Governance and Security Challenges in Microsoft 365

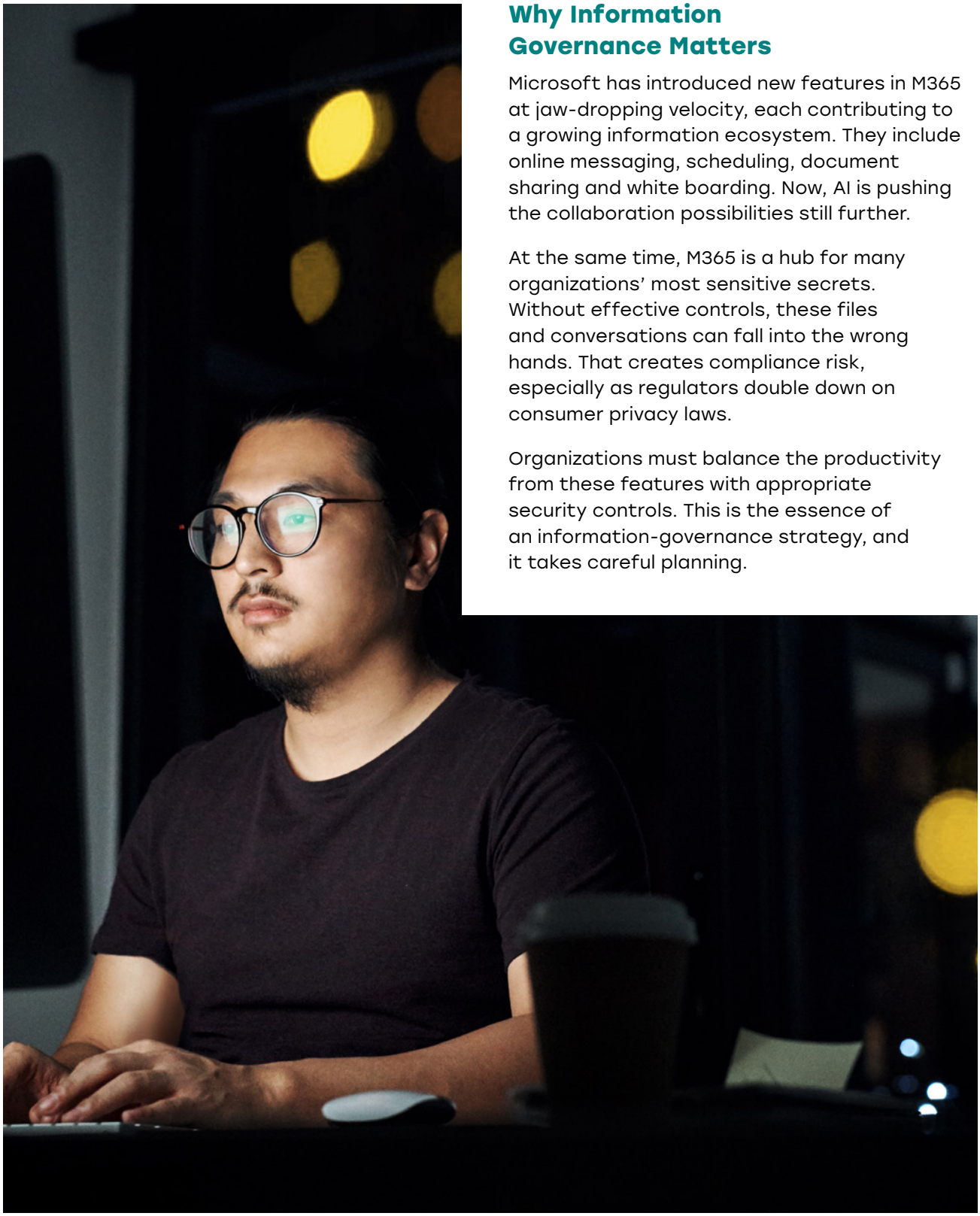
Microsoft Office first shipped in 1990, seven months before the first webpage appeared. Back then, everything happened on the user's PC.

Thirty-five years later, the world is a very different place. The suite's successor, Microsoft 365 (M365), bakes deep cross-team collaboration into the everyday user experience.

This increased productivity has created new challenges. Most people are unprepared for the security risks associated with seamless information sharing. They need frameworks for balancing security and productivity. This e-book explains how careful planning and judicious use of assistive technology can protect M365 users with digital guardrails.

In collaboration with

WeActis by Mondata



Why Information Governance Matters

Microsoft has introduced new features in M365 at jaw-dropping velocity, each contributing to a growing information ecosystem. They include online messaging, scheduling, document sharing and white boarding. Now, AI is pushing the collaboration possibilities still further.

