



**P2D**  
TECHNOLOGY SERVICES

# **ENHANCING ORGANISATIONAL RESILIENCE:**

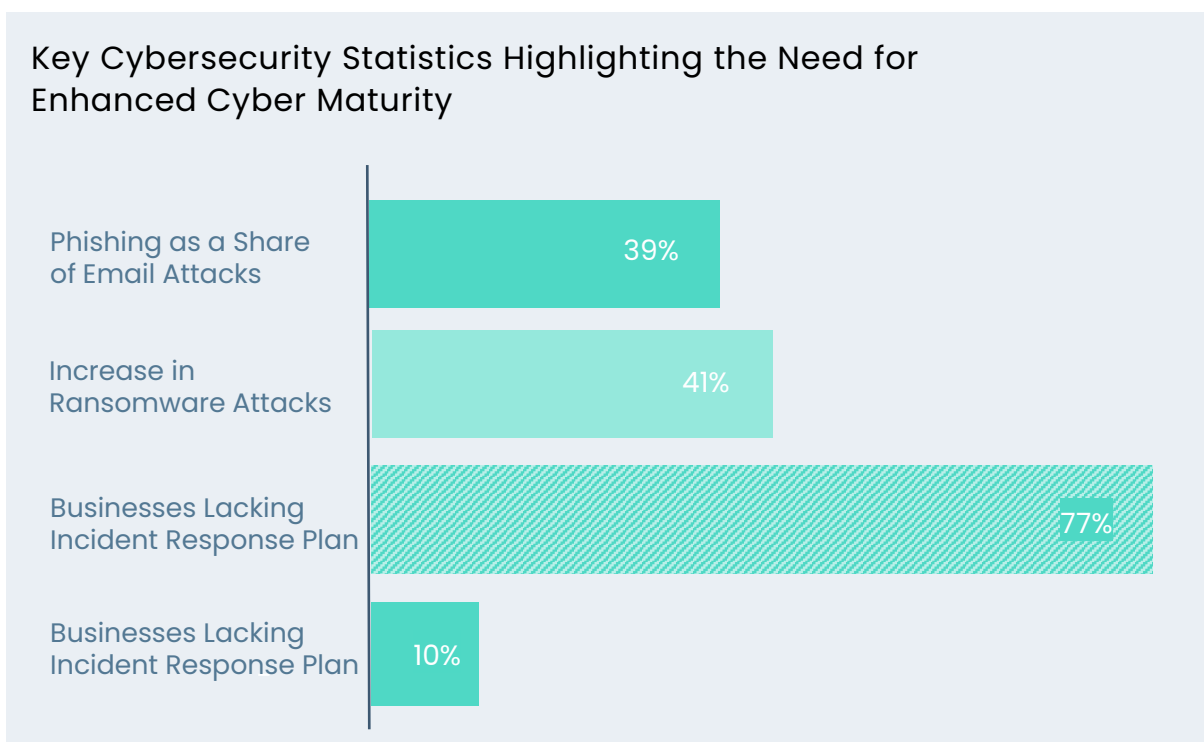
## **A Strategic Approach To Cyber Maturity**

# Introduction

In today's digital landscape, achieving cyber maturity is imperative for businesses striving to protect their operations from escalating cyber threats. The financial impact of cybercrime is projected to be staggering, with costs expected to reach \$10.5 trillion annually by 2025. This alarming projection underscores the urgent necessity for robust cybersecurity strategies.

However, many organisations are still lagging; 77% of businesses lack an incident response plan, leaving them vulnerable to potentially devastating attacks. Recent statistics reveal that ransomware attacks have surged by 41%, with remediation taking significantly longer than other types of breaches. Furthermore, phishing remains a predominant threat, constituting 39.6% of all email attacks. The complexity of these threats highlights the necessity for a comprehensive approach to cyber maturity, integrating risk management, incident response, and continuous monitoring.

