Cyberfort
Expert-led. Security Driven.

WHITE PAPER

Five key areas from an NCSC assured Cyber Resilience Audit and Review which will strengthen an organisations defence against cyber attacks

Introduction

In an era of escalating cyber threats, organisations must proactively assess and strengthen their resilience against a wide range of attack vectors. Cyber resilience audits and reviews have emerged as critical tools to help identify threats, vulnerabilities, regulatory compliance issues and risk levels.

They also help to evaluate response capabilities and drive continuous improvements in an organisation's security posture. This article explores the key components of effective cyber resilience audits, the benefits they offer, and identifies 5 key focus areas which organisations should focus on to counter common cyber threats.

The Evolving Cyber Threat Landscape

Cyber criminals, nation-state actors, and other malicious entities have expanded the scale and sophistication of their attacks, targeting organisations across all industries. From ransomware and data breaches to supply chain compromises and advanced persistent threats, the cyber threat landscape continues to evolve rapidly.

Threat actors have demonstrated their ability to exploit vulnerabilities not only within an organisation's IT infrastructure but also in its broader digital ecosystem, including cloud services, Internet of Things (IoT) devices, and third-party supply chain partners. Additionally, government and industry bodies have implemented stringent cyber security regulations and standards, requiring organisations to demonstrate robust security controls, incident response capabilities, and business continuity measures.

All organisations know the importance of being Cyber Resilient and it is estimated 63% of medium sized organisations and 72% of large organisations have undertaken some form of cyber resilience security audit in the past 12 months according to UK Government research (1). But research from Microsoft and Goldsmiths University in March 2024 (2) discovered only 13% of organisations would describe themselves as Cyber Resilient and adequately protected against cyber-attacks.

At Cyberfort we have been reviewing these reports in depth and evaluating cyber resilience audits organisations have undertaken in the past 12 months. From our research into the reports and organisations we have interacted with, it is clear there are two major gaps which need to be addressed. The first gap is making sure the Cyber Resilience Audit and Review undertaken by an organisation is completed by an NCSC assured consultancy provider to make sure the right information is captured and aligned to NCSC guidelines.

The second gap which this article covers, is the implementation of the findings from the cyber resilience audit and review. From the research findings from the Microsoft and Goldsmiths University report it is clear organisations are aware of many of the potential cyber risks. But why are they not implementing the improvement plans from their organisation's cyber resilience audit and review to ensure their organisation is resilient to cyber-attacks?

The Importance of Cyber Resilience

Cyber resilience is the ability of an organisation to anticipate, withstand, recover from, and adapt to disruptive cyber incidents. It encompasses a holistic approach to security, focusing on both prevention and response. The key components for an organisation to describe itself as Cyber Resilient are:

- **Protective Controls** - Implementing robust security measures to prevent and mitigate cyber threats.

- **Incident Response Capabilities** - Developing effective plans and processes to detect, contain, and recover from cyber attacks.

- **Organisational Adaptability** - Fostering a culture of continuous improvement and the ability to adapt to evolving threats.

- **Business Continuity** - Ensuring the maintenance of critical business functions and the restoration of normal operations after a cyber incident.

An NCSC assured Cyber Resilience Audit and Review covers 4 categories which directly correlate to the above areas an organisation needs to implement to describe itself as Cyber Resilient:

Managing security risk
Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

Protecting against cyber-attack
Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyber attack.

Detecting cyber security events
Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

Minimising the impact of cyber security incidents
Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

What are the 5 focus areas from a Cyber Resilience Audit and Review where organisations should be taking action?

As mentioned earlier in this article many organisations have undertaken a Cyber Resilience Audit and Review in the past 12 months. But for many organisations the results and findings from a review and audit of this nature can be overwhelming with a long list of improvements to be made in their IT environments, the right skills not available and budgetary constraints resulting in actions not being able to be undertaken in a timely and resource focused manner.

