Cyberfort

Expert-led. Security Driven.

WHITE PAPER

Cyber Resilience in 2025: The New Way to Secure your Future

Assured Service Provider

in association with National Cyber Security Centre

Cyber Resilience Audit

Introduction

The Cyber Security threat landscape has undergone a dramatic shift in the past decade with businesses seeing a significant increase in the volume and sophistication of attacks, partly due to factors such as geopolitical instability, the evolution of 'as a service' type products, difficulties in protecting complex supply chains, and the introduction of AI.

Cyber Security concentrated on building defences to protect a business from attack, but due to the shift in the threat landscape this is proving to not be enough.

Whilst Cyber Security is still important in the overall strategy, Cyber Resilience has evolved with the view that a breach is inevitable and to concentrate efforts on real-time detection, a swift response and recovery, minimising the impact of a Cyber Security incident and maintaining business continuity.

This whitepaper explores what Cyber Resilience is, and why you should be thinking about adopting it.

$4.45m
Average cost of a data breach in 2024 (IBM)

£6,800/min
Average ransomware downtime cost (Coveware)

48%
Reduction in losses with proactive resilience (Gartner)

75%
Enterprises with cyber resilience as a C-suite priority by 2026 (Gartner)

The Traditional Cyber Security Model

A traditional Cyber Security model focuses on protecting an organisation's IT infrastructure from cyber threats through a series of defensive measures, such as:

Perimeter Defence
Devices such as Firewalls to filter incoming and outgoing network traffic, and Intrusion Detection Systems (IDS) to monitor for suspicious activity.

Endpoint Security
Antivirus Software to scan and remove malicious software from individual devices and Endpoint Detection and Response (EDR) to provide continuous monitoring and some response capabilities.

Access Control
Authentication to ensure that only authorised users can access business resources, including the use of passwords, biometrics, or multi-factor authentication (MFA), and Authorisation to determine which resources and data users can access based on their roles and permissions.

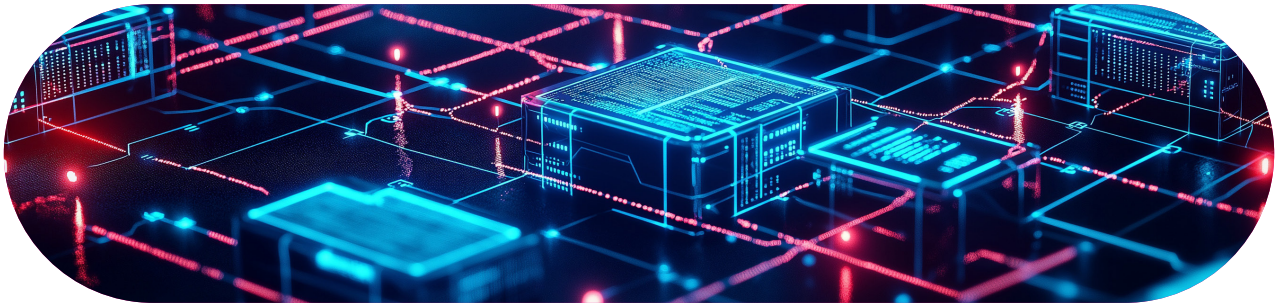
Data Protection
Encryption of data and methods for Data Loss Prevention (DLP).

Network Security
Standard methods such as Virtual Private Networks (VPNs) to secure remote access using encrypted connections, and segmentation to divide the network into smaller, isolated segments.

Security Policies and Procedures
Establishing guidelines and best practices for maintaining security within the organisation and incident response plans to outline the steps to take in the event of a breach.

Training and Awareness
Implement training and awareness programmes for staff and third parties, specifically on the identification of security incidents, and the reporting process.

Regular Audits and Assessments
Vulnerability Assessments and Penetration Testing to identify and address potential weaknesses in the IT infrastructure, and simulate cyber attacks to evaluate the effectiveness of security measures; respectively.