Adopting a strategic approach to cyber maturity not only mitigates risks but also aligns cybersecurity efforts with business objectives. As noted by industry experts, the focus should be on building resilient processes and enhancing workforce skills to adapt to evolving threats.



This copy outlines the journey towards cyber resilience, emphasising a risk-based approach and detailing three stages: foundational, advanced, and digital resilience.

Key insights reveal the variability of cyber maturity across sectors, the correlation between higher maturity and profitability, and the challenges organisations face in improving their cybersecurity practices.

Additionally, best practices and strategies employed by leading organisations are highlighted, urging cybersecurity professionals to prioritise maturity assessments, invest in advanced capabilities, and foster a security-centric culture within their organisations. This strategic approach is essential for achieving holistic digital resilience and ensuring business continuity in the face of evolving cyber threats.



With cybercrime costs projected to reach \$10.5 trillion annually by 2025, achieving cyber maturity is more crucial than ever.



A person with short, wavy hair is shown in profile, looking towards the right. They are wearing a dark jacket. The background is a vibrant, futuristic setting with glowing blue and purple neon lights, creating a sense of depth and technology. The overall mood is high-tech and forward-looking.

# THE CYBER MATURITY JOURNEY

Organisations are progressively shifting towards a risk-based approach to cybersecurity, acknowledging that a one-size-fits-all strategy for protecting digital assets is neither feasible nor effective.

While cybersecurity encompasses the practices, technologies, and processes designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access, cyber maturity, on the other hand, refers to an organisation's capability to manage and mitigate cybersecurity risks effectively as it evolves. It involves the development and implementation of comprehensive security measures that grow in sophistication and integration as the organisation advances. The journey towards achieving robust cyber resilience is typically characterised by a maturity curve, with distinct stages that mark an organisation's progression and sophistication in managing cybersecurity threats.

**FOUNDATIONAL STAGE**

At the foundational stage, cybersecurity is often an afterthought. Many organisations at this level are just beginning to recognise the importance of basic security measures. They must build essential security capabilities to address existing vulnerabilities. This stage often involves establishing baseline security protocols, conducting initial risk assessments, and beginning to implement fundamental controls to safeguard against common threats.

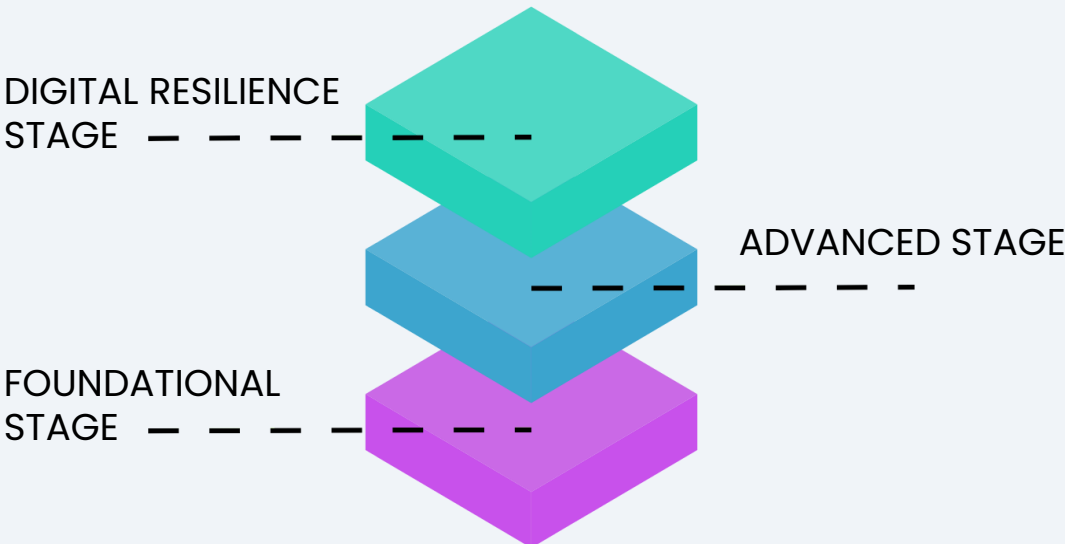
**ADVANCED STAGE**

In the advanced stage, organisations move beyond basic protections and start focusing on reducing enterprise risk through a comprehensive cyber resilience framework. This phase includes identifying, prioritising, developing, managing, and measuring security controls aligned with enterprise risk management strategies. Companies at this stage often implement more sophisticated tools and processes, such as advanced threat detection systems, regular security audits, and incident response plans to handle potential breaches.