This means IT leaders need to focus on the key areas which are mission critical and where inaction is not an option as it could put the organisation at risk of cyber attack. From our experience at Cyberfort we suggest IT teams focus on the 5 following areas to improve their Cyber Resilience in the short to medium term:

01 **Having the right management policies and processes in place to govern its approach to cyber security effectively**

02 **Putting in place the right controls to manage to supply chain security**

03 **Ensuring robust verification, authentication and authorised access to networks and information systems is in place as part of an Identity and Access Management strategy**

04 **Data security is in place in terms of how data is being stored, managed and moved in transit**

05 **Identification of security incidents and making sure the right response mechanisms are in place to identify, contain, remediate and recover from an attack**

In the next section of this article the 5 focus areas identified above will be discussed in terms of what the likely scenario is, key actions to be undertaken and where a third party cyber security provider could help to overcome the challenges your organisation is facing.

01 Having the right management policies and processes in place to govern its approach to cyber security effectively

For a Cyber Security strategy to be effective the right leadership approach that champions best practice in cyber security and empowering employees at all levels of the organisation to take action is crucial in keeping an organisation secure, resilient and compliant. If an organisation's board members and employees does not have trust in the policies and processes in place this can lead to low confidence levels that the organisation is doing the right things to remain protected, decision-making could be fragmented which can result in the organisation being unprepared for an attack as employees and board members may not have access to the right information at the right time.

To ensure that an organisation's cyber security approach is robust, IT leaders must establish and enforce the right management policies and processes. Effective governance in cyber security requires a structured framework, clear policies, consistent processes, and regular assessments to address the evolving threat landscape. Here's how IT leaders can ensure these elements are in place:

Establish a clear Cyber Security Governance Framework

A cyber security governance framework defines the structure, roles, responsibilities, and accountability for managing cyber security across the organisation. Quite often when Cyberfort reviews this area with an organisation we discover a fragmented approach to developing and maintaining a Cyber Security Framework within their organisation. IT leaders should select or develop a framework that aligns with both business goals and industry standards, such as NIST, ISO 27001, or the NCSC Cyber Assessment Framework (CAF). This framework serves as a foundation for creating policies, setting benchmarks, and guiding all cyber security-related decision-making.

The governance framework should detail specific roles and responsibilities for cyber security oversight, from IT and security teams to executive leadership. Assigning a Chief Information Security Officer (CISO) or equivalent role can centralise responsibility, ensuring accountability and a coordinated response to cyber risks. If the right cyber security leadership does not exist within the organisation or requires 3rd party validation it is suggested organisations employ a vCISO for the short to medium term to ensure the right governance framework is selected and implemented.

Develop Comprehensive Cyber Security Policies

Policies are essential for guiding behaviours and setting expectations for all employees regarding cyber security practices. It goes without saying, IT leaders should establish clear policies that address key areas such as data protection, access control, incident response, acceptable use, and remote work security. These policies should be designed to align with regulatory requirements and industry standards, ensuring compliance and setting a foundation for best practices. For maximum effectiveness, cyber security policies should be tailored to the organisation's unique risks and operational needs. For example, a financial institution might have stricter access control policies compared to other sectors due to regulatory demands. Policies should also incorporate requirements for vendor management, as third-party vendors often introduce unique security challenges.

Implement Structured Processes for Key Security Functions

Policies alone are insufficient without structured processes that ensure adherence and consistency. IT leaders must define and document processes for critical security functions, such as risk assessment, incident response, vulnerability management, and access control. These processes should be detailed enough to standardise actions and ensure that employees and teams understand how to execute their cyber security responsibilities. For example, the incident response process should define specific steps for detecting, containing, and recovering from incidents, along with designated roles and communication protocols. Similarly, the risk assessment process should specify methods for identifying, prioritising, and mitigating risks to ensure resources are allocated efficiently.

Automation and security tools can help streamline and enforce these processes. For example, at Cyberfort we can help organisations with the provision of market leading Security Information and Event Management (SIEM) systems which can assist with continuous monitoring and automated alerting, while Identity and Access Management (IAM) solutions through our MXDR platform can help enforce access controls and limit unauthorised access to systems, processes and data.

