The ABI
Together Driving Change

From prevention to resilience

Good practice guidance on cyber resilience

August 2026

The ABI | 30 Fenchurch Street, London EC3M 3BD
T +44 (0) 207 600 3333 | abi.org.uk

Table of Contents

About us 2

Introduction 3

Good practice guidance on cyber resilience 3

The role of cyber insurance 3

Existing standards 3

Cybersecurity good practice 4

Core controls included in Cyber Essentials 4

- Identity and access management 4
- Multi-factor Authentication 4
- Endpoint security 5
- Vulnerability management 5

Controls to build resilience 6

- Training and staff awareness 6
- Backups 6
- Incident response and continuity planning 7
- Logging and monitoring 7
- Encryption 7
- Supply chain understanding and security 8

Conclusion 8

Additional resources 9

About us

The ABI is the definitive voice of the UK's world-leading insurance and long-term savings industry, which is the largest sector in Europe and the third largest in the world.

We represent more than 300 firms within our membership including most household names and specialist providers, providing peace of mind to customers across the UK.

Our sector is productive, inclusive and essential to the UK economy and together, we are driving change to protect and build a thriving society.

Find out more at **abi.org.uk**

Introduction

The ABI has convened the insurance industry and government representatives to explore how collaboration can improve the cyber resilience of organisations across the UK. This document sets out what good looks like in cybersecurity and is based on the experience, insight, and claims data from cyber insurers to define what controls can best improve an organisation's cyber security posture.

Our guidance is not an exhaustive list of all cybersecurity measures that organisations could take. Neither is it a baseline that all organisations must achieve. It is intended to support wider efforts to drive up UK cyber resilience, including actions being taken by government and other stakeholders, and provide a clear selection of the most impactful cybersecurity measures and controls, to help move the dial on cyber resilience across the UK.

Good practice guidance on cyber resilience

The role of cyber insurance

Cyber insurance is a powerful tool to improve organisations' resilience to cyber incidents. It not only provides financial cover in the event of an incident, but typically includes a service element, offering a range of proactive and reactive risk management services – from threat monitoring and employee training, to cyber forensics and system restoration.

A standalone cyber insurance policy is a partnership between the insurer and the insured, working together to reduce the likelihood of a cyber incident and limit the impact should an incident occur.

Cyber insurance is a competitive market where providers offer different products, prices and levels of cover to organisations based on their own risk appetites and the different risks that organisations face. We are not trying to restrict this competition with our guidance. The controls featured below are not all required by cyber insurers to provide cover and each insurer will consider them and other factors independently as part of their underwriting processes.

Existing standards

Existing schemes like Cyber Essentials (CE) can serve as a baseline for preventing common cyberattacks. CE was designed by the National Cyber Security Centre (NCSC) in 2014 to help protect against attacks from the most common vectors – attacks carried out via the internet using publicly known techniques. It sets out five core controls to mitigate these kinds of attacks. Research carried out by the UK government has found CE to be effective in reducing cyber incidents, with the NCSC stating that around 50,000 UK organisations have an active CE accreditation.

Whilst CE helps to protect against common threats, other threats have emerged which require additional controls. Alongside preventative measures, ABI members have emphasised that they also carry out a broader assessment of cyber risk, looking at how prepared an organisation is to respond to a cyber incident, the potential severity of an attack, and how organisations can recover from an incident. Our members recommend that businesses should consider these aspects of cyber resilience in addition to the core controls in CE.

Cybersecurity good practice

Having the following controls in place will demonstrate that an organisation has carefully considered their cybersecurity posture. Such an organisation will have a strong approach to cybersecurity and should be well-placed to prevent, detect, respond to and recover from a range of cyberattacks.

It may not be proportionate for all organisations to implement the full suite of controls detailed below, but all organisations should carefully consider their cyber posture. Our guidance can be used to support discussions with brokers and insurers on the cyber risks a business faces, what measures would be most appropriate to mitigate these risks, and to inform questions to insurers on what cyber services are included in their policies.

There is clear overlap between the controls our members identified and those covered by CE. The five core controls in CE – secure configuration, user access control, malware protection, security update management and firewalls – are all included in the good practice guidelines. We have set these out first, with the additional six measures that members identified as being important for cyber resilience covered subsequently.

Core controls included in Cyber Essentials

Identity and access management

Threat actors are increasingly seeking to hijack credentials and use valid accounts rather than forcing their way into their targets' systems. Identity and access management (IAM) or 'user access control,' as it is referred to in CE, can block unauthorised access by malicious actors while allowing authorised users to do everything they need to do, and no more. It will typically involve:

- User authentication – via passwords, Multi-Factor Authentication (MFA), or biometrics.
- Authorisation – granting verified users the appropriate levels of access to a resource; most access control frameworks grant users only the permissions necessary to perform their role.
- Identity governance – who has access to what and why; this includes auditing user permissions to restrict access levels, logging user activity, enforcing security policies and flagging violations.
- Privileged Access Management – for high-risk accounts such as Directors or IT staff.

