Two-thirds of enterprises delay Microsoft Copilot over concerns AI could expose confidential SharePoint data

CoreView logo

WASHINGTON D.C., DC, UNITED STATES, July 21, 2026 /EINPresswire.com/ -- Two-thirds (66%) of enterprises have delayed or cancelled Microsoft Copilot deployments over concerns AI could expose confidential SharePoint data, according to new research from CoreView. Nearly three-quarters (73%) are concerned AI is already surfacing sensitive information internally, while organisations delaying Copilot are more than three times as likely to be highly concerned about anonymous SharePoint links than those that have already deployed it (48% versus 14%).

CoreView's State of Microsoft 365 Security and Governance 2026 report reveals exactly why that hesitation exists:

1.) Senior leaders are more likely to delay Copilot deployment

Concern about AI rises with organisational seniority. Three-quarters (75%) of C-level executives and vice presidents have delayed or cancelled Copilot deployments, compared with 60% of managers. The people with the broadest view of the organisation and the clearest view of risk across legal, compliance, finance, and HR conversations are the most likely to have paused their Copilot deployment.

2.) Most organisations overestimate their Microsoft 365 security environment

Nearly two-thirds (62%) rate their Microsoft 365 security as "established" or "advanced". Yet more than half (54%) of those organisations are still missing at least one foundational security control, including administrator MFA, privileged access management or configuration tamper detection. Copilot surfaces only what it can access, and an organisation that overestimates its own security has no true idea of what that is.

3.) The accounts most capable of controlling what AI can reach are the least protected

Administrator accounts, which can alter permissions, configurations, and access controls across the entire Microsoft 365 environment, are less likely to have fully enforced MFA than standard user accounts (55% versus 62%). One in five organisations enforces MFA more weakly on admin accounts than on everyday employees. These are precisely the accounts that determine what Copilot will find.

4.) More than one-third believe Microsoft is protecting something it definitely is not

More than one-third (37%) of respondents incorrectly believe Microsoft automatically backs up Microsoft 365 configurations, while a further 11% admit they have no configuration backup at all. An organisation that does not own its configuration baseline has no authoritative record of how permissions, sharing settings, and access controls are actually set, and no reliable way to know what AI will surface.

5.) The process most needed to clean up SharePoint before AI deployment is the one most consistently failing

Nearly two-thirds (63%) of organisations defer or limit user access reviews because they are too time-consuming, while almost half (46%) struggle to get employees to complete them. As Microsoft 365 environments continue to grow, organisations are finding it increasingly difficult to manage governance through manual processes alone, making it harder to maintain least-privilege access and prepare their environments for AI.

Simon Azzopardi, Chief Executive Officer, CoreView said: "Two-thirds of enterprises have delayed or cancelled Copilot. It is the most senior leaders who are pausing, because they can see exactly what AI will surface - a decade of sharing links and permissions nobody cleaned up. The risk was always there but AI has made it visible and urgent. We built CoreView Control for SharePoint for precisely this moment - continuous file-level visibility and remediation, below the site level where Microsoft's native controls stop by design. When you fix the SharePoint estate, Copilot stops being a board-level risk and becomes a productivity decision."

ENDS

About CoreView
CoreView delivers cyber resilience that treats Microsoft 365 as the uniquely critical and sensitive environment it is. Whether operating multiple tenants with on-premises environments or consolidating to a single tenant, CoreView provides enterprise-grade cyber resilience, simplifies and automates M365 administration, and identifies wasted spend in your tenant. CoreView empowers over 4,000 organizations – including some of the world’s largest Microsoft tenants – to secure, consolidate, and manage complex Microsoft 365 environments.

About the research

The report is based on a survey of 279 IT, security, and infrastructure decision-makers at organizations using Microsoft 365. Respondents are concentrated in North America (86% USA, 7% Canada), with representation from the UK, Australia, and continental Europe. By industry, the base is led by Technology/Software (28%), Healthcare (19%), Finance/Banking (14%), Manufacturing (12%), and State, Local, and Education (9%).

Coreview Press Office
CoreView
coreview@3thinkrs.com
Visit us on social media:
LinkedIn
YouTube