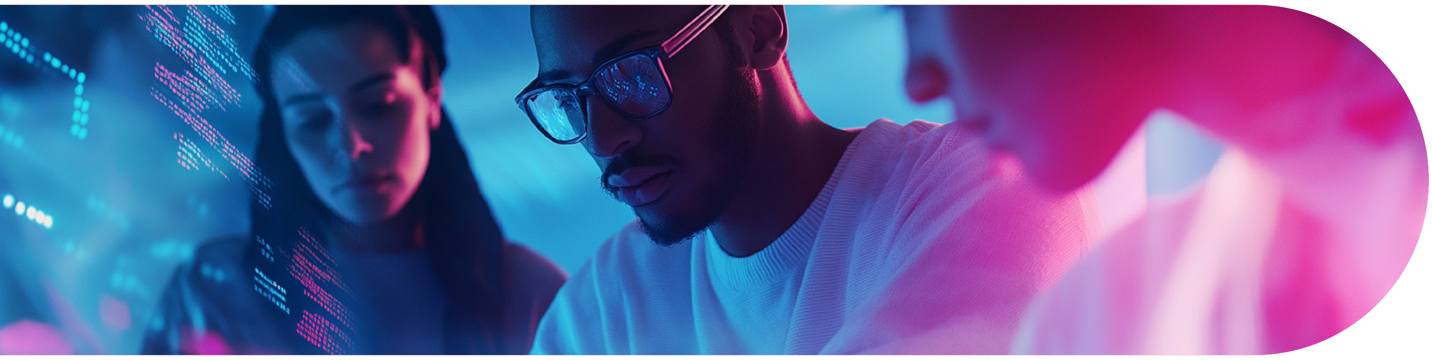
Foster a Culture of Cyber security Awareness

IT leaders must emphasise the role of all employees in maintaining cyber security. Policies and processes should be supported by ongoing security awareness and training programs that educate employees on best practices, such as identifying phishing attempts and safeguarding sensitive information. This creates a culture where cyber security is seen as a shared responsibility.

Conduct Regular Reviews and Updates

The cyber security landscape is constantly evolving, and governance practices must evolve with it. IT leaders should conduct regular reviews of policies and processes, updating them as necessary to reflect new threats, technology advancements, and regulatory requirements. Regular audits and assessments can validate the effectiveness of these policies, identify gaps, and ensure continuous improvement.

Effective cyber security governance requires a structured framework, tailored policies, well-defined processes, and a commitment to continuous improvement. By implementing these elements and working with an NCSC assured consultancy partner, IT leaders can ensure that cyber security is managed proactively, aligning security practices with organisational goals and effectively mitigating cyber risks. This approach not only strengthens the organisation's defences but also builds resilience, protecting assets, data, and reputation in the face of evolving cyber threats.



02 Putting in place the right controls to manage to supply chain security

Supply chain security involves a combination of people, processes, and technology. The potential entry points and impact of supply chain security span across procurement, operations, legal and compliance, sourcing, and a number of other functions. To address these risks, a thorough understanding and a shared posture across all the areas of the supply chain are crucial.

Following a Cyber Resilience Audit and Review Cyberfort works with IT leaders to put the right controls in place to manage supply chain security effectively these include:

Establishing Rigorous Vendor Risk Assessment Procedures

The first step in managing supply chain security is to understand the risks associated with each vendor. Cyberfort can provide IT leaders with a comprehensive vendor risk assessment process that evaluates the cyber security practices, compliance levels, and potential vulnerabilities of each supplier. This assessment should be part of the vendor selection process and should be revisited regularly for all active vendors. Risk assessments should include reviewing the vendor's policies on data protection, incident response, and access control to ensure they align with the organisation's standards. Additionally, for critical suppliers, Cyberfort can help IT leaders to conduct on-site assessments or request detailed audit reports to gain further assurance that the vendor's security measures are effective and sufficient.

Implement Security Controls in Contracts and SLAs

Contracts and Service Level Agreements (SLAs) with suppliers should clearly define security expectations, data protection requirements, and compliance obligations. Contracts should include clauses specifying security measures the vendor must follow, such as encryption protocols, secure data transfer methods, and incident reporting timelines. These agreements should also outline the organisation's right to audit the vendor's security practices, either directly or through independent assessments. Including provisions for incident response in contracts is essential. Vendors should be required to notify the organisation promptly if they experience a security breach that could impact the supply chain. Defined communication channels and protocols for such scenarios help ensure a swift response to mitigate potential damage.