**DIGITAL RESILIENCE STAGE**

The final stage, digital resilience, involves deeply embedding security measures within all technology products and processes from the outset. This stage is characterised by the principle of "security by design," where security considerations are integrated into every aspect of the development and operational lifecycle. Organisations at this level adopt proactive measures such as continuous monitoring, advanced analytics for threat intelligence, and robust data protection mechanisms to ensure ongoing resilience against evolving cyber threats.

**Stages of Cyber Maturity**



# Seven Action Areas of Digital Resilience

To advance in their cyber maturity journey, companies must develop specific capabilities grouped into seven key action areas. These areas are designed to align with industry standards such as the NIST Cybersecurity Framework, ensuring a comprehensive approach to digital resilience.

## 1. Deploy Active Defences

The first area involves implementing proactive defence mechanisms. This includes cyber intelligence and vulnerability awareness programmes that help organisations anticipate and mitigate potential threats. Active defences such as threat hunting and real-time monitoring are crucial for identifying and neutralising threats before they can cause significant damage.

## 2. Monitoring and Analytics

Continuous monitoring and analysis of security threats are essential for maintaining robust cybersecurity. This involves using advanced analytics to detect anomalies and potential security breaches in real time with an emphasis on the importance of monitoring tools that provide visibility into network activity and alert security teams to suspicious behaviour.

## 3. Security Integration

Embedding security measures deeply into the technology environment is another critical area. This means incorporating security protocols and controls into every layer of the IT infrastructure. Integrating security into the development lifecycle (DevSecOps) ensures that security is a fundamental component of technology deployment.

## 4. Incident Response

Developing and enhancing incident response capabilities through realistic simulations is crucial for preparing organisations to handle

cyber incidents effectively. Conducting regular drills and tabletop exercises helps refine response strategies and improve coordination among response teams.

## 5. Differentiated Protection

Ensuring enhanced protection for the most critical assets is crucial. Organisations must allocate resources to prioritise safeguarding high-value assets that, if compromised, could significantly impact business operations. Implementing a tiered security model that assigns stricter controls and monitoring to critical systems and data is essential.

## 6. Stakeholder Integration


Incorporating customers, partners, third parties, and regulators into enterprise resilience management ensures a holistic approach to cybersecurity. This involves establishing clear communication channels and collaborative frameworks with all stakeholders to enhance an organisation's ability to respond to and recover from cyber incidents.

## 7. Governance and Risk Management

Finally, establishing a robust cyber operating model, setting risk thresholds, and managing key risk and performance indicators are foundational for effective cybersecurity governance. Having a well-defined governance structure and clear risk management policies helps organisations align their cybersecurity efforts with overall business objectives.

