Everyday Cybersecurity

for the Modern Workplace

Navigating the Threat Landscape in the Microsoft 365 Era

Logivate

Gift Amukhoye | Cybersecurity Consultant

Webinar Agenda

Logivate

01

The Threat Landscape

Who is attacking & how they get in

02

Business Risk

The cost & the boardroom framing

03

Identity Governance

The new security perimeter

04

Data Governance & AI

The AI amplification effect

05

User Best Practices

Five habits everyone must adopt

06

90-Day Action Plan + Q&A

Concrete next steps by audience segment

The Numbers Don't Lie — The 2025/2026 Threat Reality

Logivate

These are not predictions. This is what happened to organisations just like yours over the past 12 months.

32%

Rise in identity-based attacks

Recorded in just the first half of 2025

$4.88M

Average cost of a single breach

Up significantly from the year prior

54%

AI-powered phishing click-through rate

Up from 12% — a 4.5× increase

Sources: Microsoft Digital Defense Report 2025 | Verizon DBIR 2025

Logivate

The Threat Landscape

Who is attacking, why, and how they get in

Who Is Targeting You?

Logivate

52%

Financially Motivated Cybercriminals

Primary threat to most organisations — ransomware, BEC & data extortion
80% of incidents involved data theft or leakage in 2025
Cybercrime is industrialised — access brokers & infostealer dark web markets

Nation-State Actors

Espionage, IP theft & infrastructure disruption.
Targeting IT, government, research & academia.
Adopting AI to automate influence at scale.

Cybercrime-as-a-Service

Access brokers sell entry to thousands of organisations on the dark web
Infostealers harvest credentials & session tokens silently in the background
Lumma Stealer alone: 2,300+ malicious domains disrupted in 2025

How Attackers Get In — The Three Primary Entry Points

Logivate

AI is accelerating the speed, scale, and sophistication of every attack method below. The playbook is the same — the tools are now supercharged.

28%

Phishing & Social Engineering

AI-crafted emails achieve 4.5× higher click rates. ClickFix technique lures users into running malicious scripts. Token hijacking bypasses MFA entirely after a single click.

18%

Unpatched Assets

Active exploitation of known CVEs begins within hours of disclosure. Patch latency is a consistent, preventable contributor to breach. Prioritise the CISA KEV catalog over CVSS scores.

12%

Exposed Remote Services

VPN, RDP, SMTP AUTH and legacy protocols exposed to the internet. Device code phishing is an emerging vector targeting M365 authentication flows specifically.

Source: Microsoft Incident Response engagements — Microsoft Digital Defense Report 2025

Threats Targeting the M365 Ecosystem Specifically

Logivate

Business Email Compromise (BEC)

HIGH VOLUME

AI-crafted phishing + token hijacking bypass traditional defences. One compromised mailbox leads to fraudulent wire transfers, invoice redirection, and weeks of disruption.

Office Document Zero-Days

ACTIVE NOW

Crafted Office files exploit unpatched CVEs delivered via email. January 2026 saw an emergency out-of-band patch — attackers moved within hours of disclosure.

Cloud-Hosted Phishing Links

RISING TREND

Phishing pages hosted on SharePoint, OneDrive & Azure Blob. Your email filters trust these domains. Links shared via Teams carry implicit user trust.

Infostealer Malware & Token Theft

MFA BYPASS

Infostealers like Lumma silently harvest session tokens. Stolen tokens bypass MFA — attackers impersonate users without password or auth app. 2,300+ domains seized in 2025.

Logivate

Business Risk

What a breach actually costs — and who owns accountability

The Real Cost of a Cybersecurity Breach

Logivate

$4.88M

Average cost of a breach

↑ *Financial · Operational · Reputational* ↑

Financial Impact

Ransom payments, regulatory fines, legal fees, forensic investigation, cyber insurance claims, and stock price impact.

Operational Impact

System downtime, manual process fallback, incident response effort, and recovery timelines measured in weeks — not hours.

Reputational Impact

Client trust erosion, mandatory disclosure, competitive disadvantage, and lasting damage to partner and supplier relationships.

Source: IBM Cost of a Data Breach Report 2024 | 15.7 billion records compromised in H1 2025 alone

Cyber Risk Is a Board-Level Business Risk

Logivate

> *"Cybersecurity is no longer just an IT problem — it is a business risk with financial, operational, and reputational consequences. Alignment starts and ends in the boardroom."*

Three Questions Every Board Should Be Asking Right Now:

1. What is our MFA coverage across the organisation?

What percentage of users — especially admins and executives — have phishing-resistant MFA enforced? Any account without it is an open door.

