netutils

CYBER SECURITY

THREAT REPORT

Q3 2025

Network Utilities (Systems) Ltd
www.netutils.com | +44 (0)20 8783 3800

Table of Contents

NetUtils Q3 Threat Landscape Report July – September 2025 ..... *2*

Executive Summary **2**

The Crisis of Information Overload *2*

Information Overload and Alert Fatigue **2**

The Quest for Unified Visibility 3
Platform Consolidation Strategies 3
AI and Automation as Enablers 3
Human Factors and Organisational Culture 3
Metrics and Demonstrating Value 3
Strategic Frameworks for Complexity Management 4
Regulatory Landscape and Compliance 4

Real world examples **4**

Sellafield Nuclear Site (2024) 4
Marks & Spencer (2025) 4

Conclusion **4**

The Insider Threat Landscape *5*

Rising Costs and Prevalence **5**

Types of Insider Threat **5**

Real world examples **5**

Detection Strategies **6**

Behavioural Baselines and Anomaly Detection 6
Privileged Access Monitoring 6
Endpoint and Network Visibility 6
Social and Psychological Indicators 7
Threat Intelligence and External Monitoring 7
Continuous Improvement and Feedback Loops 7

Strategic Mitigation Frameworks **7**

Conclusion **8**

Shadow AI an emerging threat *8*

Executive Summary **8**

Shadow IT and Shadow AI 8
SME-Specific Vulnerabilities 9
Security and Compliance Risks 9
Financial and Operational Impact 9
Detection and Governance Strategies 10
Mitigation and Future Outlook 10

Conclusion **10**

About NetUtils ***11***

Sources ***12***

NetUtils Q3 Threat Landscape Report

July – September 2025

Executive Summary

The NetUtils Q3 2025 Threat Report provides a comprehensive overview of some of the most pressing cybersecurity challenges facing organisations today. It highlights the growing crisis of information overload, with security teams overwhelmed by fragmented toolsets and excessive alert volumes, often investigating less than a quarter of incoming alerts. This operational strain contributes to widespread burnout and short CISO tenures, while also increasing the risk of missed threats. The report explores the strategic value of platform consolidation and AI adoption, noting that unified security platforms and automation can significantly improve visibility, reduce response times, and enhance analyst efficiency. Human factors are also examined, with emphasis on the need for cultural change, sustainable workloads, and metrics that demonstrate business value.

We discuss insider threats and outline the rising costs and prevalence of malicious, negligent, and compromised insiders, as well as third-party risks. Real-world case studies illustrate the impact of poor visibility and delayed response, while detection strategies and mitigation frameworks are recommended to strengthen defences.

Finally, the report addresses the emerging threat of Shadow AI, particularly within SMEs, where unauthorised use of AI tools poses significant compliance, data security, and operational risks. The report concludes with a call for strategic alignment across technology, process, and people to restore clarity, resilience, and trust in cybersecurity operations.

The Crisis of Information Overload

CISOs are facing a growing crisis of information overload. Organisations now deploy an average of 83 security tools from 29 vendors, creating fragmented environments that hinder visibility and response effectiveness. This complexity transforms the CISO role from strategic leadership to reactive firefighting, with consequences including alert fatigue, burnout, and increased vulnerability to cyber threats.

Security stacks have evolved from simple perimeter defences to sprawling ecosystems covering cloud, endpoints, identity, and threat intelligence. The average cost of a breach now exceeds $4.4M globally, prompting reactive adoption of new tools. Cloud migration and unstructured data have expanded the attack surface, while AI has empowered both attackers and defenders.

Information Overload and Alert Fatigue

Security teams face thousands of alerts daily, often exceeding 3,000 alerts in large enterprises. False positives and fragmented dashboards obscure genuine threats. Typically, analysts investigate only 22% of alerts, leaving 78% unaddressed. Alert fatigue leads to

missed threats, delayed response, and staff turnover. Burnout is widespread, with 84% of professionals affected and average CISO tenure under three years.

