Electric's business, with cybersecurity as a critical pillar. Effective cyber risk management extends beyond technology to governance, which is why the company has embedded key internal controls (KICs) within the three-lines-of-defence framework.

The KICs initiative establishes clear accountability for cyber risk mitigation, ensuring that business and operational cyber risk-owners (first line of defence) formally acknowledge risks and implement controls. These efforts are guided by the group CISO (second line of defence) and independently reviewed by internal audit (third line of defence). By making control expectations explicit, KICs eliminate ambiguity and ensure that cybersecurity and product security are integral to operations.

KICs are mapped to company policies and the cyber risk register, which are updated annually by the cybersecurity team. Each year, risk-owners formally sign off on control execution, providing evidence or action plans to address gaps. This structured approach strengthens compliance, enhances business resilience and enables the company to demonstrate security commitments to customers and regulators. By formalizing risk-ownership, KICs mark a significant advance in Schneider Electric's cyber maturity programme, reinforcing the company's proactive stance on cybersecurity and business continuity.

CASE STUDY 4

Dubai Electronic Security Center (DESC) – Securing critical information infrastructure: Dubai's cyber resilience approach

Critical information infrastructure (CII) is essential to the functioning of societies, supporting daily life and powering key sectors such as energy, healthcare, finance, telecommunications and transportation. As the systems become increasingly digital, ensuring their cybersecurity is vital to protecting public safety and economic stability. The Dubai Electronic Security Center (DESC), as the cybersecurity regulator in Dubai, plays a significant role in securing the emirate's CII through a structured, risk-based approach reinforced by regulatory frameworks.

To build the Dubai Cyber Resilience Plan, DESC identified critical sectors, ensuring the protection of critical services and assets that are the backbone of the city's operations.

In collaboration with the designated sector leads, DESC conducted rigorous risk assessments, mapping interdependencies that connect the various sectors to prevent cascading failures that could negatively affect the city's economy and the well-being of its citizens. The Dubai Cyber Resilience Plan includes cybersecurity guidelines and measures for sector leads to implement, such as asset classification, disaster recovery, business continuity planning and incident response plans.

The approach to fortifying Dubai's digital infrastructure integrates regulatory oversight and strategic cybersecurity initiatives, positioning the city as a global leader in cyber resilience.

3.3 People and culture

People and culture encompass an organization's strategies and practices for building and retaining a workforce, as well as empowering employees and equipping them with the necessary cyber skills and awareness. This involves:

- Growing and retaining **talent**
- Implementing **training** and **awareness** programmes to build employee ownership and engagement
- Building a **culture** of psychological safety
- Establishing a **common language** across the organization

Examples of front-line practices that organizations are applying:

- Chief information officers (CIOs), CISOs and human resources (HR) develop robust strategies for talent acquisition, training and retention to build cyber talent capacity in the organization. Organizations first understand the skills they require, then develop targeted recruitment and retention initiatives based on these needs. Approaches include partnerships with universities, cybersecurity boot camps or continuous learning and mentorship programmes.
- Cybersecurity and learning and development teams collaborate to implement cybersecurity training and awareness programmes tailored to different roles to build ownership and engagement and to prevent incidents. Local leadership educates employees on their responsibilities and how their actions affect the organization's cyber resilience. Training programmes are regularly updated to align with evolving threats and business needs.
- CISOs and local leadership cultivate a culture of psychological safety to increase the reporting of incidents and mistakes, to encourage transparency and accountability and ultimately to lead to quicker identification and resolution of issues. CISOs promote open lines of communication and regular feedback loops, paired with organization-wide policies of positive reinforcement for proactive incident reporting, to strengthen trust and to ensure that employees report potential issues.
- CISOs establish a simplified cyber and risk taxonomy to reduce departmental divisions, enhance mutual understanding and integrate cybersecurity into business processes. This unified taxonomy is incorporated into training sessions, risk management frameworks and communication channels to promote communication and collaboration at all levels and in all departments of the organization.

All of the organizations involved in this project had awareness campaigns focused on general cybersecurity and cyber hygiene practices. However, fewer organizations had context-specific programmes that explored in depth digital dependencies in particular areas of the business and consequently the unique cyber risks tied to those parts of the organization. For instance, there were examples where local business continuity plans and exercises did not cover relevant cyber risk scenarios, leaving staff unprepared for such situations. Many experts also highlighted a widespread shortage of specialist staff, which put unsustainable pressure on the available staff during times of crisis. Together with a community of cybersecurity experts, the World Economic Forum has developed the Strategic Cybersecurity Talent Framework featuring achievable approaches to help organizations build sustainable talent pipelines.

