The cost of uncertainty

Why executives need evidence that their security controls work.

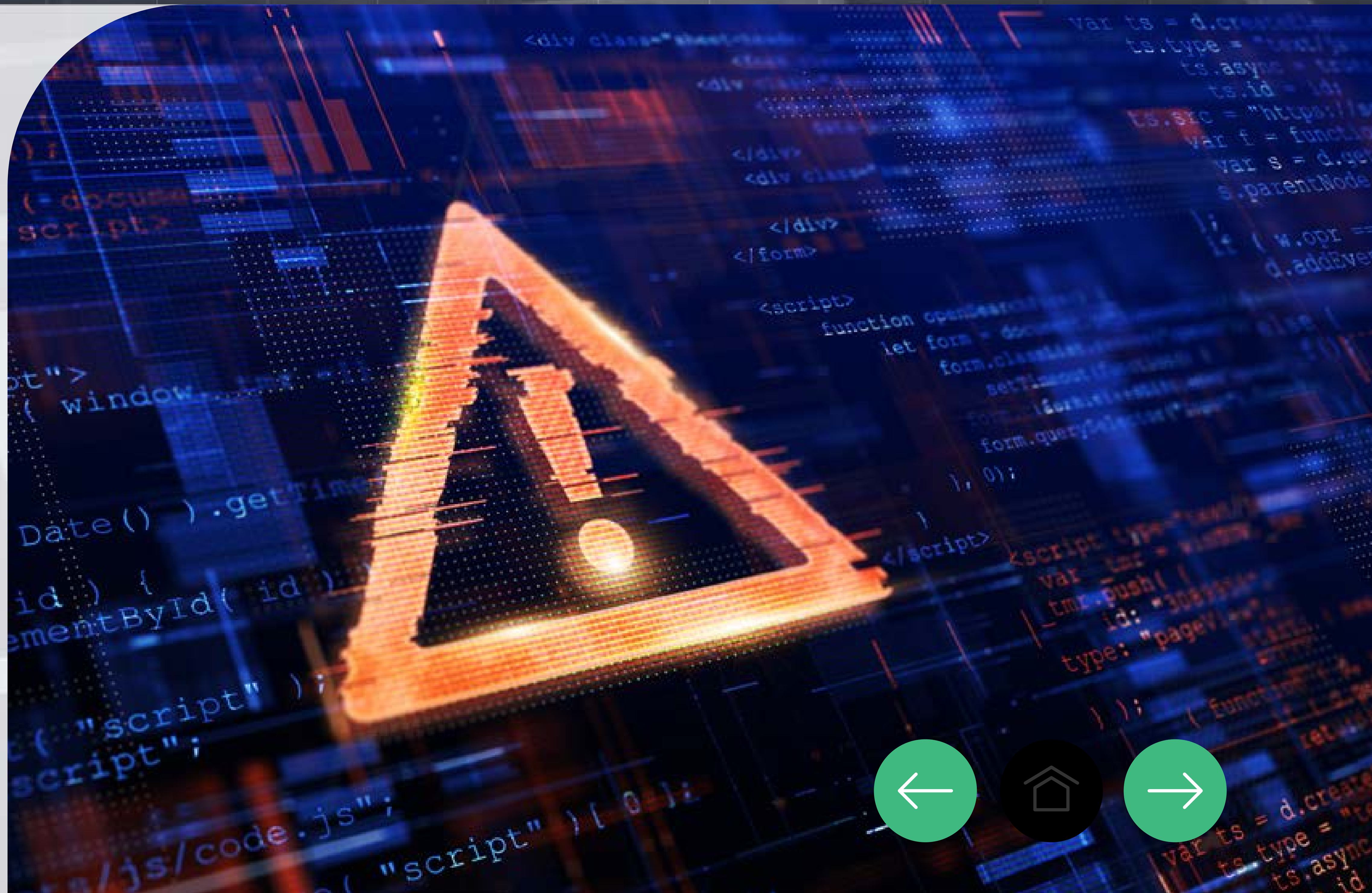
Technology leaders are under increasing pressure to strengthen resilience, manage risk, and justify security investments. Yet many organisations still reply on assumptions about whether their controls will perform when tested by a real attack.

Penetration testing provides independent evidence of where exposure exists, how weaknesses could be exploited, and where remediation should be prioritised. For executives, this shifts security from a technical reporting exercise to a business decision-making tool, helping protect profitability, reduce operational risk, and build confidence in the organisation's security posture.

1 Why cyber risk is now a business performance issue

Every technology investment is ultimately judged by its impact on business performance. Cybersecurity is no longer a standalone technical concern. It directly influences operational continuity, customer trust, regulatory compliance, and profitability.

As organisations rely more on technology for daily operations, the cost of disruption increases. Downtime affects not only IT, but also revenue, productivity, and customer confidence. Boards now recognise this connection, making cyber governance a regular board-level priority.



2 The hidden cost of assumptions

At times, cybersecurity is perceived as a governance issue, not just a technical one. Boards and executive teams expect assurance that risk is being actively managed, not simply that controls exist on paper.

Meanwhile, the environments organisations must secure are constantly evolving. New cloud services, applications, identities, third-party connections, and AI-enabled tools introduce additional risks.

