

Securing Against AI and Quantum Threats – Building Our Cyber Safe Culture - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/securing-against-ai-and-quantum-threats-building-our-cyber-safe-culture>

Details:

Originally published on 24 October 2025, this article explores the changing digital threat landscape. Artificial Intelligence (AI) and the looming quantum era are reshaping how organisations must approach cybersecurity. As Cyber Security Awareness Month (CSAM) spotlights the importance of “building our cyber safe culture,” this article examines how business leaders—especially Chief Information Security Officers (CISOs)—can drive future-ready, people-centric security in the face of sophisticated new risks.

The Rise of AI-Powered Attacks

AI is starting to revolutionise productivity and efficiency, but it has also made cyber threats smarter and more scalable. Attackers now leverage AI to rapidly craft highly convincing phishing schemes, exploit vulnerabilities at machine speed, and automate fraud. Our original article highlighted CISO concern about AI-assisted social engineering. Assess that risk against your organisation's exposure and incident evidence. The result: security teams find themselves in a constant race against increasingly creative adversaries.

Cultural Habits for AI Resilience

Cyber safety in the AI era is not just about deploying smarter tools—it's about everyday behaviours. Training executive teams on AI governance and helping staff apply clear policies can strengthen resilience across the organisation. Combine appropriately evaluated defensive technologies and threat intelligence with cyber awareness training, clear responsibilities and tested response procedures.

Quantum Computing: The Emergent Disruptor

A sufficiently powerful quantum computer could threaten public-key cryptography such as RSA and ECC. The timing of that capability remains uncertain; preparation should account for both migration time and how long information must remain confidential. Threat actors may already be “harvesting” encrypted data for decryption when quantum computers go mainstream, exposing sensitive information in the future.

Quantum-Ready Security Posture

Proactive CISOs are mapping cryptographic assets and initiating transition plans to quantum-safe algorithms, in accordance with new standards released in 2024. Crypto-agility—rapidly updating cryptographic protocols as risks evolve—is emerging as a critical practice. Key and certificate lifecycle management can support crypto-agility, but rotation alone does not make a quantum-vulnerable algorithm quantum-resistant. However, upgrading technology alone is insufficient: organisations must cultivate a culture of continual learning, vigilance, and adaptability, ensuring all staff understand why

tomorrow's risks matter today.

Reinforcing Cyber Safe Culture: Practical Actions

As CSAM reminds us, future-proofing security starts with culture. Every leader and staff member is responsible for adopting strong security habits and staying vigilant against emerging threats. To align resilient habits with modern risks, organisations should: Regularly review and catalogue critical cryptographic systems and asset inventories. Encourage ongoing reporting of potential threats and run exercises exploring AI-driven attacks and quantum scenarios. Host panel discussions or Q&A sessions with CISOs about tackling new threat vectors and making security a shared responsibility. Motivate teams by sharing real-world stories of how strong habits and preparation have prevented incidents.

Conclusion

AI and quantum technology introduce continual, complex risks, but building a “cyber safe culture” rooted in resilient habits can improve organisations’ preparedness. Proactive leadership, employee empowerment, and strategic investments provide the foundation for defending against both today’s automated threats and tomorrow’s quantum challenges. With every individual playing a part, security becomes a living, evolving aspect of business success.

Sources:

ACSC Cyber Security Awareness Month – Cyber Security Awareness Month 2025
Quantum Threats Are Closer Than You Think: How Businesses Can Prepare for the Future

Two different planning horizons

AI-assisted social engineering and quantum cryptographic risk call for related but distinct preparations.

Planning question	AI-assisted social engineering	Quantum cryptographic risk
Risk to assess	Convincing fraudulent messages and impersonation attempts.	Future attacks on vulnerable public-key cryptography, including encrypted data collected today.
Evidence to examine	Your incident reports, simulation results and verification processes.	Your cryptographic inventory, data confidentiality requirements and supplier migration plans.
Practical next steps	Test payment and access verification, staff reporting and response procedures.	Plan and test migration to suitable post-quantum standards.

Prioritise both workstreams using your own exposure, dependencies and delivery times. There is no universal budget sequence that suits every organisation.

AI and social engineering: practical checks

The original article highlights the risk of more convincing phishing and impersonation. Use that concern to test concrete controls:

Language quality: Do staff verify consequential requests even when the writing is fluent and free of errors?

Personalisation: Could public information about projects, suppliers or staff make a fraudulent request more believable?

Language and localisation: Do verification procedures apply equally to messages that use familiar local terminology?

Voice and video: Is an apparent familiar voice or face supported by an independent check?

For payments, bank-detail changes, credential resets and privileged access, consider an independently initiated verification channel using established contact details. Test that procedure alongside access controls and escalation arrangements; no single check guarantees that fraud will be prevented.

Evaluating defensive technology

Our Managed Detection and Response material describes EDR, ITDR, SIEM and threat intelligence. That service description does not establish which machine-learning models are deployed in every customer environment. Confirm the selected products, detection coverage, configuration, human oversight and response responsibilities in the proposed service scope.

Harvest now, decrypt later

NIST's first three finalised post-quantum standards were published in August 2024: FIPS 203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA) for digital signatures and FIPS 205 (SLH-DSA) for hash-based digital signatures. See NIST's post-quantum cryptography project .