> **A company can be resilient only if its people are resilient. There's no point in writing fantastic incident response plans, playbooks and running exercises when, in reality, people drop out because they were already under severe pressure.**
>
> Swantje Westpfahl, Director, Institute for Security and Safety (ISS)

> **We try to make the mistakes during the tabletop exercises, so we learn and we are ready when the problem occurs. It doesn't mean that it will be perfect then, but at least we will be a bit more prepared.**
>
> Elie AbenMoha, Chief IT Security Officer, Publicis Resources

CASE STUDY 5

Engro – Collaborating for cyber resilience: Engaging stakeholders across every level

Cyber resilience cannot be achieved by the cybersecurity team alone; it requires the active engagement of key stakeholders throughout the organization. At Engro, regular tabletop exercises involve those critical stakeholders from information and communications technology (ICT), security, senior management, legal, public relations (PR) and operations to prepare for a serious cyber incident and evaluate the organization's readiness to respond. These exercises follow a structured format that includes developing scenarios based on real-world threats, participant briefings, live role-playing of incidents and post-exercise assessments. A key focus is leadership engagement, with executives actively involved in decision-making simulations, crisis communication drills and impact assessments to replicate real-world cyber incidents.

Past exercises have helped Engro to reveal gaps in detection, response, back-up validation, escalation procedures, decision-making and cybersecurity awareness across teams. Following the exercises, Engro implemented key improvements such as:

- Enhancing incident response plans with clearly defined roles and responsibilities
- Strengthening back-up and recovery strategies to ensure business continuity
- Conducting targeted cybersecurity awareness training for employees, including senior management, streamlining communication between ICT, leadership and PR teams for faster decision-making
- Deploying advanced security solutions and automation tools for real-time threat detection and response

These measures have helped to enhance Engro's cyber resilience, accelerate incident response times and strengthen crisis communication. Leadership involvement ensures that cyber resilience remains a top priority, emphasizing the need for proactive risk management and crisis preparedness.

CASE STUDY 6

Repsol – Resilience in action: The power of training and simulations

As a leading global energy company, Repsol operates critical infrastructure in highly complex digital, cloud and industrial environments. With digitalization and innovation driving the company's growth, ensuring protection against potential cyberthreats while preserving operational continuity presents a core priority of Repsol's operations.

Central to Repsol's resilience strategy is continuous training and education for users, its business operations team and its technical team. This prepares the company to minimize the impact of cyberattacks by enhancing response speed and precision. Frequent crisis simulations with business continuity and technical tests are conducted to improve detection and response capabilities while strengthening the resilience of response teams under stress.

Repsol integrates both red-team simulated cyberattack exercises and tabletop decision-making scenarios, sometimes with no prior notice. Employees from all locations participate, and some exercises escalate to the board level. Lessons learned from these exercises lead to continuous improvements, and to strategies and responses being refined.

This comprehensive approach ensures Repsol's cyber resilience is robust and adaptive, safeguarding its infrastructure and supporting ongoing digital growth by enabling quick and effective responses to cyber incidents.

3.4 Business processes

Business processes describe an organization's approach to prioritizing, designing, implementing and adapting functions. This involves:

- **Prioritizing** and tiering business services
- **Preparing** for worst-case scenarios
- Building **adaptability** and resilience into business operations
- **Reviewing** business processes regularly to meet changing priorities

Examples of front-line practices that organizations are applying:

- Top leadership identifies the most critical business services and tiers them regularly to (re-)prioritize their importance under shifting circumstances. Clarity and prioritization allow enhanced decision-making and effective allocation of resources during a crisis.
- Local leadership anticipates failures and builds key business processes to continue operations despite worst-case disruptions. Business processes embed resilience from the outset with redundancy and acceptance of risk built into process design. Similarly, data protection officers (DPOs), CISOs and local leadership establish information governance policies that mitigate the potential impact of significant data breaches by reducing the volume of data at risk.
- Teams periodically review and refine business processes to meet changing priorities and incorporate lessons from past incidents. Business processes are able to adjust to internal and external factors, such as regulatory and legislative changes, an evolving risk landscape and business priorities, emerging supply-chain dependencies and shifts in digital infrastructure.

