netutils

CYBER SECURITY

THREAT REPORT

Q4 2025

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

Table of Contents

NetUtils Q4 Threat Landscape Report

October - December 2025

Executive Summary

The current threat landscape highlights a clear shift for UK organisations. Cyber risk is now driven less by traditional malware and more by identity compromise, supplier exposure, and the increasing complexity of cloud environments. Over the past quarter, this shift has been consistently reflected across Microsoft 365 related incidents, high profile UK retail breaches, and the evolving role of artificial intelligence in both attack and defence.

Microsoft 365 continues to represent a critical risk concentration point. Recent incidents show attackers routinely bypassing perimeter controls by exploiting compromised credentials, MFA fatigue, and excessive permissions. Once access is obtained, threat actors prioritise persistence and data access across email, collaboration, and file sharing platforms. The resulting impact is often subtle but material, ranging from data exposure and financial fraud to increased regulatory and compliance risk. These incidents underline the limitations of baseline security controls when they are not supported by continuous identity threat detection, effective response, and clear visibility across the tenant.

Recent UK retail and consumer brand incidents further demonstrate how cyber events translate directly into operational disruption, customer impact, and reputational damage. Common themes include third party access risk, delayed detection, and limited oversight of identity and SaaS environments. While most visible in retail, these lessons apply equally to organisations with complex supplier ecosystems, large volumes of customer data and heavy reliance on cloud platforms.

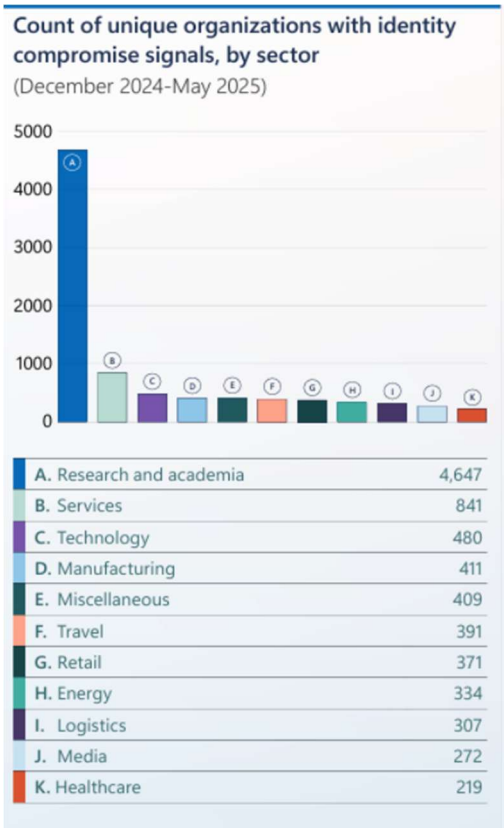
Alongside these challenges, a more positive and strategic trend is emerging. Organisations are increasingly using AI in a controlled and effective manner to strengthen cyber defence and validate resilience. AI is proving most valuable when applied to threat detection, identity and behavioural analysis, analyst support and continuous security testing. When governed correctly and combined with skilled security teams, AI reduces noise, accelerates response, and enables more realistic testing of real world attack paths. This represents a clear contrast with the unmanaged use of AI tools highlighted in the previous quarter.

Taken together, these findings point to a maturing security focus. The most resilient organisations are those that prioritise identity security, maintain strong oversight of suppliers and cloud platforms, invest in continuous detection and response, and adopt AI as a governed capability rather than an unmanaged risk. Cyber security is no longer about isolated controls, but about sustained visibility, continuous validation, and the ability to respond decisively as threats emerge.

Microsoft 365 Threats and Defensive Priorities

Microsoft 365 remains a primary target for threat actors due to its central role in identity, email, collaboration, and document management across UK organisations. Recent incident response activity continues to show that successful compromises are far more likely to originate from identity-based attack paths than from traditional malware delivery.

