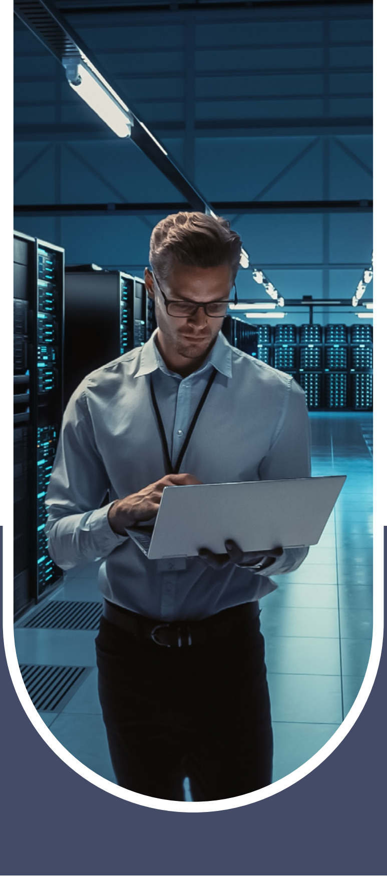
Cyberfort
Expert-led. Security Driven.

WHITE PAPER

Discover how the right Cyber Resilience Audit and Review will improve the Cyber Security strategy for your organisation

Introduction to the cyber resilience audit and review



It is no secret - cyber security breaches and attacks remain a major risk to many organisations across the UK. In the latest UK Government Cyber Security Breaches report released in April 2024 (1) they discovered 50% of businesses and 32% of charities have experienced a security breach or attack in the past 12 months.

Many of the attacks are not new news and usually quite unsophisticated. With the primary sources of attacks being identified in the report as Phishing (84%), Social Engineering (35%), devices being targeted with Malware (17%) and company bank accounts being hacked (7%).

However, why is the prevalence of cyber-attacks still happening and being seen as a major organisational risk? Especially when it is reported that 63% of medium sized organisations and 72% of large organisations have undertaken some form of cyber resilience security audit in the past 12 months?

Cyber Security risk is not only the IT team's responsibility it should also be on the board of directors' agenda as they are responsible for the running of an organisation on a day-to-day basis.

At Cyberfort we have helped many organisations undertake audits of their cyber security environment to improve their exposure to cyber security risks and to inform their ongoing cyber security strategy. Quite often when we start work with Cyber Security teams, we discover many who have undertaken audits of their cyber security resilience themselves without specialist independent 3rd party knowledge or used a quickfire audit from a non-specialist cyber security partner. The information from these cyber resilience audits and reviews usually are not asking the right questions or capturing enough detail so meaningful action can take place following the audit.

For example, does the last Cyber Resilience Audit and Review your organisation carried out cover the 4 key principles set out by the NCSC in their Cyber Assessment Framework:

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

Where to start and how to prepeare

To help combat the disparate nature of Cyber Resilience audits the NCSC launched their Cyber Resilience Audit Scheme (2) at Cyber UK 2024. The purpose of the scheme is to 'understand the level of cyber resilience of individual organisations in their sector and will also contribute to a more accurate picture of cyber resilience at both a sector and national level'.

So where should your organisation start when undertaking a Cyber Resilience Audit and Review?

and

How can the right Cyber Resilience Audit and Review inform and enable your cyber security strategy today and in the future?

Firstly, those responsible for cyber security in their organisation need to start by asking:

When did the last Cyber Resilience Audit and Review take place and did it actually help inform the organisations cyber security strategy?

Was the Cyber Resilience Audit and Review linked to the organisations risk objectives or was it predominantly focused on the technology aspects?

Did the audit and review cover the basics of managing cyber security risk including:

- Who has access to the organization's most valuable information?
- The likeliest targets of cyber attacks?
- Which systems would cause the most disruption if they were attacked?
- Which data if lost or corrupted would cause financial or personal loss?
- Is the management ready to take action should a security breach occur?

Did the audit and review cover internal vulnerabilities e.g. lack of trained staff, technical debt, resources and tooling?

By analysing the last Cyber Resilience Audit and Review your organisation undertook against the questions above, IT teams and boards of directors can start to understand if the review was fit for purpose. They can also assess if the organisation requires specialist expertise/knowledge to carry out an audit and review of this nature.

Capturing and unlocking the right information from your Cyber Security Resilience Audit and Review for a better strategy

As an NCSC Assured Cyber Security Consultancy, Cyberfort enables organisations to undertake Cyber Resilience Audits and Reviews to improve their overall cyber security posture. We believe an audit of this nature should not be undertaken in a siloed fashion. The information collected from the audit and review should be taken from across the business to create a true picture of vulnerabilities with clear actionable next steps.

So, what are the areas which should be covered from this programme of work?

No two organisations are the same. Before a cyber resilience audit and review happens a trained and accredited consultant should take the time to understand the nature of work undertaken and where the potential security vulnerabilities may be.

A cyber resilience audit and review should start with evaluating how your organisation currently manages security risk and cover:

Governance – How effective is your organisational management aware of security risks at a board level, are there clear roles and responsibilities in relation to cyber security, are the risks and control procedures in place and are the right people aware of them, the confidence levels in your people, processes and systems from a security standpoint and any potential supply chain risks.

Protective measures against cyber attack – Are the right service protection and policies in place, how are identities and access being managed across different applications, what is the device management strategy, how is data being managed, stored and used in transit, does your organisation have a 'secure by design' strategy, and are your networks and technology systems actually designed to be resilient with potential vulnerabilities identified and documented.

