cognizant

# Tech modernisation: **Security in the era of AI**

## Introduction

Enterprise-scale AI is a profound challenge for cybersecurity and is both a powerful new shield and a new adversarial weapon. In the research conducted by Australian IT research and advisory firm ADAPT, we find that 38% of security leaders believe this leads to current cyber strategies becoming ineffective within five years*. In this article we outline how organisations must confront both aspects of this new reality as part of the journey toward harnessing AI's potential and preparing for a new cybersecurity paradigm.

Businesses must learn how AI will support advanced new threat detection automations to augment overburdened teams, and how we must establish new standards and processes to manage the risks of emerging AI-powered threats. With the right approach, security avoids being seen as a blocker to innovation and becomes part of enabling fast and effective innovation throughout the organisation.

**For more insights into the big picture of Australian CIOs and their goals for 2025, read our full guide here.**

## Security for new modes of AI integration and execution

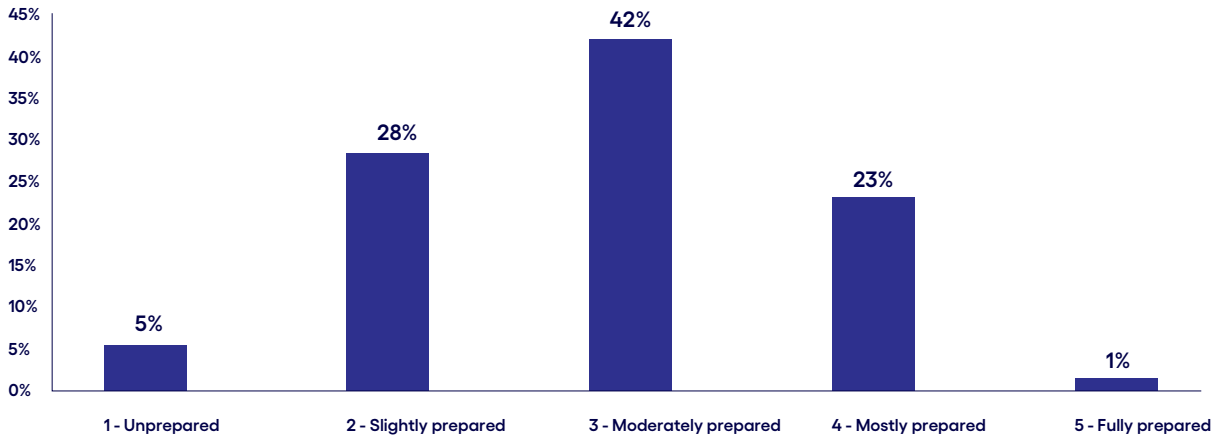
In a world of increasing threats, ensuring adequate security levels aligned to your organisation's risk appetite is a key to delivering sustained business success.

Cybersecurity is crucial for defence against active threats, but also for building trust and confidence for compliance and innovation. While we continuously evolve to strengthen the security posture, adversaries are also evolving at rapid pace to find the weak links across people, processes, and technology to breach our defences.

AI presents opportunity and risk in cybersecurity. It enhances threat detection and response capabilities by automating the analysis of vast amounts of data, identifying patterns, and predicting potential threats with greater accuracy and speed. Yet attackers can exploit AI to develop more sophisticated attacks, such as AI-enhanced phishing and deepfake scams.

Achieving the right risk balance is crucial as AI changes the playing field. Too many restrictions means security becomes a blocker to effective operations, leading to poorer controls and practices when teams try to route around restrictions. The right posture allows organisations to leverage AI's full potential as a security enhancement while safeguarding against its misuse.

### How prepared is your organisation to securely adopt and operationalise AI initiatives in the next 12 months?




**Only 24%** of organisations feel fully or mostly prepared

Source: ADAPT Security Edge Survey in Apr 2025. Sample size: 111 Australian CISOs

Even as AI opportunities enter business planning, and with them new risks, the critical approach to managing the security environment remains focused on getting our fundamentals right.

