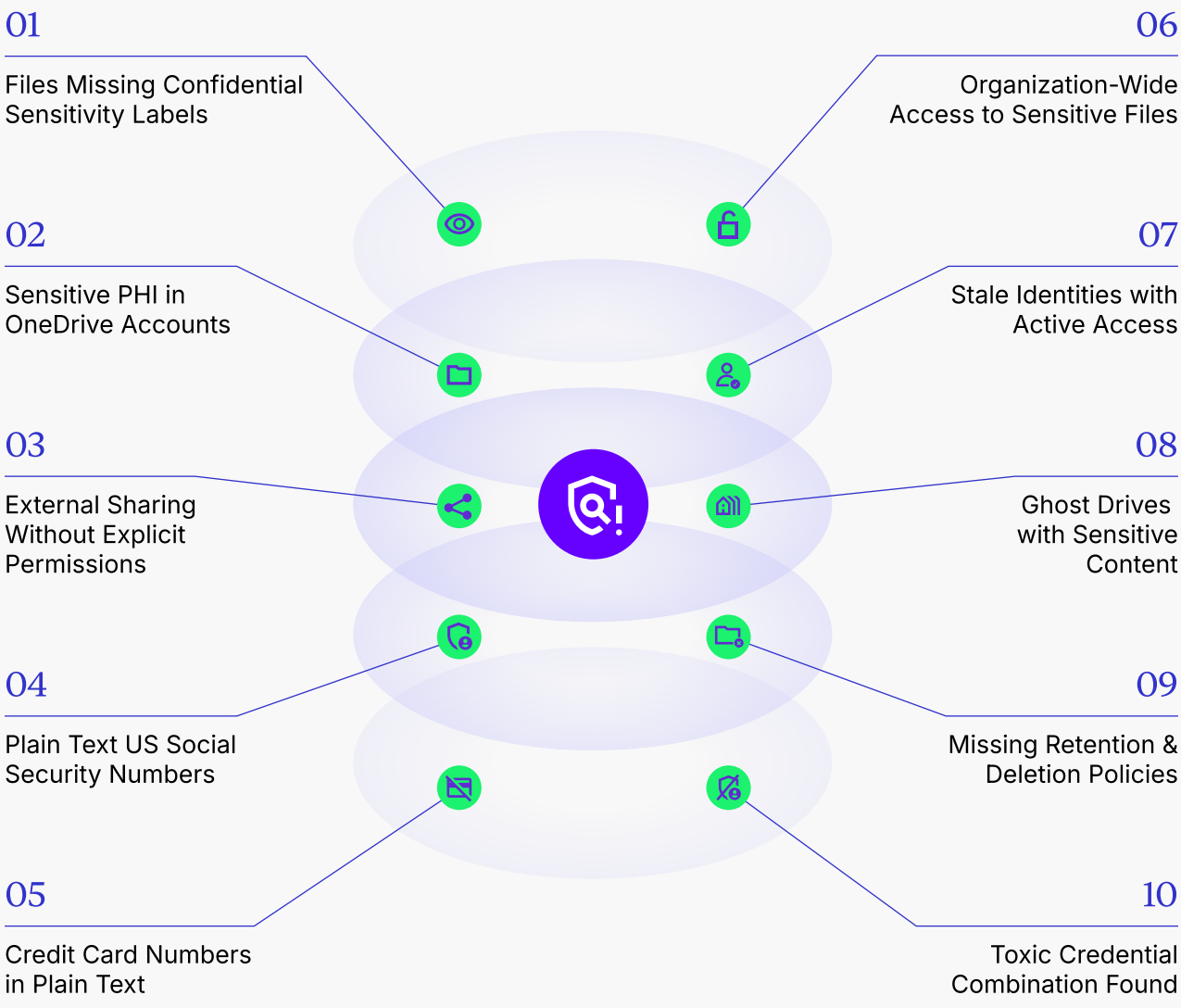
CYERA{research} LABS

# Top 10 Data Security Risks in Microsoft 365

2025 Edition

## Introduction

With over 300 million users, Microsoft 365 is essential to modern collaboration but it's also a growing surface for data exposure. Based on Cyera's 2025 analysis across enterprise environments, these are the top 10 notable Microsoft 365 risks that every CISO and data leader should actively monitor and remediate.



01

**Files Missing Confidential Sensitivity Labels**

When sensitive documents are not labeled as confidential, security policies like encryption or sharing restrictions aren't triggered. This creates a blind spot, allowing data like PI or financial records to be freely shared or accessed inappropriately violating data governance rules and compliance frameworks such as GDPR or HIPAA.

02

**Sensitive PHI in OneDrive Accounts**

Protected Health Information (PHI) was commonly found in personal OneDrive folders without proper protections. This breaks organizational policies and healthcare regulations, since personal cloud storage is rarely monitored or governed as strictly as structured enterprise systems.

03

**External Sharing Without Explicit Permissions**

Files with sensitive content were shared with external organizations that weren't explicitly authorized. This misconfiguration introduces third-party access without oversight, data leakage, intellectual property theft, and compliance violations with standards like ISO 27001.

04

**Plain Text US Social Security Numbers**

SSNs were found stored without encryption or tokenization. If a breach occurs, attackers gain full access to one of the most sensitive identifiers used for identity fraud. This lack of data protection fails PCI DSS and data privacy regulations, increasing legal and reputational exposure.

05

**Credit Card Numbers in Plain Text**

Documents containing raw credit card data were stored unprotected. This not only violates PCI DSS mandates but also enables threat actors to commit large-scale financial fraud if access is gained. Encryption and data masking are critical and clearly missing.

06

**Organization-Wide Access to Sensitive Files**

Highly sensitive files were found accessible to every employee in the organization. This "everyone" access model violates least privilege principles and increases the risk of insider leaks or accidental sharing, especially in large, distributed teams.

07

**Stale Identities with Active Access**

Former employees or unused accounts still had access to sensitive OneDrive or SharePoint files. These accounts are rarely monitored, making them prime targets for account takeover or credential stuffing attacks offering silent access to internal data.

08

**Ghost Drives with Sensitive Content**

Abandoned SharePoint or OneDrive locations from dissolved teams or past employees still stored sensitive data. These drives often fall outside of regular audits or retention policies, making them hidden vulnerabilities for data exposure or regulatory gaps.

09

**Missing Retention & Deletion Policies**

Many sensitive documents had no defined lifecycle rules resulting in long-term storage of unnecessary or outdated data. This increases storage cost, complicates audits, and raises the stakes if a breach occurs, since old data often lacks updated protection.

10

**Non-Compliance with Data Regulations**

Organizations were found to be in breach of compliance standards due to inadequate access controls, improper data classification, and poor localization enforcement. This exposes them to financial penalties, legal investigations, and erosion of customer trust.

## Conclusion

Microsoft 365 is a business enabler, but also a data risk multiplier if not governed properly. Most of these risks stem from misconfigurations or missing controls not advanced threats. With the right visibility and automation, these issues can be identified and remediated at scale.

These insights come from Cyera Research Labs based on 2025 telemetry across real-world enterprise environments.