In order to address the significant threats posed, organisations often deploy overlapping tools with little strategic planning. Large enterprises may be managing over 130 tools, yet only 10–20% are actively used on a day to day basis. This sprawl increases costs, complicates integration, and reduces visibility. Analysts must switch between interfaces, increasing errors and reducing efficiency. The requirement to be able to utilise multiple technologies along with a lack of interoperability further exacerbate the problem.

The Quest for Unified Visibility

The 'single pane of glass' remains seemingly elusive. SIEMs, XDR platforms, and custom dashboards offer partial solutions, but integration challenges persist. Most organisations operate a mosaic of panes, with limited correlation and delayed onboarding of new data feeds. Despite vendor efforts, true unification remains difficult due to technical and organisational barriers. That being said, there are some new vendors entering the market who seem to have begun to address this challenge through the delivery of a unified security operations platform. These platforms are vendor agnostic and go a long way towards overcoming the limitations of fragmented tooling by consolidating telemetry, alerts, and workflows into a single, integrated interface.

Platform Consolidation Strategies

Platformisation also offers a path forward. Consolidating vendors improves visibility, can reduce costs, and sometimes enhances response speed. Some studies show platform adopters detect and contain incidents 72–84 days faster, with 4x ROI and improved situational awareness. Strategic acquisitions by vendors support this shift, enabling integrated ecosystems with unified workflows. It should be recognised that this does contradict the traditional ‘defense in depth’ approach often cited as the more secure strategy.

AI and Automation as Enablers

AI augments human capabilities by filtering noise, triaging alerts, and automating response. 90% of CISOs are optimistic about AI’s impact. Adoption is accelerating, with 87% of organisations integrating AI into SOC workflows. It is estimated that the use of AI typically reduces investigation time by 25–50%, but trust, integration complexity, and adversarial AI remain challenges.

Human Factors and Organisational Culture

Burnout and retention are critical issues. Alert fatigue, poor work-life balance, and reactive cultures drive turnover. Addressing these requires cultural change, sustainable workloads, and technology that reduces cognitive burden. Investments in automation and consolidation improve analyst experience and preserve institutional knowledge.

Metrics and Demonstrating Value

CISOs must demonstrate ROI and effectiveness. Traditional metrics (e.g. alert counts) lack context. Modern approaches focus on mean time to detect/respond, risk exposure, and

business impact. Tailored dashboards and automated reporting help, but prioritisation is key to avoiding further overload.

Strategic Frameworks for Complexity Management

Managing complexity requires technology rationalisation, process optimisation, and cultural adaptation. Rationalisation identifies redundant tools; workflow optimisation improves triage and investigation; automation handles repetitive tasks; and training addresses the skills gap. Cultural shifts reward strategic thinking over reactive firefighting.

Regulatory Landscape and Compliance

While regulations can be seen as an administrative burden which add complexity, they can also drive improvement. GDPR, CCPA, DORA and sector-specific rules require documentation and resilience. Emerging regulations around AI and supply chain security demand new governance models. Integrating compliance into operations reduces duplication and improves visibility.

Real world examples

Sellafield Nuclear Site (2024)

One of the most striking examples of alert fatigue leading to a breach occurred at Sellafield, a UK-based nuclear facility. Security teams at the site were inundated with alerts, many of which were false positives. As a result, critical warnings were overlooked. The overload of notifications created a desensitised environment where genuine threats were missed, ultimately leading to serious cybersecurity lapses. The incident raised concerns about national infrastructure resilience and highlighted the dangers of unmanaged alert volumes in high-risk environments.

Marks & Spencer (2025)

Retail giant Marks & Spencer suffered a significant cyber attack, which disrupted online operations and exposed customer data. The breach was linked to a third-party access point, but analysts noted that fragmented monitoring and delayed response contributed to the scale of the incident. The attack, attributed to the hacking group Scattered Spider, exploited visibility gaps and overwhelmed internal systems. Deutsche Bank estimated the financial impact at over £30 million, with ongoing losses of £15 million per week.

