Picture credit: AdobeStock

THE NEW PERIMETER

James Gillies *underlines why identity, not perimeter, is the new battleground for UK Cybersecurity*

Recent industry research shows identity-based threats now rank among the most significant risks facing organisations, driven by sharp increases in credential theft, session hijacking and the exploitation of poorly governed identities.

Nearly 90 percent of organisations experienced a cybersecurity incident in the past year, with more than four in ten suffering multiple breaches, underscoring how commonplace successful attacks have become even amid sustained increases in security spending. Attackers have shifted focus away from breaching hardened network defences towards exploiting logins, privileges and identity systems that provide faster, quieter access to data and systems.

As hybrid work and cloud adoption become the norm, this identity-first threat landscape is intensifying. Traditional perimeter controls are routinely bypassed and security leaders increasingly recognise that identity has effectively become the new perimeter. This shift fundamentally changes how UK organisations must think about cyber resilience and how their security partners and service providers can support them.

The traditional security perimeter was built for a world where users worked inside offices, applications lived on-premise and firewalls formed a clear boundary between trusted and untrusted networks. That model no longer reflects reality. Many organisations across the UK have raced to adopt different cloud technologies to support hybrid and remote working needs, but often overlook security settings or fail to review configurations once the platform has been set up.

This 'if it's not broken, why fix it' approach has created a quiet security risk from within, as misconfigurations are leaving certain users with standing account privileges they shouldn't have or that should have been revoked long ago.

The rush to adopt cloud technologies has also led organisations to neglect basic cybersecurity principles, such as using weak passwords, sharing login details, and failing to apply multi-factor authentication for all users. Each issue blurs the security perimeter further and creates quiet backdoors for attackers into enterprise networks. These gaps are exactly what attackers increasingly exploit to gain a foothold inside organisations.

Nearly six in ten organisations say their security has become too complex to manage effectively

Users, devices and workloads now operate everywhere, across homes, offices, cloud platforms and partner ecosystems. Recent research shows that nearly six in ten organisations say their security environments have become too complex to manage effectively and only around half are confident they can clearly identify where their security gaps exist. In this environment, the perimeter is no longer a physical or network boundary; it is the individual user and their identity.

Access to data must therefore be based on who someone is, what they are trying to access, from where and under what conditions. This is why zero trust principles have become central to modern security strategies. Trust is no longer implicit once a user is 'inside' the network; it must be continuously verified and access should be limited to the minimum required to perform a task.

Many organisations still operate legacy access models that grant broad, standing privileges once credentials are accepted, creating an attractive opportunity for attackers. 2025 research shows that over 50 percent of organisations acknowledge they have invested in security controls they don't truly need, while two-thirds admit they are not fully using the capabilities they already have. If an identity can be compromised, the attacker effectively bypasses multiple layers of traditional defence in one step.

From an attacker's perspective, identity offers the fastest route to value. Rather than attempting to breach hardened infrastructure, they target the mechanisms that grant legitimate access. One study shows that well over half of modern breaches now involve compromised credentials rather than technical exploits, reflecting how effective identity abuse has become.

Advances in automation and AI have made phishing campaigns more convincing, increasingly personalised and considerably harder for users to distinguish from legitimate communications.

Attackers no longer rely on poor spelling or obvious red flags. Instead, they abuse legitimate authentication flows, clone cloud identity portals and exploit password reset and MFA fatigue scenarios to obtain valid credentials.

The rate in which AI is changing attacker behaviour means that relying on technical defences alone is not enough. Modern phishing attempts have evolved to target the human layer and, with attackers constantly refining their methods to evade technical defences, no amount of investment into the best security tools will compensate unless zero trust strategies are embedded across the entire perimeter.

Beyond phishing, compromised credentials are widely available through underground marketplaces, often sold by initial access brokers (IAB) who specialise in harvesting and monetising identity data. In many cases, the attacker launching a ransomware or data theft campaign did not steal the credentials themselves; they simply bought access. At the same time, around three-quarters of organisations report that credential leak risk is increasing, reinforcing why identity has become such a lucrative attack surface.

IAB is lowering the barriers for cyber crime massively. In the past, attackers often operated in isolated settings and had to rely on brute-force methods to gain access to networks. Today, they can simply buy their way in and scale their operations more easily. With the technical element of the attack outsourced, lower-skill attackers can focus their efforts on social engineering and deepfake fraud, further refining the human element of their attack.

Identity-based attacks also short-circuit the traditional cyber kill chain. Instead of moving step by step through reconnaissance, exploitation and lateral movement, attackers can log in directly using a legitimate identity. At that point, the activity may look indistinguishable from normal user behaviour unless the right controls are in place.

