Department for
Science, Innovation
& Technology

Government Cyber Resilience Pledge

Information Pack

April 2026

Contents

Context

Hostile cyber activity in the UK is growing more intense, frequent and sophisticated. This is causing significant financial and social harm to UK businesses and citizens, with the average cost of a significant cyber attack for an individual business in the UK costing almost £195,000. When scaled to an annual UK cost, this generates an estimate cost to businesses of £14.7bn. This does not include the wider disruption across the economy caused by cyber attacks. There is a direct and active threat to our economic and national security which requires an urgent collective response.

Recent high-profile cyber incidents show how attacks can seriously disrupt operations and damage profitability. Attack surfaces are expanding with vulnerabilities in supply chains becoming increasingly exploited. In this progressively hostile landscape, organisations recover better from incidents when they have planned for the worst and rehearsed their business continuity and recovery.

The government is taking significant action to counter the cyber threat and has developed tools to help businesses to defend themselves, but we cannot do this alone. Against this backdrop, a ministerial letter was written to the CEOs and chairs of leading UK companies (including the FTSE 350) inviting them to take three specific actions that will have an immediate positive impact on the cyber resilience of our nation. To build on the excellent response from industry, the government has developed a voluntary Cyber Resilience Pledge which formalises the three actions contained within the letter and provides a tangible way for organisations to differentiate themselves on cyber resilience, from their competitors.

Government Cyber Resilience Pledge

Organisations signing the pledge commit to take the following actions:

1. **Make cyber a Board responsibility:**
    a. Implement all actions within the Cyber Governance Code of Practice.
    b. Ensure all board members undertake the NCSC's Cyber Governance Training within three months and then on an annual basis.
2. **Sign up to Early Warning:**
    a. Register for the Early Warning service within one month of signing the pledge
3. **Require Cyber Essentials across supply chains:**
    a. Register to the Cyber Essentials Supplier Check Tool within two months of signing the pledge.
    b. Ensure that a comprehensive audit of Cyber Essentials coverage has been conducted across your entire supply chain and that it is presented to and discussed by the Board.
    c. Take a risk-based approach to requiring Cyber Essentials across your supply chain (which may include requiring it from all suppliers). If Cyber Essentials is not required for certain suppliers, the board should ensure that this decision aligns with the organisations risk appetite and strategy and that adequate assurance is obtained through other means.

In addition to the above three actions, organisations signing the pledge would commit to the following:

- **Encourage these actions within your own supply chains** - signatories should strive to engage with their suppliers to understand and better manage the cyber security risks that they are exposed to through their supply chain and encourage adoption of the above measures.
- **Publish the signed pledge declaration on your website** - within two months, publish the signed pledge declaration on your company website. Additionally, publish an annual public update, either in your annual report or on your company website, on the steps taken to deliver against the pledge.

While the pledge is voluntary, we expect organisations that sign to implement the three actions in line with the timeframes outlined below. Where organisations do so, and are able to demonstrate such, we will seek opportunities to publicly recognise and acknowledge those measures taken to build resilience and secure the UK economy.

Why should organisations sign up to the pledge?

Security

The UK's technical authority – the National Cyber Security Centre – has stated that the three actions of the pledge, if applied at scale, will have an immediate positive impact on individual companies' resilience to cyber attacks, as well as material impact on the resilience of the UK economy.

Trust

Resilient businesses are built on foundations of strong cyber resilience. When done right, it is a strategic enabler and helps to build confidence and safeguard reputation, at a time when digital trust is currency for businesses. The pledge provides a tangible mechanism to promote transparency and build trust within your organisation and with key external stakeholders.

Recognition

The pledge allows organisations to publicly showcase the steps they are taking to strengthen their cyber resilience, and to be publicly recognised for doing so, both by government and industry.

Competitive Advantage

Cyber resilience supports business transformation. Organisations can therefore gain an advantage over competitors by managing their cyber risk more effectively and recovering better from incidents. By committing to taking the actions in the pledge, organisations can safeguard their growth and differentiate themselves from their peers.

National effort

Cyber resilience is a critical enabler of economic growth. Securing the UK's resilience will promote growth and foster a stable environment for investment and innovation. To do so and to combat threats to our economic and national security requires a collective effort. Organisations signing this pledge demonstrate a commitment to this joint endeavour.

Actions Overview

What is the Cyber Governance Code of Practice?

The Cyber Governance Code of Practice (the Code) brings together the critical governance areas that directors need to take ownership of in one place, in a form that is simple to engage with. The Code, which was co-designed with the NCSC and industry experts, is tailor-made for boards and directors of medium and large public-sector and private organisations. Whilst it has not been specifically created for small organisations, they play a critical role in the resilience of the UK economy and should seek to implement the Code's principles.

The Code forms part of the government's free package of support on cyber governance and should be the first point of reference for board members. It is underpinned by Cyber Governance Training, which helps boards and directors to strengthen their understanding of how to govern cyber risks, the Cyber Security Toolkit for Boards, which supports boards and directors in implementing the actions set out in the Code, and the Cyber Governance Mapping which shows how the Code maps to existing cyber standards and frameworks.