Conclusion

Information overload is eroding the effectiveness of cybersecurity programmes and placing unsustainable pressure on CISOs and their teams. Fragmented tooling, excessive alert volumes, and reactive workflows are contributing to missed threats, burnout, and rising breach costs. To mitigate these risks, organisations may consider consolidating platforms to reduce complexity, adopt AI and automation to streamline operations, and optimise processes to prioritise high-impact threats. Cultural change is equally vital, security teams need sustainable workloads, recognition, and the tools to focus on strategic defence rather than firefighting. By aligning technology, process, and people, organisations can restore clarity, improve resilience, and empower their security leadership.

The Insider Threat Landscape

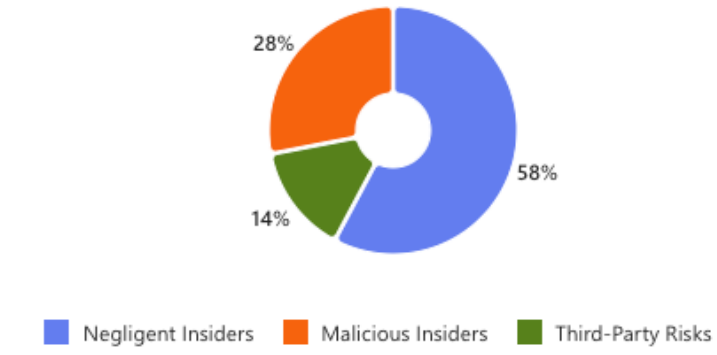
Insider threats remain one of the most persistent and costly cybersecurity challenges. Unlike external attackers, insiders possess legitimate access to systems and data, making detection and prevention significantly more complex. With 74% of organisations considering themselves moderately or highly vulnerable to insider threats, and average annual costs exceeding £13.5 million, the need for robust, balanced strategies is urgent. This article explores the nature of insider threats, key case studies, detection challenges, and strategic frameworks for mitigation.

Rising Costs and Prevalence

According to the Ponemon Institute, insider threat costs have surged by 95% since 2018, with organisations spending an average of £211,000 per incident on containment, yet only £37,000 on proactive monitoring. Credential theft and malicious acts are the most expensive to remediate. Industries with large, distributed workforces and sensitive data, such as finance, healthcare, and technology face heightened risks.

Types of Insider Threat

- **Malicious Insiders**
  Motivated by financial gain, revenge, or ideology.
- **Negligent Insiders**
  Account for up to 58% of incidents. Common errors include falling for phishing, misconfiguring systems, and mishandling data.
- **Compromised Insiders**
  External actors exploit legitimate credentials via social engineering or technical compromise.
- **Third-Party Risks**
  Vendors and contractors with privileged access can introduce vulnerabilities.



https://www.keevee.com/insider-threat-statistics

Real world examples

- **Waymo (Google)**
  Anthony Levandowski, a lead engineer who had played a key role in developing Waymo's technology, resigned from the company and shortly thereafter founded his own self-driving car company called Otto. What appeared to be a typical departure of a senior executive to pursue entrepreneurial opportunities was revealed to be a

carefully orchestrated theft of intellectual property that had been planned well in advance of his resignation.

- **Capital One**
  Paige Thompson, a former software engineer who had previously worked for Amazon Web Services, leveraged her intimate knowledge of cloud security architecture to identify and exploit a misconfigured web application firewall protecting Capital One's environment. Through this vulnerability, Thompson gained unauthorised access to the accounts and credit card applications of more than one hundred million Capital One customers, making it one of the largest data breaches in the financial services sector
- **Anthem Healthcare**
  The Anthem breach demonstrates how social engineering attacks that target employees can lead to massive data exposure. In this incident, hackers sent phishing emails to Anthem employees containing links to malware. When unsuspecting employees clicked on these links, malware was installed on their workstations, providing attackers with a backdoor into Anthem's network and enabling them to access the organisation's database remotely. This ultimately led to the theft of data from 78.8M individuals. Detection relied on a vigilant employee.

Detection Strategies

Detecting insider threats is inherently complex due to the legitimate access insiders possess and the subtlety of their actions. Effective detection requires a multi-layered approach that combines behavioural analytics, contextual awareness, and continuous monitoring across diverse environments.