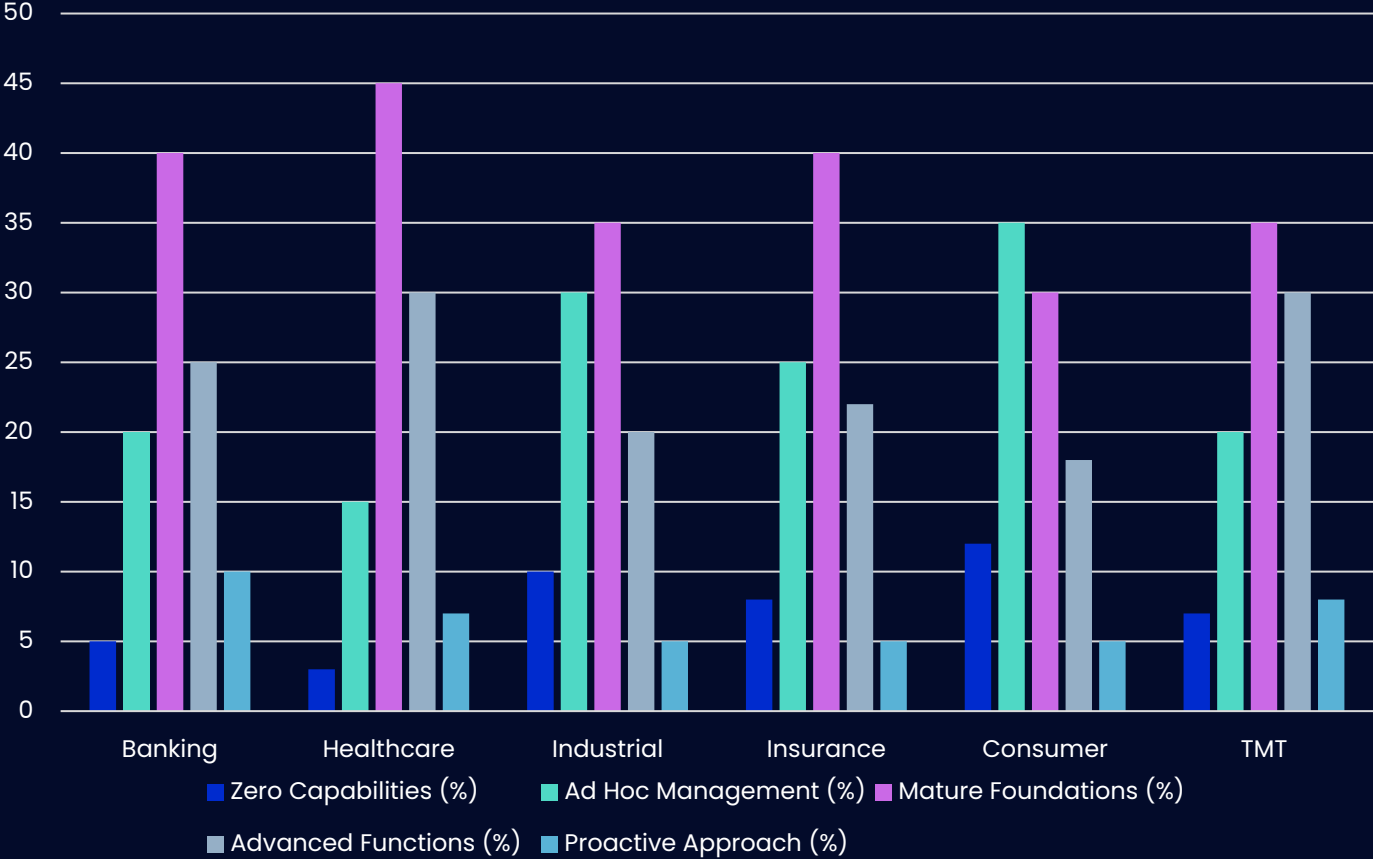


# CURRENT STAGE OF CYBER MATURITY

A photograph of a laptop with a purple screen, a white mouse, and a stack of books on a reflective surface. The laptop screen shows a purple background with a circular graphic and the word 'ING'. The mouse is white and sits on the laptop's base. The books are stacked on a reflective surface, and the entire scene is lit with a purple and blue glow.

Findings on the current state of cyber maturity indicate a mixed landscape where certain industries, have made significant strides, while many organisations still have substantial progress to make. McKinsey's survey reveals that only 10% of organisations are nearing advanced cybersecurity functions, while a significant 70% have yet to fully embrace a mature, risk-based approach. This discrepancy is particularly evident within sectors: banking and healthcare lead in maturity levels due to stringent regulatory requirements, heightened consumer expectations, and intense competitive pressures. In contrast, sectors with less regulatory scrutiny exhibit lower maturity levels.