Enforce Access Control and Least Privilege Principles

One of the primary risks associated with supply chain security is the level of access vendors have to an organisation's systems and data. Cyberfort can help IT leaders to enforce access control measures that limit vendor access strictly to what is necessary for their role or service provision. By applying the principle of least privilege, vendors only have access to the data and systems required to perform their function, minimising exposure to sensitive information. Multi-factor authentication (MFA), strict password policies, and role-based access controls further strengthen the protection of the organisation's assets. IT teams should also regularly review and revoke access for vendors who no longer require it, such as at the end of a project or contract term.

Monitor and Continuously Assess Third-Party Activities

Continuous monitoring is essential for detecting unusual or unauthorised activities within the supply chain. IT leaders can employ tools like Cyberfort's MXDR platform and User and Entity Behaviour Analytics (UEBA) to monitor vendor activity in real-time and identify potential threats. These monitoring solutions provide visibility into vendor interactions with critical systems, allowing IT teams to detect and respond quickly to any suspicious activity. Periodic reassessments of vendor risk profiles are also essential. Vendors may change their practices, use new subcontractors, or alter their security postures over time, necessitating regular evaluations to ensure ongoing alignment with the organisation's standards.

Provide Vendor Security Awareness Training

Many cyber incidents result from human error, including among vendors. Cyberfort offers security awareness training for vendors who interact with a customers systems, focusing on best practices in data protection, phishing avoidance, and secure communication. For high-risk vendors, periodic refresher training sessions reinforce a security-first mindset and reduce the risk of human error within the supply chain.

Managing supply chain security requires a layered approach that combines vendor assessment, strong contractual controls, access restrictions, continuous monitoring, and security awareness. By implementing these controls and working with an NCSC assured consultancy partner IT leaders can reduce supply chain vulnerabilities, protect sensitive data, and ensure that third-party vendors contribute to, rather than compromise, organisational security. This proactive approach to supply chain security is essential in today's interconnected digital environment, where a single vulnerable link can expose the entire organisation to cyber threats.

03 Ensuring robust verification, authentication and authorised access to networks and information systems is in place as part of an Identity and Access Management strategy

Identity and Access Management resilience is crucial to an organisation's defences against cyber-attacks. By not having the right resilience measures in place, Identity and Access management can be the biggest cause of failure for a cyber security strategy. IT leaders need to make sure their Identity and Access Management strategy is not just about managing user verifications but that the whole strategy is built on a robust infrastructure designed to support an organisations operations under all circumstances.

Here's how Cyberfort can help IT leaders to build a robust IAM strategy that includes verification, authentication, and authorised access:

Implement Strong User Verification and Identity Proofing

At the heart of a robust IAM strategy is the need to accurately verify users before granting access. Cyberfort has a deep understanding of how IT teams can establish rigorous identity proofing processes to verify users' identities, particularly during account creation and onboarding. This may involve multi-step verification methods, such as identity documents, biometric verification, or knowledge-based authentication questions, to ensure that only legitimate users gain access. For ongoing verification, organisations should implement continuous identity validation checks, especially for high-risk roles or sensitive data access. Regular identity re-verification (e.g., every few months) or during significant changes in user roles can prevent unauthorized access if credentials are compromised or misused.

Enforce Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a core component of a secure IAM strategy. MFA requires users to provide multiple pieces of evidence (factors) before granting access, typically including something the user knows (e.g. password), something they have (e.g. security token or mobile app), and/or something they are (e.g. fingerprint or facial recognition). Implementing MFA significantly reduces the risk of unauthorised access because it prevents attackers from gaining access even if they acquire a password. IT leaders should enforce MFA especially for privileged accounts, remote access, and applications containing sensitive data. Adaptive MFA, which adds extra authentication steps based on risk (e.g. logging in from a new location), can further enhance security without inconveniencing users.