An Introduction to Cyber Resilience

Traditional Cyber Security measures, while essential, often focus on preventing attacks. However, as cyber threats become more sophisticated and persistent, it is increasingly clear that prevention alone is not enough. This is where Cyber Resilience comes into play.

Cyber Resilience is the ability of an organisation to prepare for, respond to, and recover from cyber incidents. It goes beyond prevention, encompassing a holistic approach that ensures business continuity and minimises the impact of disruptions. Cyber Resilience integrates robust security measures with comprehensive response and recovery strategies, enabling organisations to withstand and manage cyber attacks.

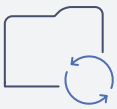
The concept of Cyber Resilience is built on five key principles:

01 **Preparation**
Proactively identifying and mitigating potential risks and vulnerabilities

02 **Detection**
Continuously monitoring for signs of threats and anomalies

03 **Response**
Having well-defined plans and trained personnel ready to respond effectively to incidents

04 **Recovery**
Ensuring that systems and data can be restored quickly to maintain operations



05 **Continual Improvement**
Learning from security events and incidents, threat intelligence, maturity and capability assessments, new trends and tooling, exercising, and feeding this back into the Cyber Resilience capability.

By adopting a Cyber Resilient approach, organisations can not only protect their critical assets but also ensure that they remain operational in the face of adversity. This approach fosters a culture of adaptability and continuous improvement, allowing organisations to adapt to emerging threats.

Cyber Resilience is about building a robust and adaptable defence that not only prevents attacks but also ensures that an organisation can function despite them. It is a crucial component of modern Cyber Security strategies, providing a comprehensive framework for managing and mitigating the risks of a digital existence.

The Business Push for Resilience

Many organisations may view Cyber Resilience as a compliance requirement, rather than a competitive advantage. However, in 2025, resilience has become a financial, operational, and reputational imperative.

Competitive Advantage

There are several positives of adopting a Cyber Resilience approach, combining to potentially provide a competitive advantage, or at least to avoid costly or time-consuming distractions:

- Improve operational continuity, allowing business operations to continue during adverse cyber events, and to maintain service delivery.
- Protecting the business finances by avoiding operational disruption, fines, and loss of business.
- Providing a stable landscape for innovation and growth, and protecting intellectual property.

Financial Impact of Cyber Disruptions

- The average cost of a data breach in 2024 was $4.45 million (IBM Cost of a Data Breach Report).
- Ransomware downtime costs businesses an average of £6,800 per minute (Coveware).
- Organisations that proactively invest in Cyber Resilience reduce financial losses by up to 48% (Gartner).
- Regulator penalties or fines being imposed.
- Increase in insurance premiums or inability to procure insurance.

Case Study: A successful cyber attack on a telecommunications company resulted in significant brand damage, the loss of over 100,000 customers, regulatory fines, and a loss of a third of the company share value.

Reputational Damage

Beyond financial loss, cyber incidents can erode or lose customer trust, resulting in customers taking their business elsewhere. This, and attracting extensive negative press coverage can damage a brand beyond repair.

A company is less likely to be judged negatively on a cyber attack if they demonstrate the capability to be resilient, in fact this can enhance their reputation especially if they can be transparent and timely with their communications and showing operational competence.

Case Study: In 2023, a UK energy provider suffered a nation-state cyber attack. Due to poor resilience planning, operations were disrupted for two weeks, leading to regulatory penalties and loss of investor confidence.

The Compliance Push for Resilience

In response to the increasing cyber threats we now face, global regulators have shifted their focus from security controls to operational resilience. Resilience is therefore becoming mandatory in certain sectors, and the regulators are widening the range of businesses under the regulation. Regulators are becoming more powerful authorities and are backed by law. The following frameworks will set the minimum baseline for resilience in 2025:

Cyber Security and Resilience Bill

The UK's Cyber Security and Resilience Bill is a legislative proposal by the UK Government aimed at strengthening the country's cyber defences to protect essential public services and can be seen as the NIS2 equivalent. The bill seeks to address the growing threat and the speed in which they can occur, ensuring that the UK's critical infrastructure and digital services remain secure.