# Cyber Maturity Levels Across Sectors



Profitability appears to be linked to cyber maturity, with more mature organisations demonstrating better profit margins. Larger, publicly traded companies tend to display higher levels of cyber maturity compared to their smaller, privately owned counterparts, suggesting that resource availability and scale play critical roles in advancing cybersecurity capabilities.





## Challenges and Best Practices in Achieving Cyber Maturity

The journey to achieving cyber maturity is complex, marked by numerous challenges and the necessity to adopt best practices. As organisations strive to enhance their cybersecurity posture, understanding these challenges and identifying areas of excellence are crucial for progressing along the cyber maturity curve.

## Challenging Activities in Cyber Maturity

One of the main difficulties in improving cyber capabilities is the precise mapping of organisational data flows. This task is essential for understanding where sensitive data resides and how it moves within the network. Yet, it doesn't remain easy due to the dynamic nature of modern IT environments. The increasing adoption of cloud services and the proliferation of mobile and IoT devices complicate this task, creating numerous data points that require effective management.

Frequent cybersecurity response simulations are another critical yet challenging area. These simulations are vital for preparing response teams for real-world incidents, but they require substantial resources and coordination. The SANS Institute notes that many organisations do not conduct these simulations regularly enough, resulting in unpreparedness when actual breaches occur, thereby hindering their cyber maturity progress.

Reviewing and rewarding secure coding practices presents another obstacle. Developing secure software necessitates adherence to best practices throughout the software development lifecycle. However, according to OWASP, many organisations lack the necessary training and incentives for developers to prioritise security, leading to vulnerabilities being introduced during the coding process, which impedes achieving higher cyber maturity levels.

## Well-Performed Activities in Cyber Maturity

Despite these challenges, certain activities are well-executed across many organisations, contributing to their cyber maturity. Effective communication of cybersecurity requirements to suppliers and third parties is one such area. As supply chains become increasingly complex, ensuring that all partners adhere to rigorous cybersecurity standards is crucial. ISACA's findings suggest that many organisations have established clear protocols and requirements for their suppliers, thereby significantly reducing third-party risk and enhancing their cyber maturity.

Managing the security of remote access has also become a strong point for many organisations, especially in response to the COVID-19 pandemic, which necessitated a rapid shift to remote work. Cybersecurity Ventures reports that companies have widely adopted secure remote access solutions, such as VPNs and Zero Trust architectures, to protect their networks against unauthorised access, thereby advancing their cyber maturity.

Continuous improvement of cybersecurity standards is another area of strength. Organisations increasingly recognise the need to stay ahead of evolving threats by regularly updating their cybersecurity policies and procedures. The National Institute of Standards and Technology (NIST) advocates for a dynamic approach to cybersecurity, where standards are continually reviewed and improved to address new vulnerabilities and attack vectors, thus facilitating higher cyber maturity.

### LEADER'S EDGE IN CYBER MATURITY

Leading organisations distinguish themselves by excelling in specific, high-impact activities that are crucial for cyber maturity. Maintaining low phishing click rates

through continuous employee education and sophisticated phishing detection systems is one such activity. These organisations implement regular training programs to educate employees on recognising and responding to phishing attempts, significantly reducing the success rate of these attacks and enhancing their cyber maturity.

Revisiting and updating cybersecurity priorities annually is another best practice observed among leading organisations. This approach ensures that cybersecurity strategies remain aligned with the latest threats and business objectives. Gartner reports that regular reviews and updates help organisations adapt to new risks and technologies, maintaining a robust security posture and advancing their cyber maturity.

Additionally, leading organisations utilise central identity and access management solutions, which streamline the provisioning and de-provisioning of access rights. This practice enhances security and simplifies compliance with regulations. Centralised identity management is critical for reducing the risk of insider threats and ensuring that only authorised personnel have access to sensitive information, contributing to higher cyber maturity.