To build resilience in the AI era, we recommend a layered defence strategy that evolves with emerging threats and enterprise complexity:

### Human-centric security awareness

Move beyond basic training to adaptive, AI-enhanced education that evolves with threat landscapes. Empower users to recognise deepfakes, social engineering, and AI-generated scams.

### AI-augmented threat monitoring and AI Security Posture Management (SPM)

Leverage behaviour-based analytics and contextual intelligence to reduce false positives and accelerate incident response. Real-time visibility is no longer optional—it's foundational. With appropriate industry leading SPM, organisations can manage and mitigate threats and stay compliant.

### Secure by Design with AI in mind

Embed security into system architecture from the ground up, with specific consideration for agentic AI, automated code generation, app security & pen testing, data encryption, secure access and dynamic data flows. Design frameworks must now anticipate autonomous decision-making and evolving access patterns.

## AI for Security

AI offers tremendous opportunities as a security support system, improving our default security systems to reduce risk and enhance our ability to respond to any given situation.

AI can improve the efficacy of our traditional tools as we move away from rules based and signature-based monitoring and into behaviour-based security management. This adaptive approach can detect the most subtle signs of malicious activity across organisation-wide data to identify and mitigate attacks. This proactive capability greatly reduces the time to resolution compared with manual intervention.

We now deploy the SOUL tool to turn security playbooks into AI orchestrated automations that include end-to-end audit trails. We have seen typical cycles from threat detection to active response reduce from 8-16 hours down to 15-30 minutes through these automations.

## False positive management

With thousands of alerts coming into security dashboards at false positive rates commonly around 60-70% it becomes the norm for alerts to be errors, making it easy for real incidents to slip past our human teams. By contextualising alerts with threat intelligence and insights drawn from real-time assessments of the network, we can now reduce false positives to below 10% and bring the focus onto real problems that need attention.

## AI dashboards and analytics

A typical enterprise will have dozens of security controls across a range of tools and services. Getting a view of the full security posture requires many reports and integrations to see the full picture.  At Cognizant, our innovative Neuro® Cybersecurity platform integrates and orchestrates diverse security tools, delivering a unified user experience for CISOs, CIOs, risk management teams, vulnerability management teams, and security analysts. By leveraging AI models of the client's choice, Cognizant Neuro Cybersecurity enables use cases across risk & compliance, threat and vulnerability management, infrastructure and network security policy Enforcement, and identity & access management (IAM) for application and account onboarding. This empowers organisations to mitigate risks effectively and strengthen their overall security posture.

## Security skills shortages

With cybersecurity skills in limited supply, access to security expertise remains a key concern for organisations. AI can help to reduce dependency on human workloads by automating routine tasks and providing actionable insights.

## Enhance user awareness training

Unsophisticated attackers now have access to tools that make it a breeze to create deepfakes and to exploit business users in a highly targeted fashion. But we can use AI to improve how we educate users and engage them in security literacy. Smarter, more engaging training will keep every user in the best possible mindset for avoiding the most common risks to our business environment.

## Security for AI

With AI heading toward a new embedded normal throughout business IT systems, we must incorporate the new risks of AI into our security frameworks. This means data governance must be updated to accommodate new privacy and compliance norms if we allow data to flow into AI systems.

When updating security policies for AI, we recommend key considerations should be:

- Which AI is allowed?
- Who owns the AI?
- Who owns the data?
- What types of data are acceptable?

We discussed the need for better data governance models and personas above. Bringing AI into persona designs alongside robust data classification is now more important, helping define layers of data security control for different uses around the business and in different AI services and platforms. For example, Personally Identifiable Information (PII) must be treated very differently than knowledge bases or general document libraries.