Behavioural Baselines and Anomaly Detection

Establishing behavioural baselines is critical. Organisations must monitor typical user activity such as login times, data access patterns, and system usage and flag deviations that may indicate malicious intent or compromise. Behavioural analytics tools can identify anomalies such as unusual data transfers, off-hours access, and unauthorised application use. Contextual factors must be considered to reduce false positives.

Privileged Access Monitoring

Privileged users pose elevated risks. Monitoring requires PAM solutions enforcing least privilege and just-in-time access, audit trails of administrative actions, and segregation of duties. High-risk activities should trigger alerts and require secondary verification.

Endpoint and Network Visibility

Detection must extend beyond the perimeter. EDR tools monitor device-level activity, DLP systems control data movement, and SIEM platforms correlate logs. CASBs provide visibility into SaaS usage across remote environments.

Social and Psychological Indicators

Technical monitoring must be complemented by human-centric detection. Behavioural changes such as disengagement, financial distress, or policy circumvention should be reported confidentially. A culture of trust is essential.

Threat Intelligence and External Monitoring

Monitoring external sources like dark web marketplaces and threat intelligence feeds can reveal signs of insider compromise. Tracking emerging social engineering tactics is also vital.

Continuous Improvement and Feedback Loops

Detection strategies must evolve. Post-incident reviews should inform system tuning and training. Metrics such as dwell time and false positive ratio should be assessed regularly.

Strategic Mitigation Frameworks

Effectively managing insider threats requires a strategic approach that integrates technical controls, governance, and cultural awareness. Two widely adopted frameworks, **the NIST Cybersecurity Framework** and **Zero Trust Architecture** offer structured methodologies for mitigating insider risk across the threat lifecycle.

The NIST Cybersecurity Framework provides a flexible, risk-based model built around five core functions: Identify, Protect, Detect, Respond, and Recover. Organisations begin by identifying critical assets and mapping access privileges across employees and third parties. This includes conducting risk assessments and establishing governance structures, such as cross-functional insider threat teams. Protection measures focus on reducing the likelihood and impact of incidents through least privilege access, encryption, network segmentation, and comprehensive security awareness training. Detection capabilities rely on behavioural analytics, log correlation, and data loss prevention tools, while also encouraging staff to report behavioural red flags. When incidents occur, response protocols ensure coordinated investigations, containment, and communication with stakeholders. Recovery efforts aim to restore operations, support affected teams, and integrate lessons learned into future policy and training.

Zero Trust Architecture complements this by rejecting the notion of implicit trust within the network perimeter. It enforces continuous verification of users, devices, and access requests based on identity, device posture, location, and context. Access is granted on a least privilege, just-in-time basis, and revoked when no longer needed. Micro-segmentation limits lateral movement, and adaptive controls respond to behavioural changes in real time. Zero Trust is particularly effective in mitigating insider threats by reducing the impact of compromised credentials, preventing privilege escalation, and maintaining visibility across hybrid and remote environments.

Together, these and other frameworks enable organisations to build resilient, adaptive insider threat programmes that balance security imperatives with operational flexibility and employee trust.

Conclusion

Insider threats represent a complex and evolving challenge that demands a proactive, multi-dimensional response. Whether driven by malice, negligence, or external compromise, insiders operate with legitimate access, making their actions difficult to detect and potentially devastating in impact. The financial, operational, and reputational consequences of insider incidents can be severe, particularly when detection is delayed or response mechanisms are underdeveloped.

To address this risk effectively, organisations must move beyond reactive measures and adopt strategic frameworks that integrate technical controls, behavioural monitoring, and cultural awareness. The NIST Cybersecurity Framework and Zero Trust Architecture offer robust foundations for building resilient insider threat programmes. These models emphasise continuous verification, least privilege access, and adaptive response capabilities, enabling organisations to limit exposure and respond swiftly to anomalies.

Equally important is the cultivation of a security-conscious culture that empowers employees to act as allies in threat detection rather than subjects of suspicion. Training, transparency, and psychological safety are essential to ensuring that staff understand their role in protecting organisational assets and feel confident reporting concerns.