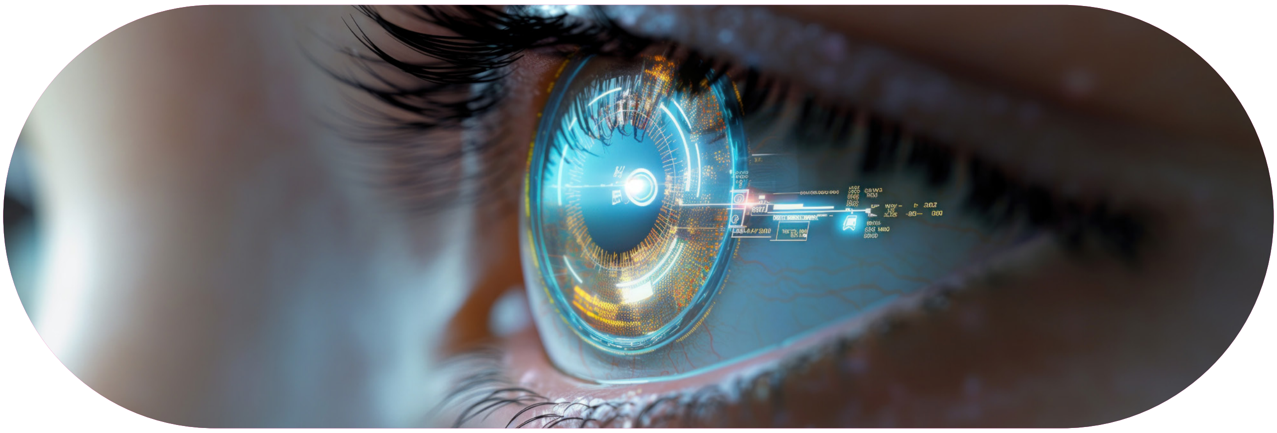
Apply the Principle of Least Privilege and Role-Based Access Control (RBAC)

A core IAM principle is least privilege access, where users are granted only the minimal level of access required to perform their job functions. IT leaders should establish Role-Based Access Control (RBAC) policies to assign access based on predefined roles, ensuring that users have access solely to the resources they need. For instance, HR staff may have access to employee data but not to financial records, while IT administrators may have access to network systems but not to customer data. RBAC simplifies management by allowing IT teams to control access for groups rather than individuals. For sensitive roles, IT leaders can implement even more restrictive policies, such as Just-In-Time (JIT) access, which provides temporary permissions for specific tasks and automatically revokes access afterward.

Conduct Regular Access Reviews and Audits

To maintain ongoing security, Cyberfort can help IT leaders to conduct regular access reviews and audits of all user accounts. This involves periodically checking that users' access aligns with their current job roles and removing or updating permissions as necessary. Access audits help identify and eliminate dormant accounts, which are common targets for attackers, and prevent privilege creep, where users accumulate excessive permissions over time. These reviews also ensure compliance with regulatory standards by demonstrating that the organisation actively monitors and manages access to sensitive information.

A robust IAM strategy that emphasises verification, multi-factor authentication, least privilege access, centralised access management, and regular audits is essential for securing access to networks and information systems. By implementing these IAM components and working with a specialist Cyber Security partner like Cyberfort, organisations can effectively control user access, minimise unauthorised access risks, and protect critical data assets. A well-structured IAM strategy not only fortifies security but also streamlines user access management, enabling a secure, efficient, and compliant digital environment.



04 Data security is in place in terms of how data is being stored, managed and moved in transit

At the heart of cyber resilience is making sure the security of data, the most critical asset of any organisation is secure in terms of where it is being stored, how it is being managed and when it is being moved in transit between different systems and infrastructure environments. Focusing on data security is essential to prevent unauthorised access, maintain confidentiality, and protect data integrity. Key areas which need to be considered as part of improving cyber resilience include Data Encryption, Access and Authentication Controls, Data Immutability, Data Integrity Checks and Continuous Monitoring and Auditing. By focusing on these key areas, organisations can secure their data and mitigate the risk of breaches or tampering, resulting in a strong defensive security foundation.