Multi-factor Authentication

Multi-factor Authentication (MFA) is a method to verify a person's identity to allow access to a digital service or system, requiring one or more proofs of identity. Typically, a password or PIN will be required as a first stage, followed by another piece of information, such as a response to an in-app prompt. This can include face or fingerprint recognition.

Most insurers now treat MFA as a critical cyber underwriting consideration. Cover or claims may be declined if MFA has not been deployed in line with the insurer's requirements. While requirements will vary across insurers, insurers will commonly require MFA for privileged and admin accounts, email access, remote access, cloud applications, and endpoints.

How MFA operates across an organisation's systems is also a consideration. Phishing-resistant forms of MFA are strongly preferred, including authenticator apps, passkeys and biometric authentication. The NCSC advises using strong cryptographic authentication approaches. MFA over SMS tends only to be seen as suitable for lower-risk scenarios. Email-based codes (especially to the same inbox being protected) are also seen as weaker.

Endpoint security

Endpoint security, including malware protection, acts as a network's first line of defence by protecting endpoints (desktops, laptops, mobile devices, servers etc.) against cyberattacks. It has grown in importance as remote work and the proliferation of connected devices have massively increased the number and kinds of endpoints threat actors can exploit.

Antivirus software was the original endpoint security. Today's antivirus software, known as next-generation antivirus, can identify and fight newer types of malware. However, anything beyond a handful of devices will likely require a more sophisticated solution, such as an Endpoint Protection Platform (EPP) or an Endpoint Detection and Response (EDR) solution.

EDR offers a greater level of security through continuously monitoring the files and applications that enter each device, checking for any activity that indicates malware or other threats. EDR also collects and stores data so it can be used for analysis. EDR can be used to automate responses, such as disconnecting and quarantining devices to mitigate damage.

Firewalls – one of the core controls listed in CE – form a part of endpoint security. They are not only an endpoint control, as they sit at the network layer, but they act as a complementary layer of endpoint defence. Host-based firewalls are also standard in endpoint security products.

Vulnerability management

Unaddressed exploits and vulnerabilities remain a major vector for cyberattacks. They can allow threat actors to launch cyberattacks, gain unauthorised access to systems or data and damage an organisation and its operations. Examples of common vulnerabilities include firewall misconfiguration or unpatched bugs in an operating system's remote desktop protocol that could allow cybercriminals to take over a device remotely.

Vulnerability management involves:

- Asset visibility: mapping an organisation's entire IT estate and establishing awareness of the operational health, status and security of all IT assets.
- Regular scanning and monitoring of systems: this can include automated scanning for known and potential vulnerabilities and episodic assessments such as penetration testing.
- Prioritisation: categorisation by level of criticality based on threat intelligence sources (e.g. Common Vulnerability Score System and list of Common Vulnerabilities and Exposures).

- Remediation of vulnerabilities: patching, configuration changes, compensating controls, or retiring a vulnerable asset. This should be done in a timely manner; for example, CE requires any critical vulnerabilities to be patched within 14 days of being identified.

Secure configuration and security update management, which are both core controls in CE, come under the umbrella of vulnerability management.

Controls to build resilience

Additional controls identified by ABI members as important for developing an organisation's cyber posture further, beyond just prevention to resilience, are roughly ranked for effectiveness below. However, as noted above, insurers all have different underwriting processes and have different assessments on the impact that each control has in preventing or mitigating the damage caused by a cyber incident.

Training and staff awareness

Business email compromise, phishing and social engineering are major causes of financial losses and cybersecurity professionals cite 'low security awareness among employees' as a top concern. Compromising end user devices through spear phishing attacks is frequently cited as the initial step of advanced persistent threats, often leading to data breaches. AI is exacerbating the problem, with threat actors able to send more realistic and a larger number of phishing attempts.

Organisations should ensure that staff are trained appropriately and create a non-punitive culture of security and learning. It is important to note that organisations should not assume that carrying out training is sufficient and technical controls are still needed.

Members have advised they judge good practice based on:

- Regular training, with the content updated to reflect likely scenarios and threats, rather than one-off onboarding sessions
- Training completion and participation rates
- Time taken to report simulated phishing emails appropriately
- Having regular phishing simulation messages in place to test staff understanding, and phishing simulation failure rates.

Backups

The growth of ransomware has underscored the importance of having robust backups in place. Backups can negate or reduce the impacts of various kinds of ransomware attack, including wiper malware, as well as non-malicious incidents including device failure, data corruption, system crashes, and accidental deletion. The NCSC recommends organisations to have backups, including through CE, but they are not mandated as part of the CE certification.

Backups should be resilient, immutable (files locked in a read only state) or offline, regularly tested and protected from credential compromise. There will be different approaches across insurers, but considerations will include: the number of copies, the medium in which it is stored, where it is stored, and if it's stored online or offline.