AROUND THREE-QUARTERS OF ORGANISATIONS REPORT THAT CREDENTIAL LEAK RISK IS INCREASING

Even low-privilege accounts can provide a foothold. Once inside, attackers can probe for misconfigurations, exploit privilege creep and move laterally towards more sensitive systems. This makes identity governance and access hygiene just as important as perimeter defences.

For organisations, the goal is not only to keep attackers outside the perimeter but also to contain their reach if they do slip through technical barriers. Once an attacker has logged in, they have already bypassed the first layer of defence. However, zero trust and least-privilege access limit the radius of their attack and create additional internal barriers. Without these frameworks in place, organisations are leaving the door wide open for attackers.

Resilience depends on how quickly organisations are able to spot suspicious network activity such as impossible logins, mass downloads and authorised data transfers. Technical tools must lock compromised credentials instantly, while being supported by internal governance that provides clear paths for reset and escalation.

Given that the average breach takes 241 days to identify and contain, and 76 percent of organisations take more than 100 days to fully recover, having the right cybersecurity strategy is no longer optional – it is vital for business continuity.

As identity-based attacks surge, organisations are right to enforce security controls for high-value users such as administrators, IT teams, finance leaders and C-suite executives. However, focusing on VIP users first and foremost creates a significant blind spot.

This 'VIP-first' approach is a tactic attackers rely on because when security attention is concentrated at the top, it diverts focus away from other users within the organisation.

From an attacker's perspective, any identity is a win. For example, a temporary worker's account may have limited access to data, but if that account lacks MFA or relies on a shared password while the organisation focuses primarily on VIP users, it becomes a prime target.

By exploiting users who are less security-aware and rarely monitored, attackers can slip past defences and breach networks quietly without raising alarm bells.

The real risk comes when attackers use their initial access to probe deeper into business systems and harvest additional data. On the surface, this data might not appear overly sensitive, but to an attacker it can be an invaluable asset that provides context for more convincing social engineering and spear-phishing campaigns.

FROM AN ATTACKER'S PERSPECTIVE, IDENTITY OFFERS THE FASTEST ROUTE TO VALUE

It is not enough for organisations to enforce strong security controls only for VIP users. Attackers view every identity within an organisation as a potential entry point, which means every user must effectively be treated as a VIP when it comes to identity protection and security controls.

This shift towards identity also reflects a broader evolution in security thinking. Traditional vulnerability management focuses on patching known flaws across infrastructure. While still important, it does not fully capture how attackers actually operate in modern environments.

Exposure management takes a wider view. It examines identities, cloud configurations, external-facing assets and connectivity between systems to understand how an attacker could realistically move through an organisation.

From an identity perspective, this means examining privilege paths, dormant accounts, excessive permissions and weak authentication flows. The goal is not to eliminate every single possible vulnerability, but to reduce what is genuinely exploitable and relevant to the organisation's real risk profile.

High-profile attacks on critical UK infrastructure demonstrate that a compromised identity is not simply a back-office IT issue for security teams to manage. It has become a fundamental risk to business continuity. When systems go down because an identity has been exploited, the impact is felt across workflows, halting transactions, freezing services and damaging customer trust.

For security partners, integrators and managed service providers, the rise of identity-based attacks represents both responsibility and opportunity. Customers increasingly recognise that point products alone will not resolve systemic identity risk. They need guidance, roadmap-driven change and ongoing operational support.

This is where a shift from reactive security strategies towards broader exposure management becomes a key differentiator. While traditional scan-patch-repeat approaches have been effective in the past, today's threat landscape is evolving rapidly. With attackers constantly adapting their tactics, organisations and their technology partners must take a more proactive view of risk.

Exposure management encourages organisations to think like an attacker by analysing the full attack surface and identifying realistic attack paths. By understanding what is genuinely exploitable and critical for business continuity, organisations can prioritise closing the most significant security gaps rather than simply working through generic vulnerability lists. Identity-first security cannot be installed and forgotten. Zero trust is a framework rather than a product, and progressing towards it requires a staged transformation across people, processes and technology.

Partners that can assess identity exposure, define risk-based roadmaps and deliver managed identity and access services will be best positioned to differentiate. Many organisations already have capable identity platforms in place, but lack the skills and operational capacity to configure, govern and monitor them effectively. As identity becomes the new perimeter, security partners and integrators have a critical role to play in helping UK organisations reduce exposure, limit the impact of breaches and build lasting cyber resilience ●

James Gillies is Head of Cyber Security at Logicalis UK&I.

Some organisations are neglecting basic principles, such as weak passwords and sharing login details