Here's how Cyberfort helps IT leaders to ensure they have the right data security across storage, management, and transit.

Secure Data Storage

Data stored within an organisation's systems whether on-premises or in the cloud, needs to be encrypted and safeguarded with strict access controls. IT leaders should implement encryption for both structured (e.g., databases) and unstructured data (e.g., files, documents) so that stored data remains secure even if it's accessed or stolen by unauthorised users. At Cyberfort we manage our own datacentres and over 100+ customers sensitive data. We understand how important it is to implement Advanced Encryption Standard (AES) with 256-bit encryption is widely used for strong data protection, Data Loss Prevention (DLP) tools can be deployed to monitor and control sensitive data storage and we can provide regular backup routines to secure data storage, ensuring that critical data is backed up frequently and stored securely in separate locations in UK based datacentres.

Data Management and Access Control

Managing data securely involves strict access control policies and user permissions to prevent unauthorized users from accessing sensitive data. IT leaders can implement Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) systems, assigning access based on job roles or specific attributes, ensuring that only authorised personnel can view or modify sensitive information. Identity and Access Management (IAM) tools are essential for enforcing these policies. Multi-Factor Authentication (MFA) should be mandated for access to critical systems, while privileged accounts should follow the principle of least privilege and be regularly audited. Additionally, automated IAM solutions can track and record all user activities related to sensitive data, providing an audit trail that is essential for both security monitoring and compliance. Cyberfort understands a wide range of data governance policies, including how data classification, is also vital for effective data management. By categorising data based on its sensitivity and regulatory requirements (e.g., confidential, internal, public), organisations can tailor security measures accordingly. Sensitive data may require additional protection layers, while public data may follow more flexible security controls.

Data Security in Transit

Whether moving within the organisation’s network or to external locations data faces significant risks of interception and tampering. To secure data during transmission, Cyberfort can help IT leaders to implement Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols, which encrypt data being sent over networks, preventing unauthorised interception. For internal network communication, IPsec VPNs or private network tunnels add a layer of security, especially for remote access. For highly sensitive data, end-to-end encryption should be used. This encryption protects data from the moment it leaves one endpoint until it reaches the destination endpoint, ensuring data integrity during the entire journey. Furthermore, digital certificates can authenticate users and devices, confirming the sender’s and receiver’s identities and reducing risks associated with man-in-the-middle attacks.

By establishing and enforcing strong encryption, access control, monitoring, and governance policies, IT leaders can secure data effectively across its entire lifecycle. This comprehensive approach not only protects data in storage, management, and transit but also supports compliance with data protection regulations and enhances organisational resilience against cyber threats. Robust data security policies, combined with proactive monitoring and regular audits, ensure that sensitive information is stored, managed, and transferred securely, safeguarding both organisational and customer data.

05 Identification of security incidents and making sure the right response mechanisms are in place to identify, contain, remediate and recover from an attack

Many organisations discover once they have undertaken a cyber resilience audit and review that they do not have the right skilled staff, systems, processes or budgets in place to be able to effective deal with a cyber security incident. At Cyberfort we have a deep understanding on a wide range of cyber security incidents and how organisations can implement effective response mechanisms to protect customers from cyber threats. To achieve this, Cyberfort has established robust tools, processes, and strategies to detect, contain, remediate, and recover from cyber incidents swiftly and effectively.

Here's how a Cyberfort can ensure comprehensive incident identification and response processes are in place and realistic for an organisation:

Implementation of Advanced Threat Detection and Monitoring

Cyberfort can deploy advanced threat detection and continuous security monitoring solutions for its customers through its market leading MXDR platform. The MXDR platform aggregates and analyses data from various sources (e.g., firewalls, endpoints, network traffic) in real time. By analysing patterns and identifying anomalies, SIEM systems provide early indicators of potential threats, enabling faster response. In addition to SIEM, by incorporating User and Entity Behaviour Analytics (UEBA) can help detect unusual activity among users and systems, such as unauthorised data access or unusual login locations. Similarly, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can monitor network traffic to identify and block suspicious activities before they escalate into full-scale incidents.