The bill extends the remit of existing legislation to cover more digital services and more focus on supply chains. It also gives regulators more power to enforce the regulation and demands more reporting requirements to assist in providing a better real-time picture of the current landscape; and to aid in a coordinated response. There is also provision for the scope of the regulation to change quickly, based on this information.

The bill is expected to be enacted by the end of 2025, key takeaways from the proposed bill are:

- Discretionary powers for the Secretary of State to extend scope under CNI without parliament approval.
- Companies in scope under direct regulatory authority, enforceable by law.
- Regulations extend into the supply chain, with authority to designate special or critical suppliers.
- Mandatory incident reporting within strict time frames.

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) is an EU regulation designed to enhance the digital operational resilience of financial entities. Its primary goal is to ensure that financial institutions can withstand, respond to, and recover from various ICT-related disruptions and threats. DORA applies to a broad range of financial entities, including banks, insurance companies, investment firms, and their critical ICT third-party service providers. By implementing robust ICT risk management frameworks, these entities are better equipped to identify, protect against, detect, and respond to ICT risks. Additionally, DORA mandates regular testing of digital operational resilience to demonstrate that potential disruptions can be managed.

Furthermore, DORA requires financial entities to report major ICT-related incidents to competent authorities and share information on cyber threats. This regulation also imposes stringent requirements for managing risks associated with ICT third-party service providers. DORA came into force on January 16, 2023, and was fully applicable from January 17, 2025. By adhering to these requirements, financial institutions can safeguard their operations and contribute to a more resilient Cyber Security environment across the EU.

Key requirements for DORA:

- Implement robust ICT risk management frameworks to identify, protect against, detect, and respond to ICT risks.
- Report major ICT-related incidents to competent authorities and share information on cyber threats.
- Regular testing of digital operational resilience is mandated to ensure preparedness for potential disruptions.
- Manage risks associated with the supply chain.

NIS2 Directive – Critical Infrastructure (EU)

The NIS2 Directive represents a significant enhancement to the original NIS Directive, designed to bolster the Cyber Security of network and information systems throughout the EU, especially within critical national infrastructure sectors. This updated regulation expands its scope to encompass a wider range of sectors and organisations.

Service providers deemed essential and important in areas such as energy, transport, health, and digital infrastructure must adhere to stringent Cyber Security measures mandated by regulators to safeguard their network and information systems. NIS2 signifies a major progression in the EU's Cyber Security strategy, addressing the shortcomings of the initial directive and adapting to the increasingly interconnected and digital nature of contemporary society. Organisations subject to NIS2 are required to proactively comply with the new standards to protect their operations and contribute to a more resilient Cyber Security landscape across Europe.

Key measures from the NIS2 Directive are:

- Covering additional sectors, including cloud computing, digital providers, manufacturing, and research.
- Reinforcing the importance of risk management, assessment, and mitigation strategies.
- Reporting obligations on applicable organisations, requiring entities to report Cyber Security incidents to all relevant stakeholders.
- Encouraging collaboration among EU member states, prompting cross-border information sharing to prevent and mitigate cyber threats.
- Introduction of strict penalties for non-compliance, including fines of up to 10% of an organisation's annual turnover.

NCSC Cyber Assessment Framework (CAF) – UK Public & Private Sector

The NCSC Cyber Assessment Framework (CAF) is a comprehensive set of guidelines developed by the UK's National Cyber Security Centre (NCSC) to help organisations manage and mitigate cyber risks. It is particularly aimed at entities that play a vital role in the UK's day-to-day life, such as those within the Critical National Infrastructure (CNI) and those subject to the Network and Information Systems (NIS) regulations.