Many experts shared examples of collaborating with colleagues within an organization to develop fallback processes, typically as part of business continuity planning. A key challenge is to ensure that these plans consistently include a broad range of relevant cyber risk scenarios. Sectors such as critical national infrastructure and the military often construct business processes to be resilient by design. Examples include eliminating single points of failure, and using the concept of separation of duties, where business process architects assume that an incident will occur and try to minimize its impact. While embedding high levels of inherent resilience into business processes is beneficial, it comes with costs in terms of financial investment and process efficiency. Recent regulations to strengthen operational resilience were cited as a major driver for organizations to focus more on the inherent resilience of their business processes.

> **Identifying 'crown jewels' is challenging because priorities can shift quickly. What is considered low priority today may become critical tomorrow, depending on evolving circumstances and business needs.**
>
> Paulo Moniz, Head, CyberSecurity and Information Technology Risk, EDP – Energias de Portugal

CASE STUDY 7

UBS – Building cyber resilient business processes

UBS recognizes the industry-wide challenge of retaining operational resilience in the face of a dynamic cyberthreat environment and prioritizes the rapid recovery of critical business services following cyber incidents, including third-party outages. This reduces potential harm to clients, business operations and other market participants and minimizes downtime. The firm plans for severe scenarios, assuming critical services could be unavailable for an extended period. This assumption guides contingency planning, which focuses on:

- **Workaround development:** Collaborating with business units, the firm creates procedures to operate without impacted elements, prioritizing key processes to minimize impact.
- **Data storage and access:** UBS utilizes air-gapped vaulting solutions for storing critical applications and data in an immutable format, ensuring heightened security and expedited retrieval to recover key processes in the event of a cyberattack.
- **Communication and coordination:** The company has mature crisis management protocols providing clear communication channels between leadership, IT, business units and clients, ensuring fast and effective decision-making during an incident.
- **Third-party risks:** UBS assumes third-party services might take longer to recover or reconnection may be prolonged, and therefore focuses on developing effective and sustainable workarounds to mitigate those risks.

By focusing on workarounds and strengthening resilience, UBS can continue operations with minimal impact following a cyber incident but also enhances overall agility, improves crisis response efficiency and builds greater confidence among clients and stakeholders.

CASE STUDY 8

IMD Business School – A step ahead: Reducing account compromises and minimizing their impact

Account compromise provides cybercriminals with a straightforward method of generating profit. By bypassing traditional security measures such as passwords and multifactor authentication (MFA), hackers can steal sensitive information, including personal details, financial data and log-in credentials. To address this concern, IMD Business School enforces strong password hygiene, number matching and context-based MFA prompts. It also strengthens phishing protection through security awareness training, advanced email filtering and risk-based access controls that block suspicious log-ins.

However, acknowledging that not all compromises can be prevented, IMD Business School has established key damage control measures:

- **Limit email exposure:** Restrict the number of emails an employee can send within a set time frame to reduce phishing risks.
- **Block self-service MFA registration:** To prevent attackers from adding their own devices during an account compromise, users must contact IT Support to register new MFA devices.
- **Restrict uploads of "IMD Confidential" files:** Documents labelled "IMD Confidential" cannot be uploaded to unsanctioned cloud storage or external USB devices. Automatic labelling identifies sensitive files based on patterns such as files including 20+ email addresses.
- **Block downloads to personal devices ("bring your own device" – BYOD):** Prevents sensitive documents from being saved on unmanaged devices, reducing insider threats and data leaks.

Through its proactive security practices, IMD Business School effectively reduces the number of successful account compromises. Equally important, IMD Business School's robust damage control measures – restriction of certain functions – ensure that even if an incident does occur, the impact is minimized, safeguarding the organization's sensitive data and systems.