The Microsoft Digital Defense Report 2025 reinforces this shift, identifying identity compromise as a dominant risk driver across cloud environments, with financially motivated threat activity accounting for the majority of observed attacks. The report highlights the scale at which identity threats now operate, with Microsoft analysing tens of millions of identity related risk signals daily across its global telemetry. This context explains why compromised credentials, token misuse, and abuse of legitimate access remain highly effective techniques against Microsoft 365 tenants.



Source: Microsoft Threat intelligence, Commercial Cloud.

Image taken from Microsoft Digital Defense Report 2025

Common attack paths observed over the last quarter include credential phishing leading to account takeover, MFA fatigue attacks against privileged users, and abuse of OAuth application permissions. Once access is established, threat actors prioritise persistence and data access across Exchange Online, SharePoint, OneDrive, and Teams rather than immediate disruption. This approach increases dwell time and reduces the likelihood of early detection.

Affected Sectors and Technologies

Attack patterns are being observed across all sectors, with particular impact on professional services, education, healthcare, and mid market commercial organisations. These environments typically combine large user populations, extensive external collaboration, and cloud first identity models.

Key technologies affected include Entra ID, Exchange Online, SharePoint Online, OneDrive, and Teams. Hybrid identity environments remain especially exposed, as misalignment between on-premises and cloud identity controls can create visibility gaps that attackers exploit.

Business and Security Impact

The business impact of Microsoft 365 compromise is often understated because incidents do not always present as clear outages. Instead, organisations experience silent data exposure, unauthorised access to sensitive communications, invoice fraud, and downstream supply chain risk.

From a security and governance perspective, the Microsoft Digital Defense Report 2025 highlights that identity led attacks frequently persist undetected when monitoring is limited to baseline controls. Limited visibility into tenant configuration, permissions, and anomalous behaviour further increases regulatory exposure under GDPR, Cyber Essentials, and ISO 27001.

Recommended Mitigation Priorities

Identity Threat Detection and Response with Continuous Oversight

Given the scale and persistence of identity-based threats, organisations should introduce dedicated identity threat detection and response capabilities. These should continuously monitor authentication activity, privilege changes, token misuse, and abnormal behaviour, supported by 24x7 SOC oversight to ensure rapid containment.

Improved Visibility Across the Microsoft 365 Tenant

Independent visibility across Microsoft 365 is critical to understanding real world risk.

Enhanced insight into permissions, external sharing, dormant accounts, and configuration drift enables improved risk reduction and clearer reporting.

Privilege and Access Hygiene

Administrative roles, application permissions, and external access should be reviewed regularly and aligned to least privilege principles. Standing access should be minimised to reduce the impact of credential compromise.

Identity Focused Incident Readiness

Incident response planning should explicitly account for identity compromise scenarios, including token revocation, session invalidation, and coordinated stakeholder communication.

Conclusion

Recent Microsoft 365 attacks continue to demonstrate that risk is driven primarily by how identities, permissions, and access are used rather than by weaknesses in the platform itself. Credential misuse, excessive privileges, and limited tenant visibility allow attackers to persist quietly and access sensitive data without triggering immediate disruption.

The key takeaway from this section is that effective Microsoft 365 security depends on continuous oversight of identity activity, clear understanding of permissions and configuration, and the ability to detect and respond to abnormal behaviour quickly. Organisations that address these areas are better positioned to limit dwell time, reduce business impact, and maintain confidence in the security of their cloud collaboration environment.

Recent UK Retail Cyber Incidents and Lessons for Defence

Context and Recent Threat Activity

Over the last three months, several UK retailers have publicly disclosed cyber incidents that resulted in operational disruption, customer communications, and regulatory engagement. These incidents have attracted significant attention not because of novel attack techniques, but because they demonstrate how well understood weaknesses are still being exploited in real environments.

Across recent cases, attackers did not rely on highly sophisticated malware. Instead, breaches commonly originated through trusted access paths, including supplier connections, compromised credentials, and poorly monitored SaaS environments. In many instances, attackers were able to operate within legitimate systems for extended periods before detection, increasing both impact and recovery complexity.