The CAF provides a systematic approach to assessing the extent to which cyber risks to essential functions are being managed. It includes a range of linked guidance and resources to help organisations achieve and demonstrate an appropriate level of Cyber Resilience. This framework is designed to ensure that organisations can protect their network and information systems from serious cyber incidents, thereby safeguarding public safety and maintaining the reliability of essential services.

In particular, the UK Government's vision is that "...core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyber attack...", with the stated strategic aims "..for government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030..." (Government Cyber Security Strategy 2022-2030).

The key objectives of CAF are:

- Managing security risk
- Protecting against cyber attacks
- Detecting cyber events
- Minimising the impact of cyber incidents

Implementing Cyber Resilience

Cyber Resilience starts with traditional Cyber Security, consisting of (but not exclusive to):

- Having accountable leadership, a clear remit, and funding.
- Having defined business objectives and a Cyber Resilient strategy that meets those objectives.
- Identifying and understanding your assets, understanding their importance, those critical to the business or operations, their vulnerabilities, the threats to them, and establishing effective vulnerability management and appropriate security controls.
- A solid risk management process.

A successful Cyber Resilience implementation builds on this and is reliant on the capability to detect, respond and resolve security incidents, which requires:

- Current threat intelligence relating to assets.
- Consistent and continuous security training and awareness.
- The capability to monitor assets and detect security events and incidents, sometimes logically encapsulated with a Security Operations Centre (SOC) with tooling such as a Security Event and Incident Management (SIEM).
- The capability to respond to security incidents in a consistent and coordinated manner, which comes from predefined response plans or Playbooks, an incident response function, qualified staff, and exercising.
- A tested backup and restoration function.
- A mechanism for continual improvement.

A substantial part of an effective response is knowing what to look for and what to do when you detect something. Exercising is a key part of the response planning process and should be held frequently. Exercising can take many forms, from a tabletop scenario where the response team can pose and discuss the most likely security incidents and how they would go about resolving those, to Red Team vs Blue Team type scenarios; where the Red Team are the offensive experts looking to attack a particular vulnerability and the Blue Team defend. Another area to practice with exercising would be recovery of assets and systems from backup. Exercising builds experience and confidence in the face of an evolving security incident situation, it can reinforce roles and responsibilities, and can help build relationships within the business that become critical at the time of managing an incident.

One other notable area of Cyber Resilience is the concept of continual improvement. The output of exercising, threat assessments, threat intelligence, maturity and capability assessments and other relevant functions can be analysed and fed back in as improvement activities. This can be adding to defensive infrastructure or exercising in a particular area, for example.

Best Practice: Businesses that conduct quarterly resilience testing recover from cyber attacks 60% faster than those that test annually (Ponemon Institute).

Final Thoughts: Cyber Resilience is a Business Imperative

In this paper we have explored the concept of Cyber Resilience and how it builds on Cyber Security, and the benefits of being resilient, now and especially in a future with more complex threats, and more capable actors.

The common themes within the regulatory frameworks point to the changing view of government and regulatory bodies, that traditional Cyber Security models are not sufficient, and that the public digital services, and critical industries must become resilient, and this will include the supply chain.

Cyber Resilience describes how businesses should consider that a breach is inevitable and to put plans in place for early detection and a swift response, to minimise the operational impact, and to continually improve, rather than the traditional view of setting up defences. Getting ahead now could provide businesses with a competitive advantage.

And finally, that Cyber Resilience is not just a technical concern, but a capability developed by the business, throughout the business, which is constantly improving, requiring strong leadership and direction, and competent staff, to help the business meet its objectives.

By 2026, cyber resilience will be a C-suite priority for 75% of enterprises (Gartner).

Discover more about Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks and proactive Detection and Response to security incidents through our 24/7 security operations centre.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Assured Service Provider
in association with National Cyber Security Centre
Cyber Resilience Audit

For more information on our Cyber Security services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you