3.5 Technical systems

Technical systems describe an organization's approach to designing, deploying and maintaining IT, OT, cloud and cybersecurity tools and controls, whether in-house, outsourced or hybrid. This involves:

- Understanding business **prioritization** of services
- Using **data** to prevent and predict incidents
- Implementing **technical controls** as preventive measures and to minimize the impact of incidents
- Evaluating **tooling** based on problems, outcomes and organizational context

Examples of front-line practices that organizations are applying:

- CISOs build awareness among the organization's technical teams of how the business operates, so these teams understand the best ways to protect the most important services and assets. Organizations train technical teams on risk assessments and impact analyses, ensuring that technical staff gain a clear understanding of business priorities and align their security efforts with the organization's strategic objectives.
- Technical teams use data as a key differentiator in crises to enable faster response, thorough investigation and detection of minor issues before they escalate into major disruptions. This includes collecting and integrating real-time information from various sources and applying advanced analytics and AI models to identify emerging issues early, coordinate responses quickly and prevent minor problems from escalating into much more significant issues.
- Technical teams implement and periodically review hardening techniques, contingent technology and fundamental technical controls to prevent incidents, create redundancy during crises and minimize impact. Those techniques include infrastructure segmentation and segregation, MFA, secure back-ups, log management, leveraging threat intelligence, adherence to standards and consistent cyber hygiene practices.

– CISOs and technical teams evaluate tools to assess their effectiveness in achieving the desired outcomes and to ensure the best fit for the organization's needs. This includes understanding case studies of similar organizations and conducting regular value assessments.

Most experts acknowledged progress has been made in raising cyber hygiene, but several pointed out that basic practices were still not being implemented universally. Others highlighted the challenge of technical debt – systems and architectures that are no longer supported or lack mitigations to prevent incidents from propagating. Just as risk-owners may not fully understand the technology behind their critical business services, technical teams sometimes fail to grasp the business priorities of the front-line operations they are intended to support. Investments in technical controls are not always aligned with the most relevant risks to the business.

> **We are thinking about potential disruptions when designing our systems. We take the premise that everything that can go wrong will go wrong, so we prepare our systems to withstand multiple points of failure and avoid single points of failure.**
>
> Deryck Mitchelson, Global Chief Information Security Officer, Check Point Software

> **I try to analyse the major attacks that occur both in the financial as well as other industries to understand the attack tactics and exploits, and if my controls would have failed in that situation to learn from it.**
>
> Jeff Farinich, Senior Vice-President, Technology Services; Chief Information Security Officer, New American Funding

CASE STUDY 9

Splunk – Beyond "tooling": A focus on quality and ecosystem collaboration

Building a security operations centre (SOC) is a complex endeavour that requires the balancing of speed, efficiency and quality in threat detection and response. Building a SOC comes with challenges such as ensuring an outcome-driven approach rather than a tool-centric one, maintaining scalability and standardization across operations, managing resource limitations and integrating emerging technologies while ensuring interoperability and effectiveness.

Splunk's approach to SOC operations addresses these challenges by focusing on quality and operational outcomes rather than simply resolving tickets quickly or deploying the latest security tools. This encompasses:

– **Data-driven decision-making:** Splunk ensures technology investments align with security outcomes, enhancing detection, response and resilience.

– **Automation for efficiency:** Automated processes reduce human error, ensure consistent responses and allow analysts to focus on higher-level tasks.

– **Improved detection and response:** Splunk achieves detection times of less than seven minutes for critical threats while enhancing collaboration and expanding services without adding resources.

– **Partnership-driven innovation:** Collaborating with vendors, including non-Splunk solutions, ensures tools meet operational needs and contribute to a stronger security ecosystem.

Building an effective SOC requires more than just assembling security tools – it demands a strategic approach focused on outcomes, automation and continuous improvement. Splunk's operations centre exemplifies this by ensuring high-quality, scalable security operations while promoting innovation through partnerships, ultimately strengthening overall resilience by enhancing adaptability and operational consistency.

CASE STUDY 10

Siemens Energy – Accelerating detection and response: Strengthening OT resilience

After acquiring the High Desert Power Plant in California, the private equity firm Middle River Power identified cyber threats to its operational technology (OT) assets as a critical risk. Limited visibility, evolving cyber threats and compliance challenges made it difficult to detect and respond to incidents effectively. To improve detection and response capabilities without disrupting operations, the company sought a comprehensive monitoring solution.

Middle River Power collaborated with Siemens Energy to deploy managed detection and response (MDR) services at the plant. Siemens Energy's analysts, operating from a remote security operations centre (SOC), leverage machine learning and OT expertise to continuously monitor and analyse data, enabling rapid detection of potential anomalies.

Moreover, MDR helps Middle River Power to accurately determine which systems have been compromised in the event of an incident. The implementation of MDR also supports regulatory compliance by providing structured security reporting and audit-ready documentation.