### Maturity in data classification for secure data policy

**32%** of organisations rate themselves as immature

Adapt Security Edge Survey April 2025

AI governance is becoming a cohort decision amongst the CIO, CISO, and data privacy officers, underpinning the future of security, integration, and wider business governance. Collective leadership must ensure that the drive for higher velocity through AI maintains a focus on the security requirements alongside the business requirements.

Automated code could be attacked with malware injection that gets deployed in your enterprise or custom LLMs could be poisoned in data attacks. This increases the emphasis on maintaining automated scanning and verification to mitigate such a risk.

## Leveraging AI for cybersecurity

Using our custom Neuro® Cybersecurity Platform, Cognizant is enabling real-time risk mitigation at enterprise-wide scale through an easy to consume user interface. By unifying the security management platform we overcome siloed operations to reduce risk exposure and enhance threat detection and response capability. The platform also helps to classify and protect sensitive data to further enhance confidentiality and data integrity, as well as strengthen identity and access management to improve confidence in control over critical systems.

**Cognizant Neuro® Cybersecurity Platform deliver an all-encompassing, adaptable, and scalable solution, empowering organization to strengthen cyber resilience and manage risks effectively**

### Cognizant Neuro® Cybersecurity Platform

Enhancing AI-Driven Automation:

- Investing in AI to streamline security tasks, reduce manual effort, and accelerate response times.

Advanced Threat Detection and Response:

- Enhances threat intelligence and incident response.
- Ensuring effective threat mitigation.

Integration with OEM AI Solutions:

- Expands integration with various OEM AI solutions.
- Streamlining incident response and fortifying defenses.

Unified Security Management:

- Integrates multiple security system outputs into one platform.
- Providing a holistic view of threats, vulnerabilities, and risks.

Scalability and Flexibility:

- Seamlessly grows and adapts with organizations.
- Handling increasing data volumes and evolving security needs.

Customer-Specific Deployment and Data:

- Tailored deployment and data management solutions.

## Secure by Design in the Agentic AI era

A Secure by Design approach to the enterprise puts accountability across the organisation and not simply upon the security team. This is integrated into our modern engineering frameworks and templates, considering the security requirements at the system design stage across authentication, authorisation, access control, and data control.

Ensuring that default access is only as deep as required is crucial, particularly as more code is written by AI and agentic AI enters our technology environment. Agentic AI requires seamless integration across applications, data, and decision-making systems. This may require new forms of access to applications and data platforms, asking security controls to allow for agentic activity which can potentially look like a security risk.

It is critical to understand at each layer what the agentic AI is going to do and who owns the outcomes. Understanding how agentic AI integrates into different systems becomes part of security controls and frameworks for security by design. And just as shadow IT introduces risks to security, so too will shadow AI as it trends toward agentic AI capabilities that mimic human usage of digital systems.

## Bringing AI empowered security to life

There is no standard solution that prepares security teams and technologies for the AI era. Identifying how existing systems need to evolve to take advantage of AI, and prepare for its challenges, is critical to finding the right security approach for each enterprise. At Cognizant, we propose the starting point is to begin investigating the security status quo for an enterprise and how to identify readiness for the opportunities and issues ahead.

With Cognizant Neuro® AI tools, we work with CISOs and CIOs to explore options in real-time that bring the art of the possible to life. We can demonstrate how AI can be applied to your security environment to alleviate pressures on your cybersecurity processes and improve detection and analysis capabilities.

Along with offering external credibility, our strategic support can help you achieve a desired security posture without locking you into any ongoing commitments. And we can offer outcome based commercial models that are zero risk to your organisation.

To learn more how Cognizant can help you strengthen security design in the era of AI:

Email: contact_au@cognizant.com

www.cognizant.com/au/en/cmp/technology-modernisation-security-in-the-era-of-ai



**World Headquarters**
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

**European Headquarters**
280 Bishopsgate
London
EC2M 4RB
Phone: +44 207 297 7600

**India Operations Headquarters**
5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

**APAC Headquarters**
1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Phone: +65 6812 4000



WF 3696162