AI adoption is expanding faster than many security models were designed to support. New tools can introduce fresh access paths, data exposure risks, and integration dependencies. Penetration testing helps organisations understand whether these changes have created new weaknesses across identity, applications, data, and connected systems.

A control effective last year may not address exposures created by recent changes. Organisations therefore use security validation activities such as penetration testing, control assessments, and assurance reviews to test whether documented controls remain effective, rather than relying solely on compliance.

While organisations may meet audit and compliance requirements, the challenge is if they can confidently state their controls will perform as expected during a real attack. This distinction is important compliance shows a process exists but does not prove it works in practice.

Threat actors continue to adapt, combining traditional techniques with automation and AI-assisted tools that accelerate reconnaissance and reveal new attack paths. As a result, organisations must assess security controls against both established and current attacker capabilities.

For CIOs, the key question is not whether controls are in place, but whether they reduce meaningful business risk and where remediation efforts should be focused. Assumptions cannot provide this confidence; evidence can.

When security assumptions go untested, organisations risk:

— Investing in controls that do not address the highest-risk exposures, as spending is based on assumptions rather than evidence.

— Entering audits with unidentified risks, only discovering control failures during the process instead of beforehand.

— Identifying gaps only after an incident, resulting in reactive and costly remediation instead of proactive planning.

— Failing to meet regulatory expectations, including SOCI's CIRMP obligations for critical infrastructure and the Privacy Act's civil penalty regime enforced by the OAIC for data-related failures.

— Facing increased scrutiny and costs after an incident, without documented evidence of due diligence for regulators, auditors, or insurers.

3 Why traditional vulnerability reporting falls short

At times, organisations are overwhelmed by securing data, not lacking it. Security teams face large volumes of vulnerabilities and limited resources, making prioritisation the main challenge rather than detection.

Compliance frameworks can help identify required controls, but are less effective at proving those controls withstand modern attacks. Security leaders need more than checklists; they require assurance that controls operate effectively in real-world conditions.

Vulnerability reporting offers a snapshot of known weaknesses, but rarely demonstrates how these could be combined, exploited in practice, or discovered through evolving attacker methods.

Security validation adopts a realistic approach by examining how weaknesses could be identified and exploited, including through AI-assisted tools accessible to both skilled and less sophisticated attackers.

How regular penetration testing strengthens cyber resilience

As organisations adopt new technologies, expand digital services, migrate to cloud environments, and increase third-party connectivity, cyber threats evolve. These changes introduce new vulnerabilities, misconfigurations, and attack paths. Controls effective a year ago may not address risks from recent changes in technology, processes, or attacker behaviour.

Regular penetration testing enables organisations to validate their security posture by assessing control performance against realistic attack scenarios. Modern testing identifies weaknesses arising from combinations of technical flaws, process gaps, user behaviour, or misconfiguration, not just known vulnerabilities.

Penetration testing provides independent evidence of exposures, potential business impacts, and prioritised remediation actions, supporting informed decisions across security, risk, governance, and compliance functions.

Regular assessment also helps organisations:

- Validate whether security controls continue to operate as intended
- Identify emerging risks introduced through technology change
- Support governance, audit, and compliance activities with evidence-based assurance
- Improve prioritisation of remediation activities
- Track improvement in security posture over time

Organisations now use penetration testing as part of an ongoing resilience strategy, rather than as a periodic compliance exercise. This approach helps them adapt to evolving threats and maintain confidence in critical systems and controls.

4 From exposure to action

Penetration testing turns the risks outlined above into a prioritised action plan, supporting audit, regulatory, cyber insurance, and board reporting requirements along the way.

Modern penetration testing should reflect current attacker tactics. Threat actors now combine automation, AI-assisted techniques, public attack frameworks, and traditional methods to find opportunities more quickly and at greater scale. Security validation enables organisations to assess their environment against both conventional and emerging attack methods.

The goal is not just to list vulnerabilities, but to identify which weaknesses pose real business risk, ensuring remediation efforts are focused where they matter most.

Meeting compliance obligations is important, but it does not confirm that controls will perform as expected under attack. While some organisations conduct penetration testing to support compliance, audit, cyber insurance, or board reporting, the greater value often lies in the assurance that independent validation provides, offering evidence-based insight into where risk exists and where remediation should be focused.

This approach elevates compliance from a reporting obligation to a strategic security discipline that strengthens organisational resilience and enhances overall security posture.

5 Measuring security through business outcomes

Organisations are increasingly measuring security posture success against recognised industry frameworks to guide the continuous improvement of their security controls. Security posture assessments and maturity reviews provide a clear understanding of current capability, helping organisations prioritise remediation efforts, optimise investment, strengthen resilience, and align security outcomes with business objectives.

Ultimately, the value of security validation lies not in the report itself, but in the confidence it provides leaders to make informed decisions about risk, investment, and resilience. Penetration testing and security assessments transform security from a reactive exercise into a proactive discipline, enabling organisations to address weaknesses early, reduce business risk, and continually strengthen organisational resilience.

Validate your security posture with confidence

Understand where your controls are working, where risk remains, and where targeted remediation will have the greatest impact.
Contact a Nexon expert today.

1300 800 000

pentest.nexon.com.au/

Follow **nexonap**