One immediate benefit of MDR was the early detection of an operational issue – an on-site historian that periodically overheated and rebooted. The system flagged this anomaly, enabling plant operators to resolve the issue before it escalated. Beyond identifying vulnerabilities, MDR allowed Middle River Power to accelerate incident response, reduce downtime and improve compliance efficiency, ultimately increasing the plant's cyber resilience.

3.6 Crisis management

Crisis management describes all components that an organization uses to respond to and recover from incidents and other crises that affect its resilience. This involves:

- Building and training crisis **response** teams
- Designing and reviewing **plans**
- Defining **decision-making** protocols
- **Preparing** for incidents by establishing alternative technical systems
- Developing strategies for external **communication**

Examples of front-line practices that organizations are applying:

- CISOs and top leadership establish and exercise crisis response teams that include senior executives and multidisciplinary experts to address various aspects of a cyber incident. To act swiftly during a crisis, teams are created before the crisis and trained to ensure familiarity with response plans and communication channels.
- Process owners develop and maintain plans for business continuity, disaster recovery and incident response to ensure preparedness and effective internal communication. Process owners and implementers practise, refine, test and tailor plans to align with organizational context. Consistent processes and policies ensure all departments adhere to the same standards.
- Top leadership supported by the CISO defines and refines decision-making protocols and managerial responsibilities to enable a rapid response, particularly in crisis escalation processes. They implement robust risk management analysis and strong trust mechanisms to empower teams at all levels to make decisions for effective and coordinated responses. Some organizations pre-emptively approve rapid response actions that can be taken when certain risk thresholds are met.
- Technical teams build infrastructure to prepare for the case of a serious incident. This includes measures such as creating "vaults" to protect critical data by storing it in an isolated environment or establishing alternative back-up communication channels (e.g. out-of-band) to secure communication even when core IT systems have been compromised or are unavailable.
- PR teams supported by the CISO and legal teams prepare strategies for external communication during cyber incidents to rapidly address mis- and disinformation and re-establish trust with key stakeholders. This includes mapping those stakeholders in advance and developing predetermined messaging frameworks to ensure swift communication during an incident.

Most of the experts consulted have crisis plans and playbooks in place, and most regularly conduct exercises, though it can be hard to effectively engage external third-party suppliers and ensure that all potential scenarios are considered. When major incidents affect multiple organizations simultaneously, ensuring quick access to the right sources of external expertise can be challenging. Alternative communication channels during a crisis are needed, and sometimes these arrangements are ad hoc. Keeping a clear record of decisions made and the information supporting these decisions is important, too. Crises provide opportunities for organizations to learn, but often organizations learn only from incidents that have negatively affected them, whereas there are also valuable insights in successfully managed incidents.

> **As digitalization accelerates and cyberthreats grow, we recognized the need to integrate IT/OT expertise into our emergency and crisis response. We have invested heavily in building robust plans, training cross-functional teams and preparing our organization to handle both traditional and cyber-driven crises.**
>
> Sigmund Kristiansen, Chief Cyber Security Officer, AkerBP

CASE STUDY 11

Henkel – Rethinking IT resilience: Building recovery from ransomware

Traditional IT service continuity plans – which are built around the assumption of physical threats such as natural disasters – often fail to adequately address the unique nature of modern cyberattacks, especially ransomware. Ransomware attacks do not just disrupt infrastructure in the same way as physical events; instead, they target primary and failover systems alike.

Recognizing the growing threat of ransomware and the need for strong cyber resiliency, Henkel, a leading global company in adhesive technologies and consumer goods, took a proactive approach. To ensure rapid recovery and minimize downtime, the company undertook a comprehensive review of its IT architecture and continuity strategies, identifying several key initiatives:

- **Green network for rapid recovery:** An isolated "green network" across global sites and cloud infrastructure enabling the immediate recovery of operations independent of ongoing forensic investigations, ensuring the swift restoration of critical services.
- **Prioritized recovery with immutable back-ups:** Clear recovery priorities for business-critical workloads, alongside a robust back-up strategy that uses immutable back-ups to protect against data tampering.
- **Enhanced end-user device recovery:** Site-specific procedures for the rapid reimaging of end-user devices at scale (restoring or reinstalling an operating system and software to a known, secure state), reducing recovery times and minimizing disruptions.

By addressing the specific challenges posed by ransomware, Henkel is significantly strengthening its cyber resilience. The new approach has enabled faster recovery, empowering the company to better withstand cyberthreats.