Ultimately, insider threat mitigation is not a one-time initiative but an ongoing discipline. Organisations must continuously refine their policies, technologies, and practices in response to emerging risks, lessons learned, and changes in the working environment. By aligning security strategy with operational needs and employee trust, businesses can reduce insider risk while enabling the innovation and collaboration that drive long-term success.

Shadow AI an emerging threat

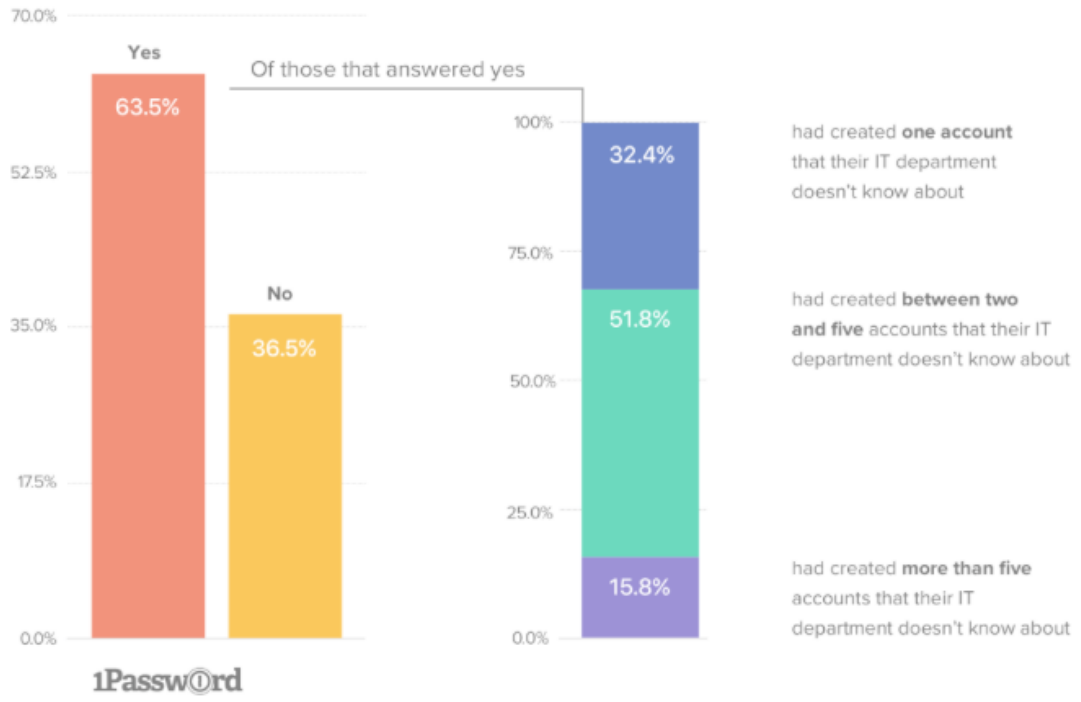
Executive Summary

The rapid adoption of AI platforms and large language models (LLMs) has transformed operations for small and medium-sized enterprises (SMEs), offering new efficiencies but also introducing significant security, compliance, and governance risks. Shadow AI (the unauthorised use of AI tools) has emerged as a critical evolution of traditional Shadow IT, with over 50% of organisations reporting at least one shadow AI application in use. This article outlines the key risks, vulnerabilities, and mitigation strategies for SMEs navigating this evolving threat landscape.

Shadow IT and Shadow AI

Shadow IT refers to the use of unauthorised software, devices, or services by employees, often driven by productivity needs or perceived inadequacies in approved tools. With the rise of AI, this has evolved into Shadow AI, with employees using AI platforms like ChatGPT without IT oversight. These tools, while accessible and user-friendly, pose serious risks such as data leakage, regulatory non-compliance, and intellectual property exposure. Studies show that 70% of employees using AI tools do so without informing their employers, and 67% use personal accounts, further complicating governance.

1Password surveyed a representative sample of 2,119 U.S. adults who work in an office with an IT department and use a computer for work.



https://blog.1password.com/challenges-of-shadow-it/

SME-Specific Vulnerabilities

SMEs are particularly vulnerable due to limited IT resources, generalist staff, and informal technology adoption practices. Financial constraints often prevent investment in robust security infrastructure, while cultural emphasis on agility can lead to bypassing formal approval processes. Fragmented IT environments and lack of centralised identity management further exacerbate the risks. Compliance with regulations like GDPR or HIPAA is especially challenging without dedicated governance frameworks.

