The AI shift in cyber risk: why leaders must act now

Five Eyes cyber security agencies urge organisations to act on rapidly transforming cyber risk.

As the leaders of the Five Eyes cyber security agencies, we are united in our call to action: the evolving landscape of artificial intelligence (AI) is rapidly transforming cyber risk, and we must act swiftly to remain ahead.

A call to action

While AI will help us improve cyber defence over time, it also accelerates the speed, scale, and sophistication of cyber threats.

Frontier AI models are anticipated to exceed current industry expectations, fundamentally transforming both offensive and defensive cyber capabilities. The timeline is not years, it is months.

In this environment, cyber resilience is integral to advancing business continuity, market confidence, and long-term value. We urge leaders to:

- understand and assess risk, readiness and accountability
- prioritise foundational cyber security practices and controls
- empower cyber leaders with authority and resources
- stay actively engaged as threats and guidance evolve

Success will come from getting the basics right, acting quickly, and integrating cyber security into core business strategy. Those that do not will face growing operational and strategic disadvantage.

The urgency is clear

AI is not a future consideration – it is already here.

It lowers barriers for malicious actors and increases the speed and complexity of attacks, shrinking the window between vulnerability discovery and exploitation ever more quickly. At the same time, AI offers powerful tools to strengthen defence.

A whole-of-organisation and whole-of-society response is required

Cyber risk can no longer be treated as a purely technical issue. This is a core business risk and leadership responsibility. Boards and executives should ensure cyber resilience is in place and works under pressure. It is not enough to have controls. Leaders must be confident those controls will perform during a real incident. This requires reassessing long-standing trade-offs and using AI deliberately to strengthen defence – not just improve efficiency.

Key Actions for Leaders

Core principles

- Secure-by-design and secure-by-default must become standard practice – not an aspiration.
- Resilience cannot depend on a single solution or technology. Defence in depth remains essential.
- As AI systems evolve, new and previously unknown vulnerabilities will emerge, including zero-day vulnerabilities.

Breaches will occur. Preparedness helps you contain them quickly and prevent escalation into major operational and financial crises.

Practical actions

These actions are not new, but are now urgent to reduce not only technical risk, but also operational, financial and reputational exposure:

1. **Reduce your attack surface:**
   Limit unnecessary system access and external connectivity. Challenge whether systems need to be exposed at all and isolate those that do not.
2. **Accelerate patching processes:**
   AI is shortening the time between vulnerability discovery and exploitation. Delays in patching increase risk, especially for operational systems with long update cycles. Prioritise security updates accordingly to manage risks.
3. **Address legacy systems:**
   Unsupported systems are easy targets. They are not just technical debt, they are strategic liabilities.
4. **Review and strengthen identity and access controls:**
   Limit who can access critical systems. Enforce strong authentication and regularly review permissions.
5. **Prepare for incidents before they happen:**
   Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery.

Use AI to strengthen defence

Adversaries are already using AI to move faster and more effectively. Defenders must do the same.

Organisations that integrate AI tools into their security operations can detect vulnerabilities earlier, improve software quality, monitor unusual behaviour, and respond faster to incidents – reducing both the cost and impact of incidents.

Success will not come from having the most tools. It will come from getting the basics right, acting quickly, and integrating cyber security into core business strategy.

We must act now

The rapid pace of frontier AI development means cyber risk assumptions can become outdated in months, not years. We must act before and be prepared to adapt and withstand evolving threats.

Cyber resilience is not an IT issue - it is central to operational continuity and market trust. Leaders who act now will reduce exposure, strengthen resilience, and build confidence with customers, partners, and investors. Those who delay will face growing and avoidable risk.

> *Our Five Eyes cyber security partnership is deep and transparent. The way we share cyber threat information is critical to our collective security. In that spirit, we call on leaders across industry – including vendors – to act now and work together to protect our people and secure our future.*
>
> - Stephanie Crowe - Head Australian Cyber Security Centre, **Australian Signals Directorate**
> - Rajiv Gupta - Head Canadian Centre for Cyber Security, **Communications Security Establishment**
> - Catriona Robinson - Head of the National Cyber Security Centre, **Government Communications Security Bureau**
> - Richard Horne - Chief Executive Officer, **National Cyber Security Centre**

- David Imbordino - Director Cyber Security Directorate, **National Security Agency**
- Nick Andersen - Acting Director, **Cybersecurity and Infrastructure Security Agency**

PUBLISHED

22 June 2026

WRITTEN FOR

Cyber security professionals Large organisations Public sector Small & medium sized organisations

NEWS TYPE

Statement