

Human Risk Management: The Human Firewall - blueAPACHE

Canonical: <https://www.blueapache.com/blog/human-risk-management-the-human-firewall>

Details:

Summary

This blog post, "Human Risk Management: The Human Firewall", is a blueAPACHE article from 2025 covering security. As Cyber Security Awareness Month continues, blueAPACHE is proud to support the Australian Cyber Security Centre's (ACSC) national initiative. Each week highlights a critical theme aligned to the official CSAM campaign – and this week, the focus is on the most unpredictable element in cybersecurity: people . It is written for readers evaluating emPOWER Security, Human Risk Management. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2025
Topic	Human Risk Management: The Human Firewall
Services referenced	emPOWER Security, Human Risk Management, Governance, Risk and Compliance
Named products or vendors	None named beyond blueAPACHE

Article

As Cyber Security Awareness Month continues, blueAPACHE is proud to support the Australian Cyber Security Centre's (ACSC) national initiative. Each week highlights a critical theme aligned to the official CSAM campaign – and this week, the focus is on the most unpredictable element in cybersecurity: people .

Human Risk: Why It Matters

People remain the pivotal factor in cyber risk. Despite advances in automation and AI-driven defenses, phishing, social engineering, and identity compromise remain the top attack vectors. KnowBe4's 2025 Phishing Benchmarking Report reveals that organisations in Australia and New Zealand record a baseline phish-prone percentage (PPP) of 36.8% – one of the highest globally. This means over a third of employees are likely to click on deceptive content before training even begins. For large enterprises (1,000+ employees), the risk is even greater, with human error now implicated in the majority of reported breaches. Effective risk management, therefore, must integrate human risk metrics into every layer of cyber defense – alongside continuous monitoring across both local and cloud environments.

The Power of Training: Turning Weakness into Strength

The positive side of the story is that training works. After 90 days of Security Awareness Training (SAT), the average organisation's PPP drops by nearly 20%, and after a year, this can fall to single digits, according to KnowBe4. In sectors such as banking, long-term programs have delivered over 90% improvement in phishing resilience, proving that informed employees can shift from being the largest risk to an indispensable line of defense.

Today's Threats: AI, Deepfakes, and Critical Infrastructure

Cybercriminals no longer rely solely on traditional phishing. In 2025, AI-enhanced phishing, QR-code scams, and voice/video deepfakes have rapidly escalated. Critical infrastructure sectors – energy, water, and transport – are increasingly being targeted, prompting legislative measures such as the Cyber Security Act 2024, which mandates ransomware reporting and sets cybersecurity standards for smart devices. In this new environment, rapid, adaptive training and secure reporting channels are no longer optional; they're essential for compliance and resilience.

Making the Human Firewall Measurable

To truly embed human risk management, organisations should:

Encourage instinctive reporting: Provide one-click phishing-report buttons, require 15-minute escalation for payment or payroll change approvals, and track report volume and SLA adherence.

Verify transactions in layers: Use out-of-band callbacks, dual-approval workflows, and "hold-to-verify" checks for financial or identity-related requests.

Enforce strong access controls: Deploy multi-factor authentication (MFA) across all administrative functions, finance, and SaaS logins, prioritising phishing-resistant methods (FIDO2, passkeys) and monitor for fatigue or bypass attempts.

Train with realism: Use short, frequent micro-simulations, region-specific case studies, and tailored onboarding training to maintain engagement year-round.

Compliance and Culture

Frameworks like ISO 27001 and the ACSC Essential Eight maturity model provide a strong foundation, but security culture goes beyond compliance. Comply to Essential Eight areas that emphasise faster patching, phishing-resistant MFA, and restricted admin privileges, underscoring the importance of continuous improvement. Cybersecurity is not a seasonal campaign – it's a daily practice of awareness, measurement, and accountability.

blueAPACHE x KnowBe4: Your Partner in Human Risk Management

blueAPACHE partners with KnowBe4, a global leader trusted by more than 70,000 organisations, to deliver a unified Human Risk Management solution. KnowBe4's AI-driven platform integrates behaviour-based awareness training, real-time coaching, and measurable benchmarking, empowering Australian and New Zealand businesses to turn their people from the largest attack surface into their strongest security asset.

Call to Action

Kick off your Human Risk Uplift Program with blueAPACHE. Leverage real metrics to baseline your workforce, implement phishing-resistant MFA, and apply staged verification playbooks to reinforce

cyber awareness across all teams. Together, let's strengthen the human firewall – and build a cyber safe culture that endures well beyond October.

