by Adam D'Arcy

# Cyber Resilience Top 3

The "Cyber Resilience Top 3" is a focused framework, highlighting the most critical challenges and actionable solutions to strengthen organisational cybersecurity resilience.

Understanding cyber resilience is critical for organisational decision-makers as they strive to strengthen defences against escalating cyber threats. This study assesses organisational readiness across three phases of resilience—resistance, response, and recovery—while acknowledging that attempted cyber breaches are nearly inevitable and represent a constant risk to organisational security.

Drawing on a 2024 survey of 49 organisational leaders across nine industries and five continents, guided by the World Economic Forum's Cyber Resilience Index, we analyse current resilience postures and identify three central challenges to organisational cyber resilience.

## 1. Cultivate a Culture of Cyber Resilience

1 | 2 | 3 | 4

### Leadership and Management Support

Appoint dedicated cybersecurity culture leaders or teams to drive change and align initiatives with the broader organisational culture.

### Behaviour-Focused Training

Transition from compliance-driven activities to Behavior-focused initiatives that simplify policies into actionable and relatable goals.

### Employee Engagement

Enlist cybersecurity champions to provide localised support and leverage targeted communication to foster shared values.

### Incentivisation Mechanisms

Implement rewards for positive behaviours to reinforce vigilance and responsibility.

To enhance cybersecurity culture, organisations should prioritise leadership and management support by appointing dedicated cybersecurity culture leaders or teams to drive change and align initiatives with the broader organisational culture. Training programs should transition from compliance-driven activities to behaviour-focused initiatives that simplify policies into actionable and relatable goals. Engaging employees across all levels is essential, with strategies such as enlisting cybersecurity champions to provide localised support and leveraging targeted communication to foster shared values. Incentivisation mechanisms, such as rewards for positive behaviours, can reinforce vigilance and responsibility.

## 2. Embrace Cyber Resilient Paradigms

1 | 2 | 3

### Assume Compromise Mindset

Shifts focus from prevention to proactive detection, preparation, and response. Leverages tools like threat modelling and frameworks such as MITRE ATT&CK to anticipate adversary behaviours and strengthen defences.

### Zero Trust Architecture

Enforces strict access controls, continuous monitoring, and granular segmentation, ensuring every access request is verified.

### Secure by Design

Embeds security into the development and design phases, minimising vulnerabilities and ensuring robust defences from the outset.

Assuming compromise, embracing Zero Trust Architecture and enabling through Secure by Design transform cybersecurity from a reactive discipline to a strategic discipline, enabling organisations to minimise risks, recover swiftly, and maintain operational continuity in an era of advanced threats. Microsoft's success in handling the SolarWinds attack through rigorous monitoring and zero-trust principles exemplifies this approach, in contrast to Equifax's failure to address vulnerabilities, which exacerbated the impact of their breach.

## 3. Communication and Reporting

1 | 2 | 3 | 4

### Establish Clear Collaboration Governance

Define roles, responsibilities, and timelines to foster alignment across teams.

### Consistent Communication of Cyber Resilience Health

Provide structured updates to stakeholders for a comprehensive understanding of ongoing efforts and risks.

### External Reporting and Threat Intelligence Sharing

Share threat intelligence with peers and partners to build a collective defense against evolving threats.

### Integrate Key Performance Indicators

Measure progress, identify gaps, and refine strategies effectively.

Threat intelligence can furnish security teams with the information they need to detect attacks sooner, reducing detection costs and limiting the impact of successful breaches. Together, these practices create a robust framework for driving improved collaboration and transparent reporting, ultimately enhancing overall cyber resilience.

## Conclusion

In conclusion, addressing the challenges of cultivating a culture of cyber resilience, embracing cyber resilient paradigms, and improving communication and reporting can significantly enhance organisational cyber resilience in 2024. A robust cybersecurity culture supported by leadership-driven initiatives and comprehensive training programs ensures that employees are actively engaged in maintaining security. The "assume compromise" mindset shifts the focus to proactive detection and response, leveraging tools like threat modelling and frameworks such as MITRE ATT&CK to anticipate and counter threats effectively. Secure by Design further reinforces defences by embedding security into the development lifecycle, reducing vulnerabilities and long-term costs. Lastly, fostering collaboration through defined governance, transparent reporting, and sharing threat intelligence promotes a unified defence against evolving threats. These improvements enable organisations to build resilience, recover swiftly from incidents, and maintain trust and operational continuity in an increasingly complex threat landscape.

---

***References***-The Cyber Resilience Index: Advancing Organizational Cyber Resilience;Protecting from Within: a review of the PSNI data breach 8th August 2023;Building a Security Propaganda Machine: The Cybersecurity Culture of Verizon Media;Building a Model of Organizational Cybersecurity Culture Identifying Factors Contributing to a Cyber-secure Workplace;Developing a cyber security culture: Current practices and future needs;Developing cybersecurity culture to influence employee behavior: A practice perspective;A Systematic Study of the Control Failures in the Equifax Cybersecurity Incident;Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense;Microsoft Internal Solorigate Investigation - Final Update;ED 21-01: Mitigate SolarWinds Orion Code Compromise;Threat Modeling: Designing for Security;Why Defenders Should Embrace a Hacker Mindset;ATT&CK 101;Benchmarking Security Skills: Streamlining Secure-by-Design in the Enterprise;Microsoft Security-What is Zero Trust?;Moving the U.S. Government Toward Zero Trust Cybersecurity Principles;Improving the Nation's Cybersecurity(2021-10460 (86 FR 26633));Zero Trust Architecture Implementation: Strategies, Challenges, and Best Practices;Zero Trust Architecture (ZTA): A Comprehensive Survey;Ivanti-2024 State of Cybersecurity Report;Trustworthy and Effective Communication of Cybersecurity Risks: A Review;A Framework for Effective Corporate Communication after Cyber Security Incidents;Observing Cyber Security Incident Response: Qualitative Themes From Field Research;Human-Human Communication in Cyber Threat Situations: A Systematic Review;IBM-What is Threat Intelligence?