TIEVA



Microsoft Digital Defense Report 2026:

Podcast Highlights & Insights



Microsoft Digital Defense Report 2026

A practical briefing for IT leaders in mid-sized UK organisations

Microsoft's annual Digital Defense Report examines developments in cyber threats and how organisations can strengthen their defences. It draws on Microsoft's global security observations and research, covering AI, the threat landscape, cybercrime and resilience. The 2026 edition explores how attackers exploit the identities, systems and trusted relationships that organisations depend on.

For IT leaders, the task is to decide what these findings mean for the systems they run, the information they protect and the services the business needs to keep operating. That includes judging where existing controls need strengthening and how responsibilities are shared with technology providers.

This briefing brings together six themes explored by TIEVA cybersecurity consultant Dominic Mounsey in our podcast about the report. It explains their practical implications and provides questions to help you review your own organisation's position, whether you've listened to the episode or are reading this independently. It closes with Dominic's three priorities: phishing-resistant multifactor authentication (MFA), a rehearsed incident response plan and stronger AI governance.



1. AI increases the pressure on familiar weaknesses

AI lets attackers automate work and run activities in parallel, increasing the pressure on IT teams to close weaknesses quickly. Microsoft distinguishes laboratory demonstrations from emerging autonomous attacks in the real world, where volumes remain low. We should prepare for greater speed and scale without assuming every attack is already autonomous.

Our starting point is your existing exposure. How quickly can you fix a vulnerable system, including services managed by suppliers? Where patching has to wait, agree how access will be restricted or the system isolated, and who owns the remaining risk.

Start with employee-led adoption too. Shadow AI includes staff putting corporate data into unvetted SaaS AI tools or connecting them to work accounts. Establish what is being used and provide approved alternatives. For agents, check what they can reach and limit permissions to the task. AI governance needs to cover everyday tool use as well as formal deployments.

Discuss internally: Do we know which AI tools staff use, what corporate data they receive and which systems or permissions they can access?

Report reference: pp. 75–77.



2. Familiar requests still need verification

A request can look like ordinary work and still be malicious. Microsoft found an impersonation signal in nearly 85% of reported phishing emails in April–June 2026. This concerns reported phishing, not all email or the proportion generated by AI. Familiar branding and plausible context are an unreliable basis for trust.

We recommend building verification into sensitive workflows. Staff handling payment changes, account resets or remote access requests need an independent way to confirm them, using contact details already held. Make that process easy to use under pressure and include outsourced IT support. Relying on people to spot every convincing fake leaves too much to chance.

Discuss internally: Could someone verify an unexpected support or payment request without using contact details supplied in that request?

Report reference: p. 49.



3. Review what happens after sign in

A compromised account can open a route to shared files, application credentials and administrative access. Look beyond sign-in: what can that identity reach, and what would stop an attacker gaining more access? Include people, applications and automated services.

MFA remains essential. One-time codes and approval prompts can still be targeted through phishing or social engineering, so we recommend working towards phishing-resistant methods such as FIDO2 security keys, Windows Hello for Business and passkeys.

Passkeys work with the legitimate service rather than a lookalike phishing site. They may be device-bound or synced through a provider. Choose according to user risk and support needs, alongside secure devices, recovery and session controls.

Check enforced methods, exceptions and recovery routes. Legacy line-of-business applications may not support passkeys or hardware keys directly. Test compatibility and sign-in integration before rollout; agree interim controls and a remediation plan where gaps remain. Prioritise privileged access without leaving other users unprotected.

Review remote management software too. Tools used legitimately by your team or suppliers can also give an attacker persistent access. Know which are authorised and investigate unexpected installations.

Discuss internally: Which legacy business applications could obstruct a passkey or hardware-key rollout, and how will we protect access while resolving compatibility gaps?

Report reference: pp. 63–65 and 69.