2. What is our average patch latency for critical vulnerabilities?

How many days between a critical CVE disclosure and our environment being protected? In 2025, that window is being exploited in hours.

3. When did we last test our incident response plan?

A plan that has never been rehearsed will fail at the worst possible moment. Tabletop exercises are a governance essential, not an IT luxury.

Logivate

Identity Governance

The new security perimeter — and why it matters beyond IT

Identity Is the New Security Perimeter

Logivate

82%

of breaches involve
a compromised identity

99.9%

risk reduction when
MFA is enforced

3.8×

more likely to be breached
without PIM controls

The Privilege Creep Problem — Why Identities Accumulate Too Much Access Over Time

Joins Org

Gets base access

Gets Promoted

Gets more access

Changes Teams

Keeps old access

AI Arrives

AI inherits ALL of it

Identity Controls Every M365 Organisation Must Implement

Logivate

Phishing-Resistant MFA

SMS and phone-call MFA are being phased out by Microsoft — migrate now. Deploy FIDO2 security keys, Windows Hello for Business, or Passkeys. Never approve a prompt you didn't initiate — that's a push bombing attack.

Conditional Access Policies

Your Zero Trust policy engine in Entra ID. Enforce MFA based on user risk, sign-in risk, device compliance, and location. Critically — disable legacy auth protocols (POP/IMAP/SMTP AUTH) that bypass MFA entirely.

Privileged Identity Management (PIM)

No standing admin privileges — ever. Use just-in-time elevation that expires automatically. Admins operate from regular accounts day-to-day. 64% fewer incidents in PIM-enabled environments.

Identity Lifecycle Management

Automate joiners, movers and leavers. Day-one offboarding is as critical as day-one provisioning. Conduct access reviews in Entra ID. Remove stale guests, orphaned service accounts, and permissions that no longer match current roles.

Logivate

Data Governance & AI

Why your data hygiene determines exactly how safe your AI is

The AI Amplification Effect

Logivate

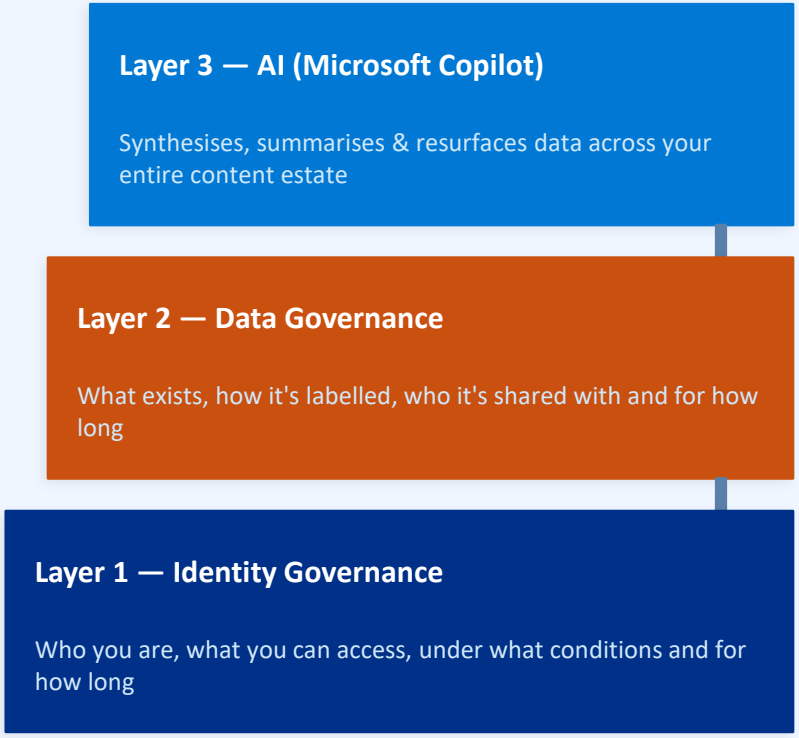
AI doesn't introduce new risks.

It surfaces and amplifies risks that already existed silently in your environment.

Privilege creep, unlabelled sensitive files, "Anyone" sharing links, forgotten guest accounts — these were dormant problems.

The moment AI enters the environment, every one of them becomes active.

> *"Deploy Copilot before fixing your governance and you haven't introduced an AI assistant — you've introduced an AI-powered data discovery engine for every user in your organisation."*



Copilot Inherits Your Permissions — Every Single One

Logivate

Copilot sees exactly what the logged-in user can see — nothing more, but critically, nothing less. A user with access to salary data, strategic plans, or HR files will have Copilot use that data in responses — even if the user would never have manually searched for it.