Security and Compliance Risks

Some of the more significant risks that shadow AI introduces includes unauthorised data processing, lack of audit trails, and potential violations of data protection laws. Also, if not properly configured or controlled, LLMs may retain and reuse sensitive inputs, leading to data leakage or intellectual property loss. The use of personal accounts and third-party integrations without oversight increases the risk of credential compromise and malware exposure. SMEs in regulated sectors face heightened risks of non-compliance, with potentially severe financial and reputational consequences.

Financial and Operational Impact

Shadow IT can lead to redundant software costs, unexpected subscription fees, and increased incident response expenses. Productivity losses arise from inefficiencies and lack of integration with official systems. Business continuity may be jeopardised if critical processes rely on unauthorised tools. Data breaches can damage customer trust and lead to lost

revenue. Additionally, cyber insurance policies may exclude coverage for incidents involving unauthorised tools, leaving SMEs financially exposed.

Detection and Governance Strategies

While not all SMEs will be in a position to implement multiple detection and governance technologies, there are some cost effective solutions on the market specifically built for the SME organisation. It is recommended that SMEs should adopt a layered approach to detection and governance. Technical measures include network traffic analysis, Cloud Access Security Brokers (CASBs), endpoint detection and response (EDR), and user behaviour analytics. Regular audits, employee self-reporting, and vendor assessments complement these tools. Governance frameworks should include clear AI usage policies, risk assessments, cross-functional oversight, data governance, and compliance integration. Training and awareness programmes are also essential to foster a culture of responsible AI use.

Mitigation and Future Outlook

Mitigation strategies should prioritise approved alternatives to unauthorised tools, implement proportionate security controls, and establish incident response plans. As AI technologies evolve, SMEs must prepare for new risks, regulatory changes, and insurance considerations. Participation in industry forums and adoption of emerging AI governance standards will be key. Investing in AI literacy and strategic planning will enable SMEs to harness AI benefits while managing associated risks effectively.

Conclusion

Shadow AI has rapidly evolved into a critical cybersecurity and governance challenge for SMEs, amplifying the risks traditionally associated with Shadow IT. The unauthorised use of AI platforms, often driven by convenience and a lack of awareness, can expose sensitive data, breach compliance obligations, and undermine operational integrity. SMEs, with limited resources and informal technology adoption cultures, are particularly vulnerable.

Mitigating these risks requires more than reactive controls. SMEs must adopt proportionate governance frameworks that define acceptable AI use, implement practical monitoring tools to detect unauthorised activity, and foster a culture of responsible innovation through targeted education. Strategic planning is essential, approved alternatives to popular AI tools should be readily available, and governance must be embedded early in the adoption process.

By taking a proactive, balanced approach, SMEs can harness the benefits of AI while maintaining control over their data, compliance posture, and business continuity. Shadow AI is not a passing trend, it is a structural shift in how technology is used. Addressing it must be a strategic priority.

About NetUtils

Network Utilities Systems Ltd (NetUtils) is a trusted cybersecurity partner dedicated to helping organisations strengthen their defences and protect digital assets in today's complex threat landscape. With extensive industry expertise, NetUtils provides tailored solutions to your security needs. From acting as an extension of your team with managed security services to preparing an incident response plan for business continuity, our services equip your organisation with the tools and support needed to address cybersecurity challenges confidently.