Effective detection of cyber security events – Does your organisation have the right level of security monitoring in place, are the alerts being generated actually being actioned on, can the IT team effectively identify different cyber security incidents, is your organisation in a reactive state or can it proactively identify threats before its too late and are the staff who are tasked with responding to these incidents trained to the appropriate level.

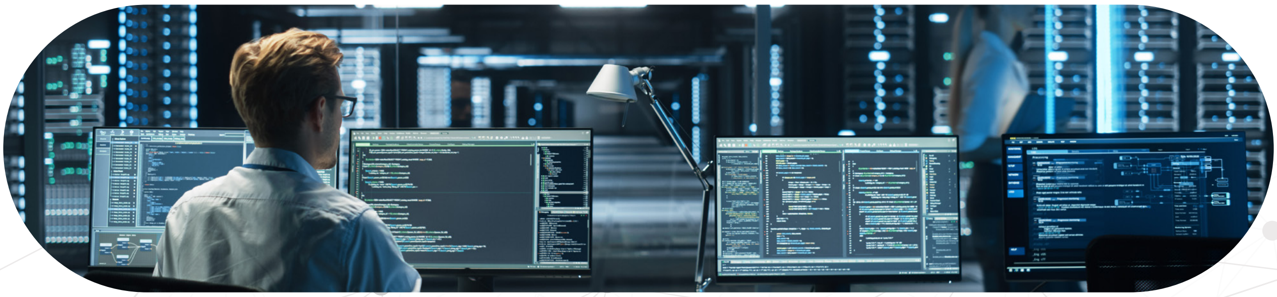
Minimising impact of cyber security events – Does your organisation have a documented response and recovery plan, when was the last time the plan was fully tested, are you able with the staff available able to undertake sophisticated root cause analysis of incidents, can you use historical incidents to drive improvements forward?

As you can see from the highlighted areas on the previous page, of what a ‘good’ audit and review should cover at a basic level, undertaking a Cyber Resilience Audit and Review is not as simple as it may seem. Many organisations unfortunately still see it as a task to just be completed. They often do not have the specialist expertise available to them to complete the audit and extrapolate the right information from the audit to improve their overall cyber security strategy.

By working with an NCSC Assured Cyber Security Consultancy, organisations can have the confidence that those consultancies who are assured by the NCSC have proven that the services they deliver meet the NCSC’s standard for high quality, tailored cyber security advice and can unlock the data and information which will keep them safer from potential attacks and make sure they are compliant with industry regulations. The data and information from the review and audit should not be taken in isolation. It should be linked to the overall cyber security and risk management strategy for an organisation and be seen as a core foundational pillar for improving an organisations cyber security strategy. By engaging a 3rd party partner who has the right accreditations for this work, organisations can also benefit from benchmarking against others in a similar sector and assess their maturity levels.

Next steps and moving forward

In this article we have covered the importance of Cyber Resilience Audit and Reviews. We have discussed how the information collected could help to inform your organisations cyber security strategy both now and in the future. Building a robust cyber security strategy is not an easy task but it all starts with the audit and review. At Cyberfort we believe the NCSC launching their Cyber Resilience Audit and Review scheme is a good initiative and will help to improve cyber security standards across the UK.



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

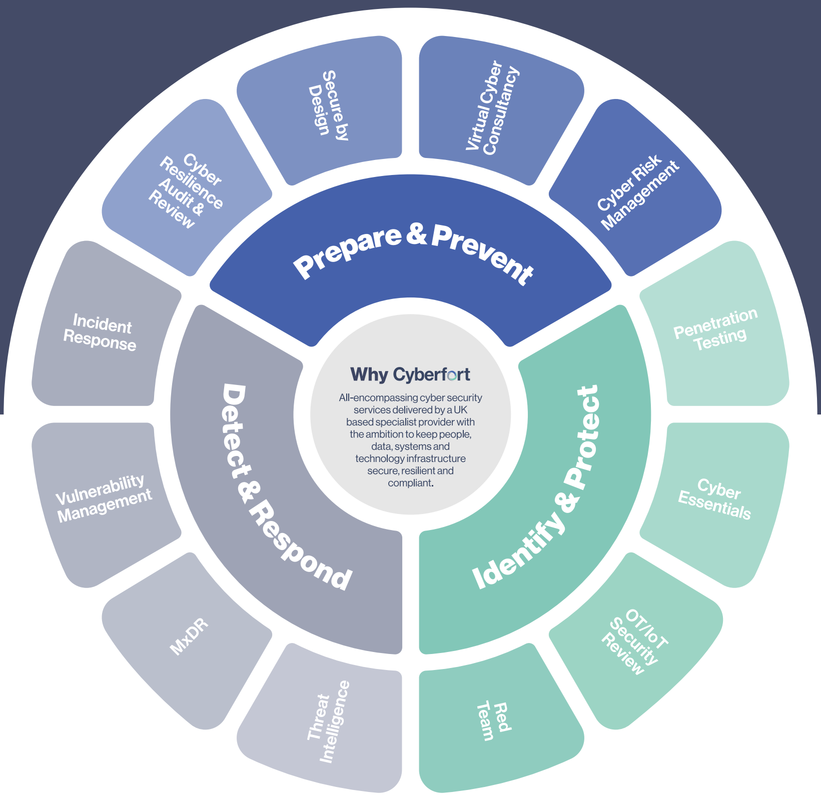
[2] https://www.ncsc.gov.uk/schemes/cyber-resilience-audit/introduction#:~:text=What%20is%20the%20Cyber%20Resilience%20Audit%20Scheme%3F%20Cyber,audits%20to%20customers%20in%20a%20range%20of%20sectors

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 Secure Cloud and 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