What is NCSC's Early Warning Service?

The NCSCs Early Warning Service helps organisations increase their confidence in the security of their network by providing free malicious activity notifications. It is a notification service that tells registered organisations about potentially suspicious activity on their network from a variety of open source, commercial and private data sources. It is free to sign up and only requires five minutes to set up.

What is Cyber Essentials?

Cyber Essentials is the minimum standard of cyber security recommended by the Government for organisations of all sizes. It is the cyber security equivalent of locking your windows and doors.

Developed by the experts at the NCSC, the certification scheme is aligned to five technical controls that protect against the most common cyber attacks.

This is critical for organisations looking to embrace the full benefits of digital technology. Through Cyber Essentials, organisations gain internal confidence that they are meeting the minimum baseline of technical cyber security. It is also increasingly used as an effective tool in managing third-party cyber security risks by providing reliable assurance that suppliers and partners have effectively implemented the technical controls.

Pledge Process

Timeline	Pledging organisation actions	Government actions
Immediate	CEO/Chair to sign pre-drafted pledge declaration (Annex A) and return it to DSIT mailbox (cybersecurity@dsit.gov.uk)	Upon receipt of declaration, add organisation name to the pledge list ahead of launch on gov.uk.
Within 1 month	Sign up to NCSC Early Warning service.	Confirm action has taken place.
Within 2 months	Publish signed pledge declaration on your website. Register for the Cyber Essentials Supplier Check Tool.	Confirm that signed pledge declaration is on the company website and that organisation has signed up to Cyber Essentials Supplier Check Tool.
Within 3 months	All board members to have undertaken the NCSC's Cyber Governance Training.	Confirm action has taken place.
After 12 months	Organisation to provide public update on tangible steps taken to deliver against the pledge on company website or in annual report.	Confirm that action has been completed.

Timing on pledge

While organisations can return the signed pledge declaration at any point, DSIT will update the list of organisations that have pledged on gov.uk on a quarterly basis.

FAQs

Does taking the pledge protect me from cyber attacks?	Taking the actions contained within the pledge will have an immediate positive impact on your organisation's resilience to cyber attacks. However, it does not guarantee protection from all cyber attacks. Organisations should therefore continue to take additional measures to enhance their resilience.
What organisations can sign the pledge?	The pledge has been designed primarily for medium and large organisations. However, organisations of any size in any sector can sign the pledge and we encourage all to do so.
Will DSIT monitor adherence to the pledge?	As this is a voluntary pledge, there is no formal assurance mechanism. Some of the pledge actions, such as signing up to both the Early Warning Service and the Cyber Essentials Supplier Check tool can be reviewed by DSIT. It is possible that in some instances, incompletion of an action may result in the company either withdrawing or being removed from the pledge.
If my company signs the pledge, is it an on-going commitment? Will our status be reviewed?	Companies that sign the pledge are committing to providing an annual public update on their progress. At that point, given that developing cyber resilience is an on-going endeavour, we would expect pledging companies to reaffirm their commitment and to undertake the actions on an annual basis. Additionally, given that the threat landscape is evolving and new complex cyber threats may emerge, government will continue to review the suitability of the pledge, with the potential of refining the actions at the end of a 12-month cycle.
Where does the pledge fit within the wider government cyber security advice, guidance and tools?	The NCSC and government have produced a wide range of advice, guidance and Codes of Practice to help organisations develop secure technology and build cyber resilience. The three actions of the pledge are a fundamental part of this holistic package of support and are the foundational actions to building economy-wide cyber resilience.
What is the relationship between the pledge and the Cyber Security & Resilience Bill?	The government is increasing protections for essential and digital services through the Cyber Security and Resilience Bill (CSRB), which, via secondary legislation, will set security and resilience requirements designed to be consistent with the NCSC's Cyber Assessment Framework (CAF) and other good practice frameworks. The pledge has not been specifically designed for organisations in scope of CSRB. However, the three actions in the pledge, which are based on learnings from previous attacks, remain essential and can help achieve outcomes in the CAF.
Can any organisation sign up to NCSC's Early Warning service?	The Early Warning Service is available for UK entities only.
Why does the pledge not ask organisations to become Cyber Essentials certified themselves?	All organisations should seek to become Cyber Essentials certified and we encourage pledging organisations to do so. It is effective for organisations of all sizes, in all sectors and many large companies have achieved Cyber Essentials or Cyber Essentials Plus. While organisations should ensure they have implemented appropriate controls relative to their risk profile, this action focuses on raising the security baseline across UK supply chains to drive resilience at scale.