3.7 Ecosystem engagement

Ecosystem engagement describes an organization's approach and practices in interacting with its wider ecosystem, including its supply chain, customers, competitors and regulators. This involves:

- Building **visibility** of upstream and downstream dependencies with external parties
- Consistently **assessing risk** bidirectionally with dependent parties
- Responding in **partnership** with external actors
- **Sharing information** in external forums
- **Adapting** to the changing technical, operational and regulatory environment

Examples of front-line practices that organizations are applying:

- CISOs, in collaboration with business units, identify critical dependencies and single points of failure by improving visibility and developing an accurate mapping to evaluate third-party risks. An accurate mapping recognizes that supply chains are non-linear, that an issue can propagate up or down the supply chain, that organizations can be both a supplier and customer, and that a single third party can hold multiple roles.
- CISOs evaluate third-party cybersecurity postures by establishing a consistent risk assessment methodology and collaborating with front-line business units and procurement teams in establishing mitigation measures. Approaches include using comprehensive questionnaires, implementing contractual requirements and collaborating with third parties to improve their capacities to respond, continue operations and mitigate impact in case of an incident.
- CISOs introduce playbooks that go beyond the immediate organization to enable faster and more effective remediation. This includes proactive collaboration with key partners, cross-organizational exercising and building relationships long before a crisis occurs.
- Organizations engage frequently and actively in information-sharing networks to identify threats faster, proactively mitigate vulnerabilities, share resources and manage systemic risk. These networks can include information security and analysis centres (ISACs), computer emergency response teams (CERTs) or other forms of collaboration, involving partnerships with governments and private-sector entities, including competitors, customers and suppliers.
- CISOs and legal teams ensure the organization remains adaptable to and engages with developments in the wider ecosystem to improve visibility of incoming changes and capacity to adapt to the new environment. This includes engagement with regulatory bodies, policy-makers and industry bodies to stay adaptable to regulatory, policy and technology developments.

Experts agreed that while organizations can take significant steps to enhance their own cyber resilience, this individual posture can depend heavily on the resilience of the broader ecosystem, which requires collaborative action. This collaboration should focus on: identifying and addressing single points of failure; optimizing the use of limited cyber talent while working to expand this talent pool over time; engaging with regulators to encourage cyber resilience throughout the ecosystem; developing a more efficient and effective systemic approach to supply assurance than current practices; and proactively addressing threats while finding ways to disrupt those who seek to exploit cyber vulnerabilities.

> **The industry has to be engaged in any solution. It can't be sort of a government in a vacuum or regulate errors without working with industry to understand what a model would look like and how they can do it.**
>
> Michele Mosca, Chief Executive Officer, evolutionQ

CASE STUDY 12

The Business Resilience Council – Coordinating the response to a global IT outage

In 2024, a widespread IT outage disrupted more than 8.5 million devices globally, bringing essential services to a standstill, including healthcare providers, government agencies, financial services and critical infrastructure operators. Minimizing operational downtime and business impact became the top priority, requiring organizations to urgently access threat intelligence, implement remediation strategies and execute a coordinated incident response.

The Business Resilience Council (BRC), a non-profit, all-sector collective defence community, quickly activated its resilience framework to facilitate a multiorganization response. With more than 2,000 engaged organizations, the BRC leveraged its network to rapidly analyse, collaborate and implement mitigation efforts:

- By 03.00 Eastern time (ET), cross-sector analysts in the BRC chat had identified the root cause of the issue.
- By 09.00 ET, rough solutions had been formulated.
- By 13.00 ET, more than 150 global organizations had joined a BRC-hosted call to refine mitigation strategies and share intelligence.
- Within two business days, BRC had hosted a joint ISAC briefing with more than 1,500 participants, providing exclusive, legally protected insights before public disclosures.

This coordinated, intelligence-driven response enabled organizations to reduce downtime by: accelerating root-cause analysis and remediation; minimizing uncertainty by sharing real-time, actionable intelligence; enhancing cross-sector collaboration, thus reinforcing collective cyber resilience; and strengthening future mitigation strategies, integrating lessons learned.

By fostering pre-established relationships and engaging vendors, suppliers and security teams ahead of incidents, the BRC demonstrated how collective defence can mitigate widespread cyber disruptions. The incident serves as a model for how rapid, coordinated response efforts can enhance organizational and national cyber resilience.

