

MS Copilot: How to Protect Data and Reduce Oversharing

Session Date: June 26, 2026

Facilitator: Tobin Conley CAE, CIP, Vice President, Client Education

Presenter: Chris Ecker, Chief Technology Officer

Duration: ~1 hour

Format: Recorded webinar with practical examples and audience Q&A

Drafted using Copilot; thoughtfully refined by one of our actual humans, Chris Ecker.

Session Description

As associations adopt Microsoft 365 Copilot, many are discovering that the real risk is not artificial intelligence itself, but existing data access practices. This session focused on helping clients understand what oversharing is, how it occurs in Microsoft 365 environments, and how to reduce risk.

Key Takeaways

1. Oversharing Happens When Access Is Too Broad

Oversharing is fundamentally a permissions issue. It occurs when files or data are accessible to more people than intended, often without the original owner realizing it. A helpful analogy shared during the session is leaving a confidential document in a shared space. It is not explicitly distributed, but anyone who comes across it can access it. Copilot simply makes content in your MS 365 tenant easier to find.

2. Copilot Uses Your Existing Permissions as Its Boundary

Copilot does not create new access or bypass security controls. Instead, it retrieves and presents information based on what a user already has permission to see across SharePoint, OneDrive, and Teams. This means that any overly broad access that already exists becomes more visible and actionable through Copilot responses.

3. Default Settings Contribute to Long-Term Risk

Many organizations adopted Microsoft 365 with default sharing configurations that prioritize ease of collaboration. In many cases, files shared through simple link-based actions default to “people in the organization.” Over time, this creates an environment where large volumes of content are broadly accessible without ongoing review or intentional governance.

4. Real-World File Sharing Creates Hidden Exposure

Everyday behaviors such as sharing files via email, Teams, or direct links can gradually expand access beyond what was originally intended. Over several years, even a small organization may accumulate hundreds or thousands of files that are accessible across the organization. This accumulation creates a large and often invisible risk surface.

5. Copilot Makes Hidden Data Easier to Discover

Copilot aggregates content across multiple sources and surfaces it through natural language queries. In practice, this means information that previously required time and effort to locate can now appear instantly in responses. While this improves productivity, it also increases the likelihood that sensitive or unintended content will surface.

6. Governance and Configuration Are Critical

Managing oversharing requires both technical configuration and organizational discipline. This includes structuring SharePoint environments appropriately, managing permissions intentionally, and avoiding large “lift and shift” migrations that carry forward outdated access models. Ongoing governance is necessary to maintain a secure environment over time.

Recommended Action Steps

✓ Assess Your Current Environment

Review how files are stored and shared across SharePoint and OneDrive. Identify how many files are accessible to broad audiences and determine whether that access is appropriate for each case.

✓ Update Sharing and Permissions Policies

Adjust tenant-level default sharing settings to reduce reliance on organization-wide access. Ensure that sharing aligns with the principle of least privilege, in which users have only the access they need.

✓ Prioritize High-Sensitivity Content

Start by reviewing access to finance, executive, and other confidential content areas. These locations typically carry the highest risk and can provide immediate impact when remediated.

✓ Educate Staff on Sharing Practices

Provide clear guidance on how to share files appropriately, including reviewing permissions before sending links. Reinforce that convenience-based sharing can create unintended exposure over time.

✓ Prepare Before Expanding Copilot Access

Conduct a focused review of permissions and data governance before assigning Copilot licenses broadly. Addressing oversharing in advance helps prevent issues from being amplified once Copilot is in use.



✓ **Establish Ongoing Governance**

Implement processes to regularly review permissions, monitor sharing activity, and maintain alignment with organizational policies. Oversharing is not a one-time fix and requires continued attention.