HM Government

70 Whitehall, London SW1A 2AS

13 October 2025

Dear CEO / Chair,

Making cyber security a board responsibility

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. There is a direct and active threat to our economic and national security which requires an urgent collective response.

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. We ask you and the CEOs and chairs of other leading UK companies to take the necessary steps to protect your business and our wider economy from cyber attacks. Cyber resilience is a critical enabler of economic growth, so getting this right will promote growth and foster a stable environment for investment and innovation.

Recent high-profile cyber incidents show how attacks can seriously disrupt operations and damage profitability. In this increasingly hostile landscape, organisations recover better from incidents when they have planned for the worst and rehearsed their business continuity and recovery.

Against this backdrop we write with three specific requests which will have an immediate positive impact on your resilience to cyber attacks:

1. Make cyber risk a Board-level priority using the Cyber Governance Code of Practice

Effective governance of cyber risk is fundamental to business resilience. Executive and non-executive directors should prioritise this and ensure it is considered in strategic decision-making.

The government's Cyber Governance Code of Practice, developed with industry leaders, sets out critical actions Boards and directors should take to govern cyber risk effectively. We urge you and your Board to use this Code to ensure your organisation is sufficiently protected. The Code is supported by free training, which we encourage all Board members to complete to strengthen their oversight.

Not all cyber attacks can be prevented. A critical part of good governance is rehearsing how you would respond to a major incident. Please plan and exercise how you would continue operations and rebuild following a destructive cyber incident.

2. Sign up to the NCSC's Early Warning service

Early Warning is a free service from the government's National Cyber Security Centre which informs your organisation of potential cyber attacks on your network, which can give you invaluable time to detect and stop a cyber incident before it escalates. We strongly advise you and your suppliers to register for this free and simple service.

3. Require Cyber Essentials in your supply chain

Supply chain cyber attacks are increasing, yet just 14% of UK businesses assess the cyber risks posed by their immediate suppliers.

Cyber Essentials is a highly effective government-backed scheme which certifies that organisations have key cyber protections in place to prevent common cyber attacks. It is the minimum cyber security standard businesses should seek to obtain. Organisations with Cyber Essentials are 92% less likely to make a claim on their cyber insurance.

The government already requires most of its suppliers to meet Cyber Essentials standards. As leaders of the nation's largest businesses, we ask you to embed the same requirements across your own supply chain. You should also implement the Cyber Essentials technical controls on your own systems, as part of your organisation's overall strategic approach to managing cyber risk.

Time to Act

Strengthening our nation's cyber resilience requires close collaboration between government and industry. Our forthcoming Cyber Security and Resilience Bill will increase protections for essential and digital services. Whether or not your business is in scope, the NCSC's Cyber Assessment Framework (CAF) can also be used to improve cyber resilience for your most critical services. The three actions described above remain essential and can help achieve outcomes in the framework. The three actions are based on learnings from previous attacks.

We are encouraged to see that more than 90% of company boards now recognise cyber security as a critical priority. We now need to convert this priority into concrete actions to fully address vulnerabilities and enhance resilience, and invite you to work with us to protect our economy and society. In the coming months we will host events to build this partnership and gather industry insight. Your involvement will ensure we can drive the much-needed improvements in our nation's resilience.

To join us in this collective endeavour, please confirm receipt of this letter to [redacted] and share the senior contact we should communicate with on this issue.

With sincere thanks,

Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and Technology

Rt Hon Rachel Reeves MP
Chancellor of the Exchequer

Rt Hon Peter Kyle MP
Secretary of State for Business and Trade

Dan Jarvis MBE MP
Minister for Security

Dr Richard Horne
CEO, National Cyber Security Centre

Graeme Biggar CBE
Director General, National Crime Agency