4. Criminal services shorten the route to business harm

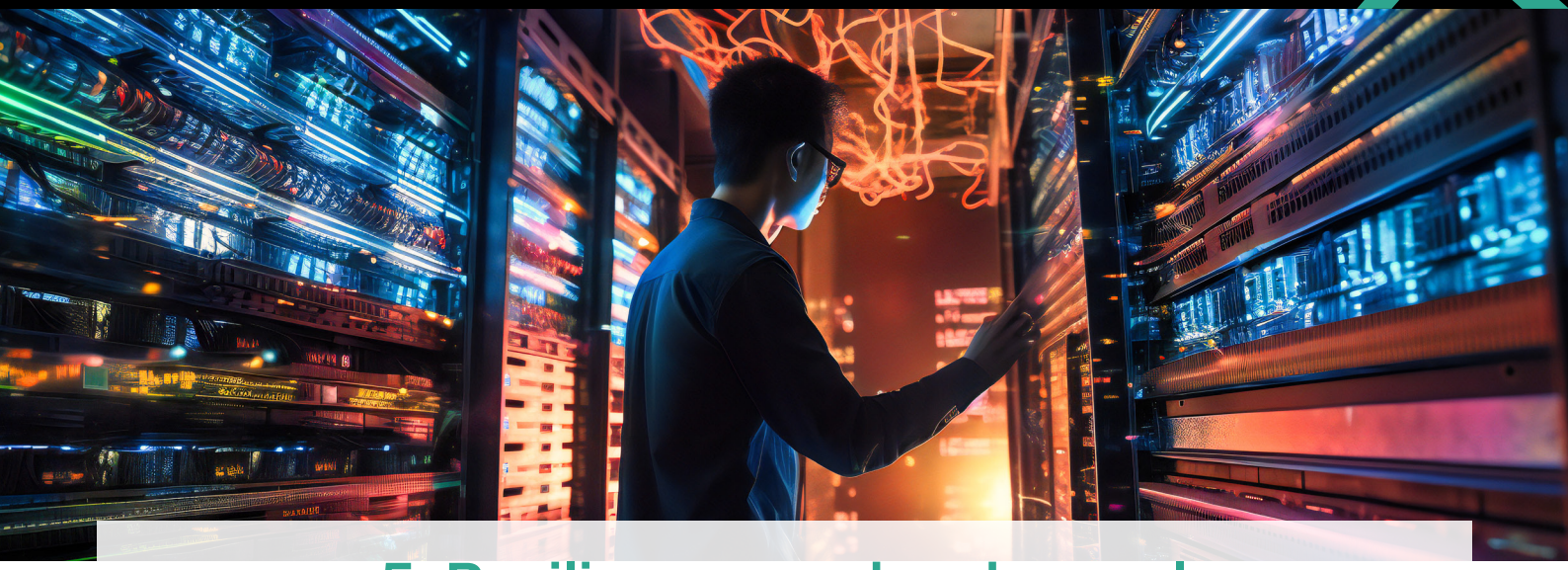
Criminal services make it easier for attackers to acquire capabilities they have not developed themselves. Microsoft describes ransomware services that package tools, infrastructure and support for affiliates. We need to plan for capable attacks even when the person initiating them has limited technical expertise.

For IT leaders, the response is to make it harder to turn an initial foothold into wider access and business damage. Assume that a stolen account may be followed by attempts to reach more valuable information or install tools that preserve access. Detection and containment need to work before the attacker reaches those objectives.

Extortion can involve publishing stolen data even when systems remain available. Plan for data theft alongside recovery. Under UK GDPR, a controller must notify the ICO of a personal data breach unless it is unlikely to result in a risk to individuals' rights and freedoms: without undue delay and, where feasible, within 72 hours of becoming aware. High-risk breaches also require informing affected individuals without undue delay. Assess and record notification decisions; ransomware that makes personal data unavailable can also be reportable.

Discuss internally: If personal data were stolen, who would assess notification obligations, gather evidence a

Report reference: pp. 75–77.



5. Resilience needs rehearsal

Criminal services make it easier for attackers to acquire capabilities they have not developed themselves. Microsoft describes ransomware services that package tools, infrastructure and support for affiliates. We need to plan for capable attacks even when the person initiating them has limited technical expertise.

For IT leaders, the response is to make it harder to turn an initial foothold into wider access and business damage. Assume that a stolen account may be followed by attempts to reach more valuable information or install tools that preserve access. Detection and containment need to work before the attacker reaches those objectives.

Extortion can involve publishing stolen data even when systems remain available. Plan for data theft alongside recovery. Under UK GDPR, a controller must notify the ICO of a personal data breach unless it is unlikely to result in a risk to individuals' rights and freedoms: without undue delay and, where feasible, within 72 hours of becoming aware. High-risk breaches also require informing affected individuals without undue delay. Assess and record notification decisions; ransomware that makes personal data unavailable can also be reportable.

Discuss internally: If personal data were stolen, who would assess notification obligations, gather evidence a

Report reference: pp. 75–77.

TIEVA

Email TIEVA
hello@tieva.co.uk

Call TIEVA
+44(0)333 0430 333

tieva.co.uk