If This Is Broken in Your Environment...	→ AI Makes It...
Over-permissioned identities	→ An AI with unintended access to everything that identity can see
Unlabelled sensitive files	→ Invisible to data protection policies — but fully accessible to AI
'Anyone' sharing links	→ An AI that answers questions with data meant for no one
Stale guest accounts	→ An AI that can be queried via a forgotten, unmonitored identity
No DLP on Copilot prompts	→ A user who exfiltrates data accidentally just by asking a question

Research: 15%+ of business-critical files currently at risk from oversharing — Metomic / Microsoft 2025

Governing Your Data Estate in M365

Logivate

Sensitivity Labels (Microsoft Purview)

Foundation

Classify every file — Public, Internal, Confidential, Highly Confidential. Labels enforce encryption, restrict sharing, and tell Copilot what data has governance boundaries. Without labels, AI has no context. This is the non-negotiable foundation.

DLP for Copilot Prompts

AI-Specific

Block Copilot from processing files with sensitive labels. Prevent prompts from including sensitive data in web queries or AI grounding. Now generally available in Microsoft Purview. Deploy before any broad Copilot rollout.

Oversharing Remediation

Urgent Action

Run SharePoint Advanced Management (SAM) permission reports weekly. Identify and remediate 'Anyone' links, broken permission inheritance, excessive group access. Urgent pre-AI housekeeping — included in your M365 Copilot licence.

Data Lifecycle Management

Ongoing

Old data is extended attack surface. Use Purview Data Lifecycle Management to archive or delete content with no current business value. Orphaned files, stale sites, and test data with real PII are all Copilot-accessible until deliberately removed.

Logivate

User Best Practices

Five habits that apply to every single person in your organisation

Your 5 Cyber Habits — Simple, Effective, Non-Negotiable

Logivate

1

Use the Authenticator App — not SMS

SMS codes can be intercepted. Microsoft Authenticator is faster, more secure, and is the organisational standard. If your IT team offers FIDO2 keys or Windows Hello, use them — they are the most secure option available.

2

Reject MFA prompts you didn't initiate — immediately

If you receive an Authenticator notification you didn't trigger, someone is trying to break into your account. Tap Deny, then report it to IT. Approving it to 'make the notification go away' hands an attacker full access.

3

Think before you click — even in Teams and SharePoint

Attackers host phishing pages on legitimate cloud platforms. A link via Teams, email or SharePoint can still redirect you to a credential-harvesting site. Verify unexpected links before clicking, especially those asking you to sign in.

4

Share files with specific people — never 'Anyone'

'Anyone' links remove all access controls. They bypass governance, they're AI-accessible, and if forwarded, can reach unintended recipients. Always share with named individuals or defined groups.

5

Use a passphrase — and a password manager

A long simple passphrase is exponentially harder to crack than a short 'complex' password. Use a password manager to generate and store unique credentials for every account so you never reuse passwords.

Your 90-Day Action Plan — Start This Week

Logivate

Organisational Leadership

- Request a cybersecurity risk report at every board meeting — track MFA coverage & patch latency as KPIs
- Commission an M365 identity & data governance audit before expanding Copilot/AI licences
- Fund security awareness training as a cultural investment — not an IT checkbox
- Review your cyber insurance policy against current breach cost benchmarks

IT & Security Teams

- Enforce phishing-resistant MFA for ALL users — migrate off SMS and phone-call MFA methods now
- Disable legacy auth: kill POP/IMAP/SMTP AUTH and Basic Auth across Exchange Online
- Run SharePoint Advanced Management permission audit — remediate all 'Anyone' links
- Enable DSPM for AI in Purview for weekly oversharing risk assessments
- Implement PIM for all privileged roles — eliminate all standing admin access

Every Employee

- Enrol in the Microsoft Authenticator app if not already done
- Audit your own OneDrive and SharePoint shares — remove unneeded 'Anyone' links
- Complete the next phishing simulation — it's training, not a test
- Apply Purview sensitivity labels to the sensitive files you create

Start with your Microsoft Secure Score in Entra ID — your current baseline is visible right now.

Thank You

Questions & Discussion

Three things to remember from today:

- Identity and data governance are the foundation — AI inherits whatever you build
- Every person in your organisation is both a target and a line of defence
- Start with your Microsoft Secure Score — it tells you exactly where you stand today

Logivate

Gift Amukhoye | Cybersecurity Consultant | Logivate IT Consulting