Many organisations now use the cloud to store their data. However, cloud sync lacks lengthy version histories, is not immutable (any changes such as deletion or corruption of a file will be replicated to the cloud immediately), and it is not offline or air-gapped. If attackers gain access to your cloud account, they can delete, encrypt or corrupt files, with these changes being synchronised across your systems. Cloud backups however may be reliable if they are properly isolated, access-controlled, immutable or offline and regularly tested.

Incident response and continuity planning

Beyond prevention, insurers look at the next stages of response and recovery. Organisations must be prepared for the worst to happen and have a plan in place so they can effectively respond to and recover from a cyber incident. Carrying out effective business continuity planning reduces business interruption and recovery costs, which is often the largest portion of a cyber claim.

Insurers will typically consider:

- Whether an organisation has a clear, up-to-date incident response plan in place. This should include an event playbook, escalation procedures, contacts, and roles and responsibilities.
- If an incident response plan been tested in a realistic tabletop exercise. Some cyber insurers will provide access to experts to carry out this kind of exercise.
- If an incident response been integrated into cybersecurity risk management activities.
- Documentation of business continuity plans.

Logging and monitoring

Logging and monitoring refers to the continuous collection, storage, and analysis of system, network, and user activity data. This includes records of logins, system changes, network traffic patterns, access attempts, and other ‘events’ happening in an organisation’s digital environment. The NCSC advises retaining key logs for at least six months, given incidents are often detected late.

Logging and monitoring applies across all the other controls. Logging and monitoring are valuable both in a proactive and reactive way, as they can:

- Help identify and detect threats to your devices and IT systems.
- Enable cybersecurity analysts to work out what is going on across network and systems.
- Identify patterns of behaviour, in turn providing indications of anomalies and attacks.
- Enable an organisation to tell if devices are being used in accordance with policy, and audit of how controls have been implemented.
- Be used to investigate a cyber incident and in cyber forensics.

Encryption

Encryption uses algorithms to render data indecipherable. Only the right decryption key can convert it back into readable text. It has become widely expected in safeguarding sensitive data, especially for organisations using the cloud, which has expanded the possible attack surface. In certain industries, such as healthcare and financial services, encryption is also required by law.

Insurers value encryption because it reduces the frequency and severity of cyber claims and shows mature cyber hygiene. For example, it could mitigate the leverage a threat actor has in cases of data exfiltration or in a double extortion ransomware attack (when a ransom is demanded for both for a decryption key and to prevent the leaking of data), by rendering exfiltrated data unreadable.

Insurers and the NCSC both advise that data should be encrypted at rest and in transit.

- Data at rest: information stored on devices, servers, backups, databases or in cloud storage. Common methods include full disk encryption (such as BitLocker), file-level encryption or database encryption.
- Data in transit: data transferred via email, web traffic, file transfers or over remote network connections. Various methods are used, including TLS/HTTPS, secure Virtual Private Networks (VPNs), or encrypted emails.

Supply chain understanding and security

Third-party and supply chain cybersecurity risks are escalating. Cyber resilience is no longer limited to just protecting your own systems and organisations must consider how exposed they are via their suppliers, customers and other parties they interact with.

Insurers now put emphasis on vendor due diligence, continuous monitoring, and cyber supply chain risk management practices. This can be important even when dealing with the largest of companies. These should include strong access controls for vendors, vendor risk assessments, evaluations of vendor security and compliance with any contractual cybersecurity requirements.

As a minimum, organisations should be asking companies in a supply chain to ensure they are mitigating the most common internet-based attacks, as evidenced through CE certification.

Carrying out exercises to work out who your critical vendors are, as well as dependency mapping, is also growing in importance. Organisations should consider what arrangements they have in place to recover and move their data, should a partner they rely on fall victim to a cyberattack themselves.

Conclusion

Cyber threats are escalating. Organisations across the UK should implement robust controls – such as multi-factor authentication, endpoint security, staff training, backups, and supply chain risk management – to better prevent, detect, and recover from attacks.

These good practice guidelines should be considered by all organisations, whether or not they choose to purchase a cyber insurance policy. Ultimately, strong cyber resilience has become a cost of doing business in our increasingly connected age and is a strategic imperative for the safeguarding of the UK's economy.

Additional resources

The NCSC has a range of free resources available to help organisations with their cybersecurity:

- The NCSC's Cyber Advisor service makes it easy to find trusted companies who can help implement cybersecurity controls
- Independent validation can be achieved through gaining certification (ideally CE+) through an NCSC-recognised Certification Body, overseen by IASME, NCSC's delivery partner
- Further information on logging and monitoring
- Further advice on Ransomware-Resistant backups
- Companies unfamiliar with carrying out tabletop exercising can use free resources from the NCSC or seek support from a company offering a NCSC-recognised Exercising service
- Should the worst happen, organisations can get help from companies offering NCSC assured cyber incident response services

Disclaimer

This document was produced by the ABI for general information purposes only. While care has been taken in gathering the information and preparing the document, the ABI does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied.

The ABI accepts no responsibility or liability for any loss or damage of any nature as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this document. This document does not constitute legal or financial advice of any kind.