Sources:

KnowBe4 Phishing Benchmarking Report 2025

ACSC Cyber Security Awareness Month – Cyber Security Awareness Month 2025

ACSC Essential Eight Maturity Model – Essential Eight maturity model | Cyber.gov.au

Cyber Security Act 2024 – Cyber Security Act 2024 – Federal Register of Legislation

Related

emPOWER Security

emPOWER Security (pillar hub)

Human Risk Management

Governance, Risk and Compliance

blueAPACHE Security (case study)

Frequently asked questions

What baseline phish-prone percentage does the KnowBe4 2025 Phishing Benchmarking Report cite for organisations in Australia and New Zealand?

36.8%, described as one of the highest globally, meaning over a third of employees are likely to click on deceptive content before training even begins.

By how much does the article say Security Awareness Training reduces phish-prone percentage after 90 days, according to KnowBe4?

Nearly 20%, and after a year this can fall to single digits, according to KnowBe4 data cited in the article.

What improvement in phishing resilience does the article cite for long-term banking sector training programs?

Over 90% improvement in phishing resilience, per the article's discussion of long-term Security Awareness Training programs in banking.

What four measures does the article recommend to make the "human firewall" measurable?

Encouraging instinctive reporting (one-click phishing-report buttons, 15-minute escalation for payment changes), verifying transactions in layers (out-of-band callbacks, dual-approval workflows), enforcing strong access controls (MFA prioritising FIDO2 and passkeys), and training with realism (short, frequent micro-simulations).

What legislation does the article cite as mandating ransomware reporting and smart device security standards?

The Cyber Security Act 2024, referenced in the context of AI-enhanced phishing, deepfakes, and critical infrastructure threats emerging in 2025.

Which vendor does blueAPACHE partner with for Human Risk Management, according to this article, and how many organisations trust it?

KnowBe4, described as a global leader trusted by more than 70,000 organisations, delivering a unified Human Risk Management solution with blueAPACHE.

What emerging threat types does the article say cybercriminals were using beyond traditional phishing in 2025?

AI-enhanced phishing, QR-code scams, and voice/video deepfakes, with critical infrastructure sectors like energy, water and transport increasingly targeted.

What two frameworks does the article cite as providing a foundation for security culture beyond compliance?

ISO 27001 and the ACSC Essential Eight maturity model, with the article noting Essential Eight areas emphasise faster patching, phishing-resistant MFA, and restricted admin privileges.

Source

origin post (2025)

Knowledge Base

What is the phish-prone percentage (PPP) for organisations in Australia and New Zealand, according to KnowBe4's 2025 report?

According to KnowBe4's 2025 Phishing Benchmarking Report, organisations in Australia and New Zealand record a baseline phish-prone percentage of 36.8%, one of the highest globally, meaning over a third of employees are likely to click on deceptive content before training even begins.

How effective is Security Awareness Training (SAT) at reducing phishing risk, ?

After 90 days of Security Awareness Training, the average organisation's phish-prone percentage drops by nearly 20%, and after a year, it can fall to single digits, according to KnowBe4. In sectors like banking, long-term programs have delivered over 90% improvement in phishing resilience.

What legislation is mentioned in relation to critical infrastructure cybersecurity?

The article references the Cyber Security Act 2024, which mandates ransomware reporting and sets cybersecurity standards for smart devices, in response to increased targeting of critical infrastructure sectors.

What four practices do you recommend for making the 'human firewall' measurable?

We recommend: (1) encouraging instinctive reporting via one-click phishing-report buttons and 15-minute escalation for payment/payroll approvals; (2) verifying transactions in layers using out-of-band callbacks, dual-approval workflows, and hold-to-verify checks; (3) enforcing strong access controls including MFA prioritising phishing-resistant methods like FIDO2 and passkeys; and (4) training with realism through short, frequent micro-simulations and region-specific case studies.

Who is your partner for Human Risk Management, and what does this partnership offer?

We partner with KnowBe4, a global leader trusted by more than 70,000 organisations, to deliver a unified Human Risk Management solution. KnowBe4's AI-driven platform integrates behaviour-based

awareness training, real-time coaching, and measurable benchmarking to help Australian and New Zealand businesses turn their people from the largest attack surface into their strongest security asset.