CASE STUDY 13

Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT) – The power of information sharing: Combating phishing attacks in Bangladesh

Bangladesh has faced a surge in phishing attacks targeting government agencies, law enforcement and educational institutions. Attackers impersonate official entities using spoofed domains, malicious attachments and fraudulent links to steal credentials and sensitive information. Traditional security measures often focus on reactive threat responses, struggling to keep pace with attackers' evolving tactics. The challenge lies in shifting from a tool-centric, detection-based approach to an intelligence-driven, proactive security strategy that prioritizes outcomes – minimizing successful attacks and strengthening long-term cyber resilience.

The BGD e-GOV CIRT plays a key role in advancing this collaborative, intelligence-driven resilience model through three key elements:

- **Threat identification:** Continuous monitoring and investigation of malicious domains, fraudulent email campaigns and attack patterns to uncover evolving phishing tactics.
- **Detection and prevention support:** Development of intelligence-driven detection rules to enhance cybersecurity defences.
- **Stakeholder alerts and risk mitigation:** Delivery of timely alerts and actionable insights to government agencies and security teams, enabling pre-emptive actions to block phishing attempts.

Through cybersecurity threat intelligence and early-warning capabilities, BGD e-GOV CIRT strengthened threat detection, improved incident response coordination and promoted a proactive security culture across critical sectors in the country, contributing to stronger national cyber resilience.

Conclusion and next steps

Using the Cyber Resilience Compass to share front-line cyber resilience strategies that work will help organizations ready themselves for ever-changing future challenges.

Cyber resilience is no longer optional; it has become a fundamental requirement for organizations in an increasingly digital and interconnected world. As it is becoming impossible to prevent all cyber incidents, it is essential to shift the focus from prevention to a cyber resilience mindset – minimizing incidents' potential impact on critical objectives, stakeholder confidence and long-term growth.

There is no one-size-fits-all solution to cyber resilience, as each organization's approach must be tailored to its specific context and goals. However, by sharing knowledge and learning from front-line experiences, organizations can make well-informed decisions when building their cyber resilience strategies. The Cyber Resilience Compass, showcasing front-line practices in seven categories, seeks to provide the valuable insights that can help organizations develop and refine their cyber resilience journey.

Looking ahead, more work is needed to move from individual success stories to a scaled, structured approach to resilience. The aim is for the Cyber Resilience Compass to become a vehicle for the exchange of front-line experiences and insights – a dynamic tool that serves as a reference for cyber leaders to enhance their cyber resilience strategies. Building on the leading insights in this report will help organizations transition to a more consistent, measurable and future-ready approach to cyber resilience. Please access additional insights and contribute to the Cyber Resilience Compass here.

Methodology

This paper is anchored in the thematic analysis of five virtual community workshops, two in-person expert community workshops, five smaller virtual working groups and 39 semi-structured one-on-one consultations, which took place between May 2024 and March 2025. A total of 102 experts from 84 different organizations participated in the discussions and consultations.

While most participants held positions specifically overseeing cybersecurity – such as CISOs and chief technology officers (CTOs) – a diverse array of profiles participated, including chief executive officers and consultants. The representation included 18 different industry sectors and participants from North America, South America, Europe, Africa, Asia and Oceania.

Contributors

Lead author

Luna Rohland
Specialist, Cyber Resilience,
World Economic Forum

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Kirsty Paine
Project Fellow, Cyber Resilience, World Economic Forum; Field Chief Technology Officer, EMEA, Splunk

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 with the contribution of many 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 virtual and in-person workshops, events and one-to-one consultations. The World Economic Forum would like to thank the following individuals for their insights and feedback:

Claudia Jacy Barenco Abbas, University of Brasilia

Elie AbenMoha, Publicis Groupe

Mansur Abilkasimov, Schneider Electric

Michael Adams, Zoom Video Communications

Paige Adams, Zurich Insurance Company

Tamim Ahmed, BGD e-GOV CIRT

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

Yasser N. Alswailem, Saudi Telecom Company (STC)

Ricardo Amper, Incode Technologies

Romain Aviolat, Kudelski Group

Sanjay Bahl, Indian Computer Emergency Response Team (CERT-In)