How Recent Retail Breaches Occurred

Analysis of public disclosures and incident reporting highlights several recurring breach mechanisms:

Compromise via third party or supplier access

In multiple incidents, attackers gained an initial foothold through third party providers rather than directly breaching core retail infrastructure. Where suppliers had persistent access to systems or data, compromise within the supply chain enabled attackers to inherit trusted access and move laterally without triggering perimeter defences.

Use of legitimate credentials and services

Rather than deploying custom tooling, attackers frequently abused legitimate accounts, cloud services, and administrative features. This allowed activity to blend into normal operational noise, delaying detection and reducing the effectiveness of traditional security controls.

Limited visibility across cloud and SaaS platforms

Once inside, attackers exploited gaps in visibility across email, collaboration, and customer data platforms. In several cases, organisations were unable to quickly determine what data had been accessed, which users were affected, or how long unauthorised access had persisted, extending investigation timelines and increasing customer impact.

Delayed detection and response escalation

In many incidents, initial compromise was not identified until secondary indicators emerged, such as unusual customer activity, service disruption, or third-party notification. By this stage, attackers had often already accessed sensitive data or disrupted business processes.

Affected Sectors and Technologies

While these incidents are most visible in retail due to brand exposure and disclosure requirements, the breach patterns themselves are not retail specific. Similar access paths and failure points are increasingly observed across any sector that relies on:

- Third party providers with ongoing system or data access
- Cloud based collaboration and identity platforms
- Distributed workforces and outsourced operational services

Commonly involved technologies include identity platforms, remote support tooling, SaaS collaboration environments, e-commerce integrations, and customer communications systems.

Business and Security Impact

The impact of these incidents extended well beyond the initial technical compromise:

- Operational disruption, affecting store operations, fulfilment, and customer services during containment and recovery
- Customer impact, including notifications, increased support demand, and prolonged reputational scrutiny
- Regulatory engagement, particularly where personal data exposure could not be immediately ruled out
- Extended recovery costs, driven by forensic investigation, legal support, security uplift, and supplier reassessment

In several cases, uncertainty around the scope and duration of access proved as damaging as the breach itself, reinforcing the importance of visibility and preparedness.

Lessons for Defence

Recent retail incidents show that effective resilience comes less from adding isolated controls and more from understanding how attackers exploit trust relationships, legitimate access, and visibility gaps in real environments. The most resilient organisations combine strong day-to-day defensive controls with proactive testing of how those controls could fail in practice, allowing weaknesses to be identified and addressed before they are exploited.

Controls Matrix: Defensive and Offensive Measures

Risk Area	Defensive Controls	Offensive / Validation Controls
Supplier and third party access	Access governance, least privilege, monitoring of supplier accounts, contractual security requirements	Breach path testing to simulate supplier compromise and identify lateral movement opportunities
Use of legitimate tools and accounts	Identity threat detection, privilege management, behavioural monitoring	Adversary simulation using real accounts and permissions to validate escalation paths
Cloud and SaaS visibility	SaaS security posture management, permission and sharing visibility, audit logging	Configuration and permission testing to identify exposure that would delay containment
Detection and response speed	Continuous monitoring, SOC oversight, defined escalation playbooks	Continuous exposure validation to identify high-risk paths that require prioritised monitoring

Conclusion

Recent UK retail incidents highlight that many breaches succeed not through novel techniques, but through the exploitation of trusted access, supplier relationships, and operational blind spots. Public disclosures show that once attackers gain a foothold, limited visibility and delayed detection often amplify both customer impact and recovery effort.

The key lesson from these incidents is that resilience depends on understanding how real attacks unfold across third party access, cloud services, and day-to-day operations. Organisations that focus on reducing trust-based exposure, improving visibility across critical platforms, and accelerating detection are better placed to limit disruption and contain the business and reputational impact of future incidents.

