

CYBER SECURITY AWARENESS MONTH

Large Orgs & CNI

Strong cyber foundations

- › Cyber risk
- › Building strong foundations
 - › Cyber Governance for Boards
 - › Cyber Assessment Framework
 - › Early Warning
 - › Assured Services
 - › Preparedness, exercising and recovery
- › How to support Cyber Security Awareness Month
- › Assets





Throughout October, the National Cyber Security Centre will support Cyber Security Awareness Month by encouraging practical, expert guidance to help UK businesses strengthen their cyber resilience and bolster their defences.

This year's international theme, Don't Make It Easy For Them, focuses on making life harder for cyber criminals. The NCSC's supporting theme, Strong Cyber Foundations, focuses on the actions organisations can take to strengthen resilience before an incident occurs.

For boards, senior leaders, large organisations and cyber professionals, strong foundations mean understanding cyber risk, embedding governance, strengthening resilience and preparing for disruption.

We're encouraging organisations to:

- › Understand and prioritise cyber risk
- › Strengthen cyber governance arrangements
- › Use the Cyber Assessment Framework to assess and improve resilience
- › Adopt Early Warning
- › Improve preparedness and recovery planning

We invite you to help reinforce resilience messages and amplify this campaign by sharing our messaging and signpost your customers, stakeholders, and networks, to relevant NCSC guidance and services.

CYBER SECURITY AWARENESS MONTH



National Cyber
Security Centre
a part of GCHQ

STRONG
CYBER
FOUNDATIONS

Recognising cyber risk

- Cyber security is considered a high priority for senior management in around seven in ten businesses (72%).
- Larger organisations continue to experience higher levels of cyber disruption. Medium (65%) and large (69%) businesses were more likely to have experienced a cyber breach or attack in the last 12 months compared to micro (42%) and small (46%) businesses. Despite this, formal incident response plans remain relatively uncommon (25% of businesses).
- Phishing attacks remained the most prevalent type of breach or attack by far (experienced by 38% of businesses).
- AI adoption is outpacing cyber risk management. Around a third of businesses (31%) were either using AI, actively adopting it or considering its use. Of those organisations, only 24% reported having cyber security practices or processes in place to manage AI-related risks. As AI accelerates both offensive and defensive cyber capabilities, the fundamentals matter more than ever.
- Cyber incidents can drive reputational and financial harm. There has been an increase in businesses reporting that a breach or attack resulted in loss of revenue or share value (2% in 2024/25 to 5% in 2025/26) and reputational damage (1% in 2024/25 to 3% in 2025/26).

NCSC tools & services

Cyber Governance for Boards

www.ncsc.gov.uk/cyber-governance-for-boards/overview

The NCSC's Cyber Governance Training programme is available to boards and is designed to empower them to confidently implement the Cyber Governance Code of Practice.

This training ensures boards are equipped to meet their cyber security responsibilities with clarity and confidence.

The Cyber Governance Training aligns with the five core principles from the Cyber Governance Code of Practice, which are:

Risk Management

Strategy

People

Incident Planning, Response & Recovery

Assurance & Oversight

Board-level responsibility for cyber security sat at 31% of businesses. Supports messaging around leadership accountability and Cyber Governance for Boards¹.



NCSC tools & services

Cyber Assessment Framework

www.ncsc.gov.uk/collection/cyber-assessment-framework

The Cyber Assessment Framework, is a tool to help organisations assess and improve their cyber security and resilience. Built around cyber security and resilience outcomes, it provides a systematic approach to understanding how cyber risks to critical functions are being managed and identifying areas for improvement.

It is particularly relevant for organisations responsible for critical services and infrastructure, helping them understand and manage risk across complex technology estates, interconnected supply chains and operational environments. This is increasingly important as organisations face capable and well-resourced cyber actors.



NCSC tools & services

Early Warning

www.ncsc.gov.uk/section/active-cyber-defence/early-warning

For many organisations, the cost of network monitoring is prohibitive, and the specialist skills it requires often aren't available in-house. Early Warning helps organisations move from understanding risk to actively identifying issues before incidents escalate.

Early Warning is a free service that notifies organisations who have enrolled, of any potential cyber attacks, intrusions or vulnerabilities detected on their network, as soon as possible, therefore giving invaluable time to detect and stop a cyber incident before it escalates.

NCSC tools & services

Preparedness, exercising and recovery

<https://www.ncsc.gov.uk/collection/what-to-do-when-cyber-attacks-disrupt-your-organisation>

Strong cyber resilience extends beyond preventing incidents. Organisations should be prepared to respond to and recover from cyber attacks when they occur.

The NCSC provides a range of guidance and resources to help organisations improve their preparedness, including incident response and recovery guidance, exercising programmes such as Exercise in a Box, and advice on building resilience across critical services and supply chains.

Preparedness activity helps organisations understand their response capabilities, identify gaps before an incident occurs and improve their ability to recover quickly from disruption.

How you can support Cyber Security Awareness Month

Encourage action

Help SMEs take the next step on their cyber resilience journey.

Whether that's adopting passkeys, using the Cyber Action Toolkit, working towards Cyber Essentials or signing up for Early Warning

Signpost

Use your channels and networks to share relevant NCSC guidance, products and services that can help organisations build strong cyber foundations.

Social media

Share or comment on the NCSC's content. Use the suggested copy and hashtags provided in this pack.

Tag NCSC and use the hashtag:

#CyberMonth2026

Assets

[Click here to download all assets](#)

Assets within the pack

- Social statics in 1x1 9x16, 16x9
- Email signature

Planned Cyber Month Content themes:

w/c 5th – Passkeys & Cyber Governance for Boards

w/c 12th – Early Warning & Cyber Essentials

w/c 19th – Cyber Essentials & Cyber Assessment Framework

w/c 26th – Cyber Action Toolkit



You can find us on: [LinkedIn](#), [X \(Twitter\)](#), [Instagram](#), [Bluesky](#), [Facebook](#), [Threads](#)



Suggested Copy

Cyber threats are evolving, but so are the ways to protect against them. This #CyberMonth2026, explore @NCSC's guidance to help your organisation stay secure.
#SecureOurWorld

Learn how your organisation can improve its cyber resilience all #CyberMonth2026 with tools and advice shared by @ncsc throughout October
#SecureOurWorld

Cyber security is everyone's responsibility. This #CyberMonth2026, @NCSC is sharing tools and tips to help organisations and individuals build resilience together.
#SecureOurWorld

Wondering how to boost your organisation's cyber resilience? This #CyberMonth2026, @NCSC is sharing expert tips and tools all October long.
#SecureOurWorld



Thank You

For terms and conditions, please refer to the NCSC website:
[Terms & conditions - NCSC.GOV.UK](https://www.ncsc.gov.uk/terms-conditions)