Establishment of Clear Incident Response Plans and Playbooks

Cyberfort works with organisations to develop tailored Incident Response plans and playbooks for different types of cyber incidents. These playbooks outline specific steps for detection, containment, remediation, and recovery, ensuring that response teams can act swiftly and consistently during a crisis. Playbooks cover a range of incident types, from ransomware and phishing attacks to insider threats and Distributed Denial of Service (DDoS) attacks. Key components of an Incident Response plan include detection protocols, which define what constitutes an incident, and escalation procedures, which detail who should be informed and involved at each stage of the response. By establishing these predefined procedures, Cyberfort ensures that customers have a structured, repeatable approach for incident handling, minimising uncertainty and delays during an actual event.

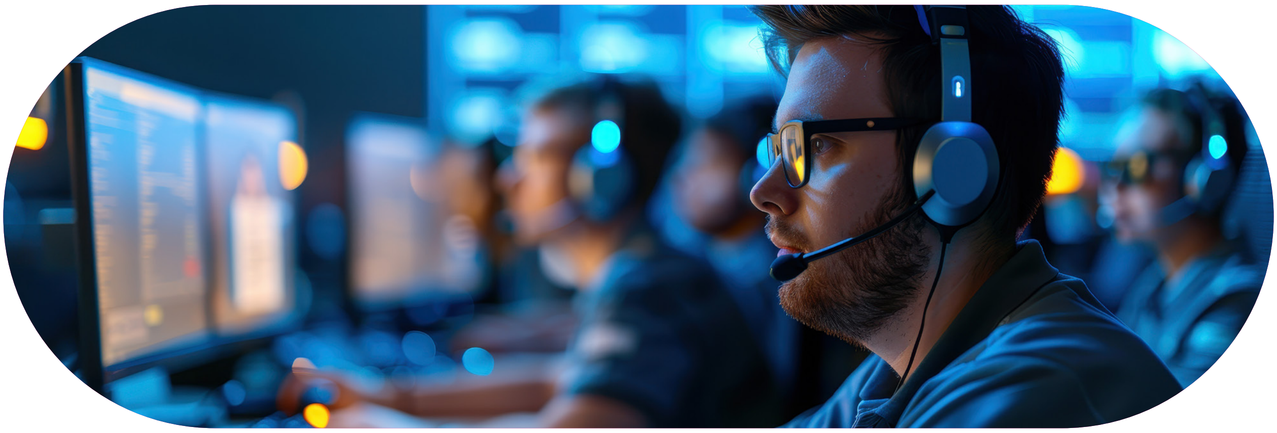
Ensuring Rapid Incident Containment

Once an incident is identified, swift containment is essential to prevent further spread. As part of an Incident Response service Cyberfort can implement isolation protocols to restrict the attacker's movements within the network. For instance, if a ransomware attack is detected, automated containment measures can disconnect the infected system from the network immediately to prevent the malware from propagating. Additionally, through the deployment of endpoint detection and response (EDR) solutions that provide real-time visibility into endpoints (e.g., laptops, desktops, servers) allows security teams to isolate or quarantine compromised devices quickly. These containment strategies are crucial for limiting damage and enabling a focused remediation effort.

Facilitate Effective Remediation and Recovery
Remediation involves eliminating the threat from affected systems and restoring the customers environment to a secure state. Cyberfort has forensic investigation capabilities to determine the root cause of an incident and ensures that any vulnerabilities exploited by attackers are addressed. This can involve patching systems, updating firewall configurations, or enhancing access controls. To support recovery, Cyberfort supports customers to restore data from secure backups, rebuild affected systems, and validate the integrity of all recovered systems. Regular disaster recovery exercises can ensure that both Cyberfort and the customer are prepared to restore operations quickly and efficiently after an incident.

Provide Continuous Improvement through Post-Incident Analysis - After an incident, it's essential to conduct a post-incident analysis to understand what worked well and what could be improved. Cyberfort can facilitate a review with a customer to analyse the incident, identify lessons learned, and make recommendations for strengthening defences. This process includes updating response playbooks, implementing additional detection tools, and refining incident response workflows.