Nik Bartholomew, Occidental Petroleum Corporation

Alejandro Becerra, Telefónica

Mauricio Benavides, Metabase Q

Janus Friis Bindslev, PensionDanmark

Arnab Bose, Okta

Jalal Bouhdada, DNV

Grant Bourzikas, Cloudflare

Duncan Bradley, Kyndryl

Stefan Braun, Henkel

Marijus Briedis, Nord Security

Ian Buffey, AtkinsRéalis

Hazel Diez Castaño, Santander

Ronald Charron, Canadian Centre for Cyber Security

Nic Chavez, DataStax

Piotr Ciepiela, EY

Larry Clinton, Internet Security Alliance

Steve Cobb, SecurityScorecard

Stefan Deutscher, Boston Consulting Group

Donna Dodson, evolutionQ

James Dolph, Guidewire Software

Ali El Kaafarani, PQShield

Mohammed Elofi, Gulf International Bank BSC (GIB)

Gregory Eskins, Marsh McLennan

Peter Evans, New South Wales Police Force

Yusuf Ezzy, PG&E

Jeff Farinich, New American Funding

Sabrina Feng, London Stock Exchange Group

Jacky Fox, Accenture

John Frazzini, X-Analytics

Sam Gabbai, PayPal

Jonathan Gill, Panaseer

Tracie Grella, American International Group (AIG)

Paul Guckian, Lloyd's

Jassim Happa, Royal Holloway, University of London

Khawla Hassan, Dubai Electronic Security Center (DESC)

Ronald Heil, KPMG

Paul Hopkins, Vodafone

Maman Ibrahim, Ginkgo Resilience

Rotem Iram, At-Bay

Öykü Isik, IMD Business School

Amit Jain, HCLTech

Debbie Janeczek, SWIFT

Lawrence Jarvis, Iron Mountain Information Management

Rosa Kariger, Iberdrola

Anssi Kärkkäinen, Finnish Transport and Communications Agency (Traficom)

Engin Kavas, Aydem Enerji

Shaun Khalfan, PayPal

Andreas Kind, Siemens

Sigmund Kristiansen, Aker BP

Ryan Lasmaili, Vaultree

Simon Leech, Hewlett Packard Enterprise

Shawn Lonergan, PricewaterhouseCoopers

Kris Lovejoy, Kyndryl

David Mabry, Gulfstream Aerospace

Rishi Mehta, HCLTech

Michael Meli, Bank Julius Bär

Deryck Mitchelson, Check Point Software Technologies

Aysha Mohammed, Dubai Electronic Security Center (DESC)

Saket Modi, Safe Securities

André Luiz Bandeira Molina, Secretariat of Information and Cyber Security of the Institutional Security Office (GSI/SSIC)

Paulo Moniz, EDP – Energias de Portugal

Sean Morton, Trellix

Michele Mosca, evolutionQ

George Moser, S&P Global

Emmanuel Mugabi, Centenary Technology Services

Tejas Mulay, Bajaj Financial Services

Claus Norup, Euroclear

Laura Jiménez Orgaz, Santander

Natalia Oropeza, Siemens

Mark Orsi, Global Resilience Federation

Pankaj Paul, Burjeel Holdings

Christoph Peylo, Robert Bosch

Andy Powell, Mærsk

Javier Garcia Quintela, Repsol

Rahayu Ramli, PETRONAS

Philip Reitinger, Global Cyber Alliance

Cyril Reol, Mercuria Energy Group Holding

Craig Rice, Cyber Defence Alliance

Katheryn Rosen, JPMorgan Chase

Jason Ruger, Lenovo

Mehzad Sahar, Engro

Jesús Sánchez, Naturgy

Andreas Schmitt, Zurich Insurance

Ralf Schneider, Allianz

Arno Sevinga, Royal Vopak

Vikram Sharma, QuintessenceLabs

Leo Simonovich, Siemens Energy

Colin Soutar, Deloitte

Alex Spokoiny, Check Point Software Technologies

Mark Stamford, OccamSec

Ian Tien, Mattermost

Alex Tiley, CLS Bank International

Phil Tonkin, Dragos

Marc Uldry, IMD Business School

Prashant Verma, Bajaj Finance

Luke Vile, Financial Conduct Authority (FCA)

Alexander Ward, Thales

Swantje Westpfahl, Institute for Security and Safety (ISS)

Ollie Whitehouse, UK National Cyber Security Centre (NCSC)

David Wilson, UBS

Kate Yamashita, Accenture

Suman Ziaullah, Financial Conduct Authority

Production

Bianca Gay-Fulconis
Designer, 1-Pact Edition

Simon Smith
Editor, Astra Content

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