Using AI for Good: Defensive and Testing Applications in Cyber Security

Context and Recent Developments

In the previous quarter, the focus was on the risks associated with Shadow AI and the uncontrolled use of generative tools within organisations. While those risks remain valid, the last three months have also demonstrated a more balanced and

encouraging trend: the effective and governed use of AI to strengthen cyber defence, improve resilience, and test organisational readiness.

Across the cyber security industry, AI is increasingly being applied in controlled, security led use cases rather than ad hoc productivity tools. The emphasis has shifted towards augmentation rather than replacement, using AI to reduce noise, accelerate decision making, and simulate attacker behaviour at scale. When deployed with oversight, AI is proving to be a force multiplier for already stretched security teams.

Where AI Is Being Used Effectively

Threat Detection and Signal Prioritisation

AI driven analytics are now widely used to process large volumes of security telemetry and identify patterns that would be difficult to detect through manual analysis alone. By learning normal behaviour across users, devices, and workloads, AI can identify subtle anomalies that indicate credential misuse, lateral movement, or early stage compromise.

This has been particularly effective in cloud and identity heavy environments, where traditional rule based alerts often generate excessive noise. AI assisted prioritisation enables security teams and SOC analysts to focus on genuinely high risk activity rather than alert volume.

Identity and Behavioural Analysis

AI is increasingly embedded in identity security, helping to identify suspicious authentication patterns, unusual access behaviour, and deviations from established user baselines. Rather than relying solely on static indicators, these models adapt over time, improving detection accuracy as environments change.

When combined with human led investigation and response, this approach improves both speed and confidence in containment decisions, reducing the dwell time of identity based attacks.

Automated Response and Analyst Support

AI is also being used to support, not replace, security analysts. Common applications include automated enrichment of alerts, summarisation of incidents, and recommendation of next actions based on historical outcomes. This reduces cognitive load, shortens investigation timelines, and helps less experienced analysts operate more effectively within a governed framework.

AI as a Tool for Security Testing and Validation

Beyond defence, AI is increasingly used to test security controls proactively.

Adversary Simulation and Attack Path Testing

AI powered security testing platforms can safely simulate attacker behaviour, identifying exploitable paths across identity, endpoint, and cloud environments. Unlike traditional point in time testing, these tools can be run continuously, validating whether changes in configuration, permissions, or exposure have introduced new risk.

This approach supports a shift from compliance driven testing to resilience driven testing, providing clearer insight into real world exposure rather than theoretical vulnerability.

Continuous Control Validation

AI enables more frequent and targeted testing of controls such as MFA enforcement, privilege boundaries, and detection coverage. This allows organisations to verify that defensive investments are working as intended and to prioritise remediation based on exploitability rather than severity scores alone.

Governance and Guardrails Remain Critical

The positive impact of AI is dependent on clear governance, defined use cases, and human oversight. Successful organisations treat AI as part of their security architecture, not as an unmanaged toolset. Key enablers include:

- Clear policies defining approved AI driven security use cases
- Integration with existing detection, response, and testing processes
- Ongoing validation of AI outputs by experienced security professionals
- Alignment with regulatory, data protection, and ethical considerations

This contrasts sharply with Shadow AI, where lack of oversight creates risk. The distinction is not the technology itself, but how it is selected, deployed, and governed.

Business and Security Impact

For UK organisations, the effective use of AI in cyber security is delivering tangible benefits:

- Faster detection and response without linear increases in staffing
- Improved visibility across complex hybrid and cloud environments
- More realistic testing of security posture and resilience
- Better evidence for boards and regulators that controls are effective

Importantly, AI is helping organisations move from reactive security toward a more preventative and continuously validated model.

Strategic Recommendations for Improving Cyber Resilience

The themes identified across this quarter's threat landscape point to a need for practical, sustainable improvements rather than wholesale technology change. The most effective organisations are focusing on visibility, validation, and response capability, supported by trusted partners and clear governance.

Prioritise Identity as the Primary Security Control Plane

Identity has become the most consistently exploited attack surface across cloud platforms, collaboration tools, and third party access. Organisations should treat identity security as a core resilience capability rather than a supporting control.