Is Cyber Essentials a sufficient standard for my supply chains cyber security?	Cyber Essentials is the minimum standard of cyber security recommended by the government for organisations of all sizes. For many suppliers, Cyber Essentials certification alone will not provide sufficient assurance. Depending on the risk a supplier poses to your security, the protection of your data and ability to deliver your own services, you may ask for additional cyber security assurance.
What support is available to help organisations embed Essentials across their supply chains?	*For suppliers* - the Cyber Advisor scheme provides NCSC assured consultancy, designed to help small and medium organisations improve their cyber security and certify to Cyber Essentials. Currently, customer organisations can purchase a package of Cyber Advisor hours to allocate to suppliers. *For customers* - NCSC and DSIT have published a Cyber Essentials Supply Chain Playbook which provides practical guidance on how to embed Cyber Essentials within supply chains. The Cyber Essentials delivery partner, IASME, also provide a range of support services to organisations looking to require it in their supply chains.
I have hundreds/thousands of suppliers. Am I meant to require this from each and every one?	Cyber Essentials is proven to be effective. Where some organisations have mandated it from their third parties, they see up to an 80% reduction in incidents. Therefore, the more companies that have Cyber Essentials in your supply chain, the more resilient it will be. However, we recognise that for some companies with complex supply chains this will take time. The pledge invites boards to take a risk-based approach to requiring Cyber Essentials across their supply chain, which may result in requiring it from all suppliers.
Is Cyber Essentials only relevant for my suppliers?	No. Cyber Essentials can provide assurance that any business partner has put in place fundamental controls that protect against common cyber attacks. Organisations should seek assurance from all business partners that the Cyber Essentials controls are in place and to seek for independent verification through certification where possible.
I have lots of international suppliers – is Cyber Essentials still relevant?	The principles behind the Cyber Essentials scheme are universally relevant and the controls are important for businesses all over the globe. If your suppliers operate internationally, the most effective approach is to ask them to demonstrate they meet equivalent basic controls to those defined in Cyber Essentials.
Do multination organisations, with boards based outside of the UK, need to complete the NCSC Cyber Governance Training?	The NCSC Cyber Governance Training supports boards to implement the Cyber Governance Code of Practice. We encourage pledging organisations with non-UK based boards to undertake the NCSC Cyber Governance Training annually but complementary training offerings in their respective geographies, that support the adoption of the principles outlined in the Governance code, would be acceptable.
My organisations complies with other governance standards instead of the Cyber Governance Code of Practice. Can we still sign the pledge?	When the Cyber Governance Code of Practice was published, it was done so alongside a cyber governance mapping tool. This free tool illustrates similarities and differences between the Code and existing standards, such as NIST and ISO27001. For some standards and frameworks, you may need to take a few additional actions. We encourage you to use the tool to check whether you have any governance gaps.

Will publicly committing to the pledge increase my organisation's exposure to cyber threats?	There is no evidence to support this as the majority of cyber attacks are not targeted at specific companies. The majority of cyber attacks are typically commodity attacks that seek to exploit known vulnerabilities – which the three actions in the pledge can help companies combat. Signing the pledge does not mean that an organisation is not already doing some/all of the actions and it should not be viewed as a public declaration that an organisation has not taken the prescribed steps.
Our company works in the defence sector and supplies MoD. Is the pledge a suitable substitute for Defence Cyber Certification (DCC)?	No. The Pledge should not act as a substitute for the Defence Cyber Certification (DCC). The DCC is an organisation-wide cyber security certification framework for UK defence suppliers. It provides a single, organisation-level, assurance which can be presented in support of UK Defence Procurements (subject to annual attestation and re-certification every three years). We recommend you speak to your contact at the MOD to discuss the DCC further. More information about you can become certified can be found on IASME's website: Defence Cyber Certification - Defence Cyber Certification

Annex A – Pre-drafted pledge declaration

Government Cyber Resilience Pledge

Following the government's ministerial letter of October 13, [organisation name] hereby pledge to undertake the following actions, as outlined in the letter:

1. **Make cyber a Board responsibility:**
    a. Implement all actions within the Cyber Governance Code of Practice.
    b. Ensure all board members undertake the NCSC's Cyber Governance Training within three months and then on an annual basis.
2. **Sign up to Early Warning:**
    a. Register for the Early Warning service within one month of signing the pledge
3. **Require Cyber Essentials across supply chains:**
    a. Register to the Cyber Essentials Supplier Check Tool within two months of signing the pledge.
    b. Ensure that a comprehensive audit of Cyber Essentials coverage has been conducted across our entire supply chain and that it is presented to and discussed by the Board.
    c. Take a risk-based approach to requiring Cyber Essentials across our supply chain (which may include requiring it from all suppliers). If Cyber Essentials is not required for certain suppliers, the board will ensure that this decision aligns with our organisations risk appetite and strategy and that adequate assurance is obtained through other means.

In addition to the above three actions, we commit to take the following steps:

- **Encourage these actions within our own supply chains** - we will strive to engage with our suppliers to understand and better manage the cyber security risks that they are exposed to through their supply chain and encourage adoption of the above measures.
- **Publish the signed pledge declaration on our website** - within 2 months, we will publish the signed pledge declaration on our company website. Additionally, we will publish an annual public update, either in our annual report or on our company website, on the steps taken to deliver against the pledge.

While the pledge is voluntary, we commit to take positive and meaningful steps to fully implement the three actions. If our company has been unable to implement any of the pledge actions, we will promptly provide DSIT with relevant feedback as to why.

Signed, [Chair/CEO name]