By deploying advanced monitoring systems, establishing clear incident response plans, ensuring rapid containment, and supporting remediation and recovery efforts, Cyberfort can effectively protect customers from evolving threats. Continuous improvement through post-incident analysis strengthens the response framework, ensuring that both detection and response mechanisms remain agile, effective, and aligned with the latest threat landscape. This proactive, comprehensive approach enables Cyberfort to provide resilient, adaptive protection that minimises the impact of cyber incidents on our customers.



Final Thoughts

Cyber resilience audits and reviews are essential components of a comprehensive security strategy, enabling organisations to identify vulnerabilities, evaluate response capabilities, and drive continuous improvements in their ability to withstand, recover from, and adapt to cyber threats. By leveraging the insights and recommendations provided by these audits, organisations can strengthen their defences, enhance their incident response readiness, and foster a more resilient digital ecosystem.

As discussed in this article it is now time for IT teams to partner with specialist third party cyber security providers to take action on the results from their Cyber Resilience Audit and Reviews if they want to stay one step ahead of attackers and remain secure, compliant and resilient in the future.

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

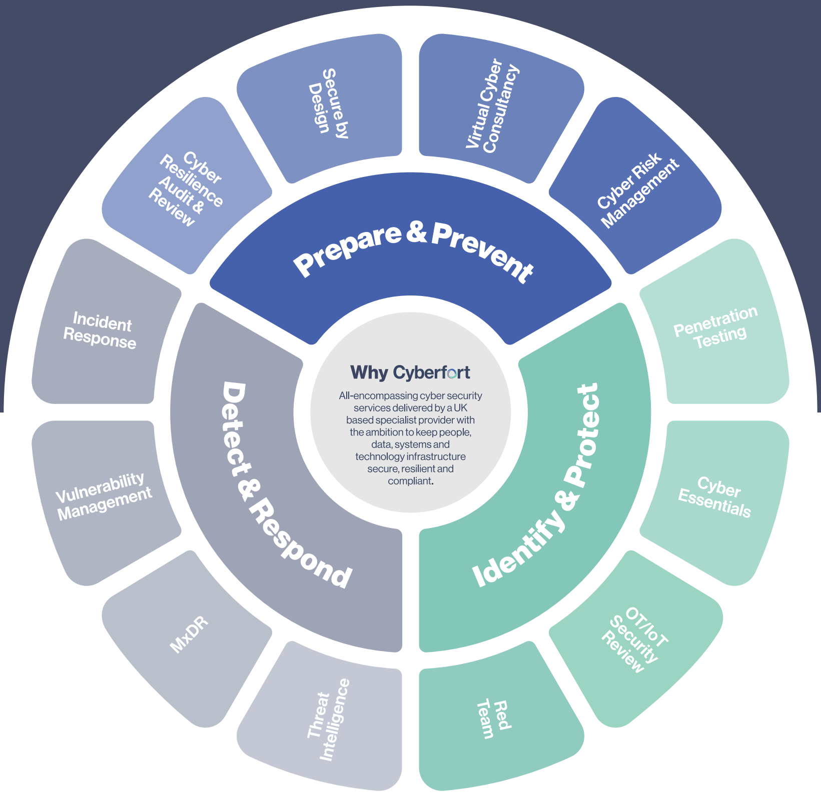
https://www.techrepublic.com/article/microsoft-cyber-attacks-uk-ai/#:~:text=Microsoft%20has%20called%20on%20UK%20business%20leaders%20to,vulnerable%20and%20the%20remaining%2039%25%20facing%20high%20risk

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.


Why Cyberfort
All-encompassing cyber security services delivered by a UK based specialist provider with the ambition to keep people, data, systems and technology infrastructure secure, resilient and compliant.
Prepare & Prevent
Cyber Resilience Audit & Review
Secure by Design
Virtual Cyber Consultancy
Cyber Risk Management
Identify & Protect
Penetration Testing
Cyber Essentials
OT/IoT Security Review
Red Team
Detect & Respond
Threat Intelligence
MxDR
Vulnerability Management
Incident Response

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