NIST explains that encrypted information can be collected now and retained for possible future decryption. Its value depends on the information and required confidentiality period; a recorded network session can contain long-lived secrets too. Consider health, legal, identity, government and intellectual-property information according to its actual sensitivity and retention requirements.

Assess confidentiality duration alongside migration time, supplier dependencies and the uncertain timing of a cryptographically relevant quantum computer. A two-year confidentiality period is not a universal exemption from planning.

Crypto-agility means being able to replace cryptographic mechanisms as requirements change. Inventory algorithms, certificates, protocols and dependencies, then test suitable migration options for compatibility and performance. Key rotation is part of lifecycle management, not a substitute for changing a vulnerable algorithm.

Against AI-enabled social engineering

Human Risk Management , published as powered by Mimecast, with four components on a prevent, detect, respond and reduce lifecycle: awareness training, phishing simulation, per-user risk scoring and targeted remediation.

Use simulations and risk reporting to examine behaviour alongside training completion. Agree the measures, baseline and follow-up actions for your organisation, including staff who handle payments, bank-detail changes or privileged access.

Managed Detection and Response , combining EDR, ITDR, SIEM and threat intelligence, operating 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike.

Identity-focused detection can help investigate suspicious account activity; coverage and response depend on the deployed controls, telemetry and agreed scope.

Our MDR material includes an illustrative compromised Microsoft 365 account scenario involving a rogue OAuth application. It is an example of account abuse, not a claim about the usual outcome of every phishing attack.

Exposure Management provides visibility into potential exposures. Discuss whether the proposed scope covers the external assets and information relevant to your threat assessment, and how findings will be prioritised and acted on.

Against the quantum transition

Vulnerability Management can support assessment of existing weaknesses. Confirm any cryptographic discovery or post-quantum migration work separately; the service name alone does not establish that scope.

Framework position

We publish alignment with Essential Eight Maturity Level 3, the highest of the three levels, ISO/IEC 27001, APRA CPS 234, the NIST Cybersecurity Framework, the Australian Privacy Principles, GDPR where applicable, and SOC 2 Type II. It holds ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in the provision and management of our emPOWER Infrastructure and managed service offerings.

An Essential Eight maturity assessment should not be used as proof that a system has completed a post-quantum migration. Assess cryptographic readiness against the relevant algorithms, protocols and migration requirements, including NIST's standards.

For social-engineering risks, discuss appropriate authentication, application control, user application hardening and administrative access restrictions alongside staff verification procedures.

Our emPOWER Cloud material describes Australian data residency capabilities. Confirm the locations and handling of your data in the agreed service scope. Residency alone does not establish protection against interception or future decryption; assess access controls, data flows and cryptographic protection separately.

Agreeing scope and responsibilities

Confirm containment authority, incident escalation and service availability arrangements in your applicable agreement and response plan. A general right to suspend services should not be treated as a promise that a particular account or endpoint will be isolated during an incident.

Before selecting services, ask us to confirm:

The scope and availability of cryptographic inventory and post-quantum migration assistance, including supplier dependencies.

Applicable AI-use policies and whether customer data will be processed by AI systems.

Detection, triage and response measures, reporting and any contractual service levels.

The phishing-simulation baseline, agreed targets and remediation process.

Supported MFA methods and their suitability for the relevant threat scenarios.

Any vCISO Advisory, Vulnerability Management, Incident Response Retainer and Human Risk Management inclusions in the Service Order.

Quoted pricing, assumptions and exclusions for the selected services.

These are scoping questions; this article does not establish that the capabilities, policies or commercial terms are unavailable.

How can AI-assisted social engineering affect cyber security?

Our October 2025 article highlights the risk of convincing phishing and impersonation. Assess your organisation's exposure through incident evidence, staff reporting and tested verification procedures for payments, bank-detail changes and access requests.

Why is quantum computing considered a major emerging cybersecurity risk?

A sufficiently powerful quantum computer could threaten public-key cryptography such as RSA and ECC, but the timing remains uncertain. Encrypted information collected today may retain value for future decryption, so planning should consider confidentiality requirements and migration time.

What steps are proactive CISOs taking to prepare for the quantum era?

Inventory cryptographic assets and dependencies, assess confidentiality requirements, and plan and test migration to suitable post-quantum standards. NIST published FIPS 203, 204 and 205 in August 2024. Key and certificate rotation can support lifecycle management, but does not itself make a vulnerable algorithm quantum-resistant.

What sources does the blueAPACHE article cite?

The original article cites the ACSC Cyber Security Awareness Month 2025 page and Cybernetic Global Intelligence's article on quantum threats. The expanded guidance also links to NIST's post-quantum cryptography project and its explanation of harvest-now, decrypt-later risk.

What is the historical context of the 82% human-element figure?

Proofpoint's 31 May 2022 summary of Verizon's 2022 Data Breach Investigations Report states that 82% of breaches involved a human element. This is a historical report finding, not a current universal rate or a claim that 82% of breaches began with human behaviour. Source: <https://www.proofpoint.com/us/blog/email-and-cloud-threats/key-findings-2022-verizon-data-breach-investigations-report-dbir>