

MINISTER URGES BUSINESSES TO TAKE CYBER SECURITY SERIOUSLY

Act now to protect your business from one of the UK's fastest-growing threats

Security Minister Dan Jarvis has called on business leaders to take immediate action to strengthen their cyber resilience, warning that cybercrime remains one of the most significant threats to the UK economy.

Speaking at the launch of the National Cyber Security Centre's (NCSC) 2025 Annual Review, Jarvis stressed that cyber security is no longer just a technical issue — it is now a board-level responsibility.

The Growing Threat

The scale of the challenge continues to rise. Over the past year, the NCSC handled more than 200 major cyber incidents — more than twice as many as the year before. These incidents have the potential to disrupt essential services, inflict serious financial losses, and even endanger national security. High-profile organisations such as Marks & Spencer, The Co-op, and Jaguar Land Rover have all faced cyber-attacks this year, but Jarvis emphasised that businesses of every size are at risk.

Support for Businesses

The NCSC has expanded the tools and services available to help organisations protect themselves:

- Cyber Action Toolkit – A practical starting point for sole traders and small firms looking to secure their systems and data.
- Cyber Essentials Certification – A recognised accreditation that demonstrates protection against common online threats. For smaller organisations (under £20 million turnover), certification includes automatic cyber liability insurance.
- Early Warning Service – Used by more than 13,000 organisations, this service alerts businesses to potential cyber-attacks, giving them crucial time to respond.
- Takedown Service – Has removed over 1.2 million phishing campaigns, with half taken down within an hour of detection.



MINISTER URGES BUSINESSES TO TAKE CYBER SECURITY SERIOUSLY

Why It Matters

Many organisations still treat cyber security as a secondary issue until they experience an attack. Jarvis urged a shift in mindset, warning:

“It’s not a case of if you will be the victim of a cyber-attack, it’s about being prepared for when it does happen.”

Beyond the immediate financial impact, cyber incidents can cause long-term reputational damage. Increasingly, customers, suppliers, and investors expect the businesses they work with to demonstrate strong cyber defences.

A Board-Level Priority

The government has written to the CEOs of all FTSE 100 and FTSE 250 companies — and other leading UK firms — urging them to make cyber risk a board-level issue and to sign up to the NCSC’s Early Warning Service.

The letter also encourages these companies to require Cyber Essentials certification within their supply chains, reflecting the growing threat from supplier-based cyber-attacks. Currently, only 14 % of UK businesses assess the cyber risks posed by their direct suppliers.

Taking Action

If your business has not reviewed its cyber protections recently, now is the time to act:

1. Start with the basics – Visit the NCSC website and use the Cyber Action Toolkit to identify practical steps.
2. Consider Cyber Essentials certification – As more organisations adopt it, your customers may begin to expect it. You may also want to require it from your suppliers.

The Minister’s message is clear: act now, not later. Cyber security is not just an IT concern — it’s essential to protecting your livelihood, your team, and your reputation.

Contact us for more information