Key actions include strengthening monitoring of authentication activity, privilege changes, and abnormal behaviour across cloud identity platforms. This should be supported by continuous oversight rather than periodic review, ensuring compromised accounts are detected and contained quickly. Where internal coverage is limited, extending monitoring and response through a fully resourced Security Operations Centre provides assurance that identity based threats are addressed at all times.

Improve Visibility Across Microsoft 365 and SaaS Environments

Many of the incidents reviewed this quarter were exacerbated by limited visibility into how cloud environments were configured and used in practice. Excessive permissions, external sharing, inactive accounts, and configuration drift all increase risk while remaining difficult to track manually.

Organisations should introduce enhanced visibility across collaboration and file sharing platforms to better understand access rights, sharing behaviour, and security posture. Clear reporting supports faster risk reduction and enables IT and security leaders to demonstrate control to senior management and auditors.

Strengthen Third Party and Supplier Risk Management

Supplier access continues to represent a significant risk multiplier. Recent UK incidents demonstrate how third party compromise can lead to direct customer impact even when core systems remain unaffected.

Organisations should reassess how suppliers access systems and data, ensuring access is limited, monitored, and regularly reviewed. Security expectations should be clearly defined, proportionate, and aligned to business criticality. Regular validation of supplier controls supports compliance and reduces exposure across the supply chain.

Use AI to Enhance Defence and Validate Controls, Not Replace People

AI is delivering measurable benefits when applied to detection, investigation support, and security testing. Organisations should focus on controlled use cases where AI reduces noise, accelerates response, and enables continuous validation of security posture.

Successful adoption depends on governance. AI driven security capabilities should be integrated into existing processes, overseen by skilled professionals, and regularly reviewed for effectiveness. This ensures AI strengthens resilience without introducing unmanaged risk.

Focus on Preparedness, Not Just Prevention

Across all incidents reviewed, response speed and clarity had a significant impact on business outcome. Organisations should ensure incident response plans explicitly cover identity compromise, cloud platform incidents, and supplier related scenarios.

Regular testing, clear decision ownership, and access to experienced support reduce confusion during incidents and improve recovery outcomes. Preparedness is increasingly a differentiator between organisations that contain incidents quickly and those that face prolonged disruption.

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

References

- Cybersecurity and Infrastructure Security Agency (CISA). *Cloud Security Technical Advisories*.
- Computing (UK). *Cyber security and retail technology incident reporting*.
- ENISA (European Union Agency for Cybersecurity). *AI in Cybersecurity and Resilience*.
- Horizon3.ai *Enhancing Cybersecurity Through Collaborative Risk Management Use Case Document May 2024*
- Information Commissioner's Office (ICO), UK. *Personal Data Breach Reporting Guidance*.
- ISO/IEC 27001:2022. *Information Security Management Systems*.
- ISO/IEC 27036. *Information Security for Supplier Relationships*.
- Marks & Spencer. *Customer and regulatory communications relating to cyber incidents (2024–2025)*.
- Microsoft Corporation. *Microsoft Digital Defense Report 2025*.
- Microsoft Security Intelligence. *Identity and Access Threat Research*.
- MITRE Corporation. *MITRE ATT&CK Framework for Enterprise and Cloud*.
- MITRE Corporation. *Adversary Emulation and Continuous Validation Research*.
- National Cyber Security Centre (NCSC), UK. *Cyber security for large organisations*.
- National Cyber Security Centre (NCSC), UK. *Supply Chain Security Guidance*.
- The Guardian. *UK retail cyber incident reporting (2024–2025)*.
- UK incident response and managed security reporting (2025).
- UK media and industry reporting on retail and consumer cyber incidents (2024–2025).
- UK Government. *Cyber Essentials and Cyber Essentials Plus Technical Requirements*.
- World Economic Forum. *Global Cybersecurity Outlook 2025*.

Network Utilities (Systems) Ltd

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