For a detailed consultation and to explore how NetUtils can support your cybersecurity strategy, contact us:

Email: info@netutils.com
Phone: 0208 783 3800
Website: www.netutils.com

Certificate No:201792013

Certificate No:201782013

Sources

Referenced for the statistics and information contained in the report:

- https://www.cybersaint.io/blog/cybersecurity-alert-overload-is-a-ceos-problem-heres-how-to-fix-it,
- https://www.onetrust.com/resources/ciso-data-threats-infographic/,
- https://www.sekoia.io/en/glossary/alert-fatigue/,
- https://threatcop.com/blog/top-7-strategic-challenges-faced-by-cisos-in-2025/,
- https://kpmg.com/us/en/articles/2025/top-ciso-challenges-solved.html,
- https://arcticwolf.com/cybersecurity-alert-fatigue/,
- https://www.datadoghq.com/monitoring/single-pane-of-glass-monitoring/,
- https://strobes.co/blog/strategic-tool-consolidation-for-cisos/,
- https://www.jit.io/resources/appsec-tools/continuous-security-monitoring-csm-tools,
- https://www.resillion.com/single-pane-of-glass-a-remops-solution/,
- https://www.bankinfosecurity.com/platform-shift-cisos-are-embracing-consolidation-a-28111,
- https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-tools/,
- https://www.keepit.com/blog/tool-sprawl/,
- https://www.cybersecuritydive.com/news/consolidation-security-tools/738912/,
- cybersecurity-complexity,
- https://ecam.com/security-blog/5-benefits-of-an-integrated-security-system,
- https://www.salesforce.com/resources/articles/messaging-vendor-consolidation-conf/,
- https://www.paloaltonetworks.com/resources/research/ibm-study-platforms-deliver-value,
- https://www.ey.com/en_us/insights/cybersecurity/enhancing-cybersecurity-metrics-ciso-strategies,
- https://www.cybersaint.io/blog/leveraging-ciso-dashboard-metrics-to-drive-cybersecurity-strategy,
- https://www.idwatchdog.com/education/-/article/insider-threats-and-data-breaches,
- https://www.exabeam.com/explainers/insider-threats/insider-threat-examples/,
- https://deepstrike.io/blog/insider-threat-statistics-2025,
- https://www.nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html,
- https://gurucul.com/blog/famous-insider-threat-cases/,
- https://gurucul.com/blog/challenges-of-detecting-and-mitigating-insider-threats/,
- behavior-change,
- https://www.ajmc.com/view/psychological-safety-and-use-of-incident-reporting-systems,
- https://www.intelligentciso.com/2025/03/03/qa-how-organizations-can-achieve-secure-by-design-by-2030/,
- https://panorays.com/blog/cyber-threat-landscape-for-third-party-vendors/,
- https://delinea.com/blog/it-offboarding-checklist-template,
- https://www.sentinelone.com/cybersecurity-101/cloud-security/saas-security-risks/,
- https://www.exabeam.com/explainers/insider-threats/insider-threat-examples/,
- https://secureframe.com/blog/onboarding-and-offboarding,
- https://spot.io/resources/cloud-security/7-saas-security-risks-and-how-to-prevent-them/,
- https://www.dni.gov/files/NCSC/documents/features/NITTF_MaturityFramework_web.pdf,
- https://sosafe-awareness.com/en-us/glossary/human-risk-management/,
- https://blog.usecure.io/shadow-it-risks-are-your-employees-using-unauthorized-apps,
- https://www.proofpoint.com/us/blog/dspm/llm-security-risks-best-practices-solutions,
- https://blog.1password.com/new-research-uncovers-four-security-challenges-caused-by-unmanaged-ai/,
- https://www.emerge-creatives.com/post/ai-risk-assessment-template-for-smes-a-comprehensive-step-by-step-guide,
- https://www.tredence.com/blog/llm-risk-management,
- https://www.dvirc.org/learn/ai-governance-for-small-and-mid-sized-businesses/,
- https://www.proofpoint.com/us/blog/dspm/ai-and-data-protection-strategies-for-llm-compliance-and-risk-mitigation,
- https://www.ironedgegroup.com/what-are-managedai-services-why-ai-governance-is-critical-for-smbs/,
- https://owasp.org/www-project-top-10-for-large-language-model-applications/,
- https://zylo.com/blog/shadow-ai/,
- https://drj.com/journal_main/business-continuity-management-and-artificial-intelligence/

Network Utilities (Systems) Ltd

The Larches, Sevenoaks Road, Orpington, Kent BR6 7FB
www.netutils.com | +44 (0)20 8783 3800