Regularly scanning for vulnerabilities is another hallmark of leading organisations. By continuously monitoring their IT environments, these organisations can quickly identify and remediate vulnerabilities before they can be exploited. The MITRE Corporation emphasises the importance of automated scanning tools that provide real-time insights into an organisation's security posture, enabling proactive threat management and furthering their cyber maturity.

# CONCLUSION

Navigating the path to cyber maturity is not just a defensive strategy but a business imperative that can unlock numerous opportunities. As cyber threats become increasingly sophisticated and frequent, businesses must adopt a proactive stance. By implementing comprehensive risk management frameworks and robust incident response plans, organisations can not only protect their assets but also build trust with their stakeholders. As Gartner highlights, 60% of businesses will consider cybersecurity risk as a primary determinant in third-party transactions by 2025. Take the strategic step towards cyber maturity today and secure your business's future. Contact us to learn how we can help you enhance your cybersecurity posture and turn challenges into opportunities.





# Take the Next Step Towards Cyber Resilience



In today's rapidly evolving digital landscape, safeguarding your business from cyber threats is more critical than ever. Many organisations still lag in their preparedness, with 77% lacking an incident response plan and facing a 41% surge in ransomware attacks.

## Is Your Organisation Prepared?

Achieving cyber maturity is not just about defence; it's a strategic imperative that aligns cybersecurity efforts with business goals, ensuring continuity and resilience. P2D Technology Services specialises in guiding businesses through the complex journey of cyber maturity, from foundational security measures to advanced digital resilience.

## Why Choose P2D Technology Services?

- **Comprehensive Cyber Maturity Assessments:** Understand your current cyber maturity level and identify areas for improvement.
- **Tailored Cybersecurity Solutions:** Implement risk management, incident response, and continuous monitoring strategies that suit your unique needs.
- **Expert Guidance:** Benefit from the expertise of industry professionals who help build resilient processes and enhance workforce skills to combat evolving threats.

## Don't Wait Until It's Too Late

Adopting a strategic approach to cyber maturity not only mitigates risks but also builds trust with your stakeholders and aligns with industry standards like the NIST Cybersecurity Framework.

## Ready to Enhance Your Cybersecurity Posture?

Take the strategic step towards cyber maturity today. Contact us at [info@p2dl.com](mailto:info@p2dl.com) or visit [www.p2dl.com](http://www.p2dl.com) for more information. Let P2D Technology Services help you turn cybersecurity challenges into opportunities and secure your business's future.

**Secure Your Future with P2D Technology Services.**

## References

---

- Projected Cybercrime Cost by 2025: \$10.5 trillion (Cybersecurity Ventures, 2021)
- Businesses Lacking Incident Response Plan: 77% (Ponemon Institute, 2020)
- Increase in Ransomware Attacks: 41% (Verizon Data Breach Investigations Report, 2023)
- Phishing as a Share of Email Attacks: 39.6% (Mimecast Email Security Report, 2023)
- McKinsey & Company. (2021). Cyber Maturity Survey.
- Gartner. (2021). Cybersecurity Maturity Report.
- Ponemon Institute. (2020). State of Cybersecurity Report.
- ISACA. (2020). State of Cybersecurity 2020.
- Deloitte. (2020). Global Cyber Executive Briefing.
- Verizon. (2021). Data Breach Investigations Report.
- IBM. (2021). Cost of a Data Breach Report.
- Accenture. (2021). State of Cyber Resilience Report.
- SANS Institute. (2020). Incident Response Survey.
- Deloitte. (2021). Cyber Risk Report.
- ISACA. (2020). State of Cybersecurity Report.
- EY. (2021). Global Information Security Survey.
- OWASP. (2021). Secure Coding Practices.
- CyberArk. (2021). Identity and Access Management Report.
- MITRE Corporation. (2021). Vulnerability Management.





**P2D**  
TECHNOLOGY SERVICES

+44 (0) 2036 378 507

Orega 202, Marlow-International,  
Parkway, Marlow, SL7 1YL

[info@p2dl.com](mailto:info@p2dl.com)