At the same time, M365 is a hub for many organizations' most sensitive secrets. Without effective controls, these files and conversations can fall into the wrong hands. That creates compliance risk, especially as regulators double down on consumer privacy laws.

Organizations must balance the productivity from these features with appropriate security controls. This is the essence of an information-governance strategy, and it takes careful planning.

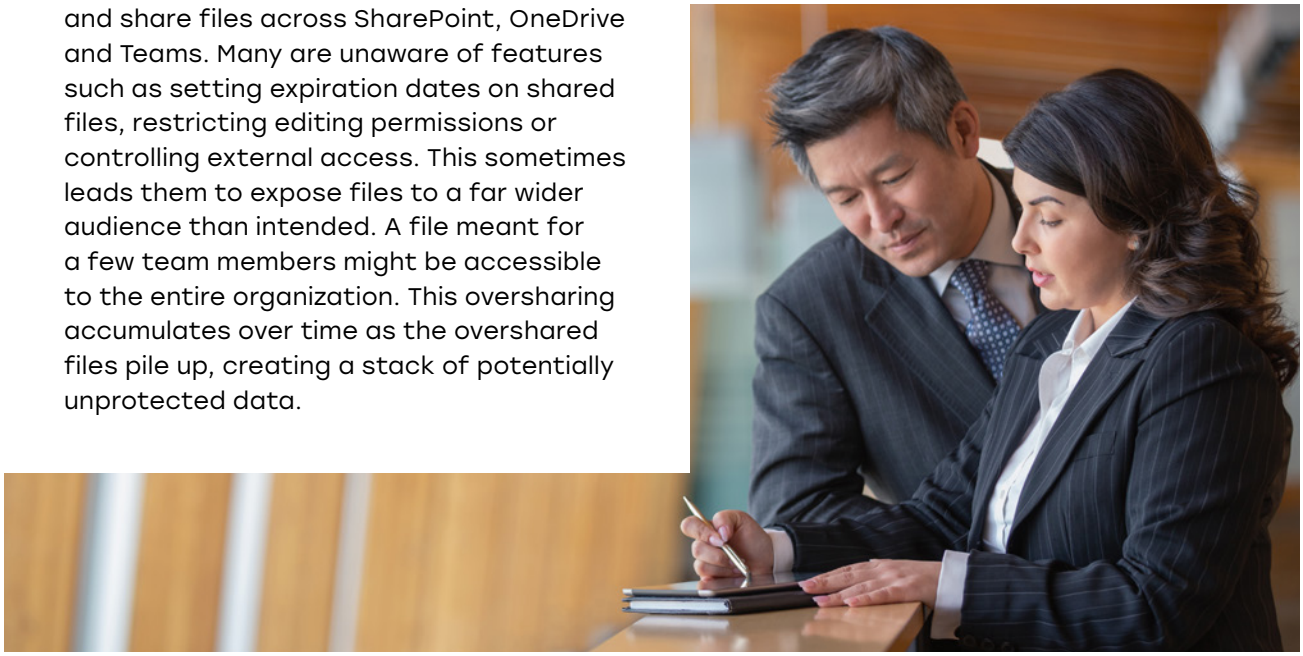
Productivity vs. Security in Microsoft 365

Balancing productivity and security is a risky business in itself. Make the security controls too permissive, and you could leak data. Make them too strict, and you risk users bypassing policies to stay productive and get their jobs done. That could create a shadow IT problem.

Companies cannot rely on Microsoft to balance productivity and security for them. M365's features focus heavily on information sharing and less on risk management. Default settings cannot perfectly balance productivity and security because each organization's needs are different, affected by factors ranging from industry sector to geographical jurisdiction to company size. Each organization has to find its own risk profile and set the security controls appropriately.

In finding this delicate balance, companies must overcome several common gaps in information governance:

- **Collaboration overload:** Users are prone to overshare information in M365 because the platform allows them to quickly create and share files across SharePoint, OneDrive and Teams. Many are unaware of features such as setting expiration dates on shared files, restricting editing permissions or controlling external access. This sometimes leads them to expose files to a far wider audience than intended. A file meant for a few team members might be accessible to the entire organization. This oversharing accumulates over time as the overshared files pile up, creating a stack of potentially unprotected data.
- **Information sprawl:** M365 makes creating SharePoint sites and sharing documents easy, but it doesn't mandate managing or deleting them, and there is no easy way to get a clear overview of all the shares. The number of unmanaged sites and document shares expands over time, and many of these won't have expiration dates.
- **Lack of data classification:** Many companies don't have a data-classification framework to help manage data based on its sensitivity at the outset. Neither do they have the skills to implement one.
- **Inadequate of user education:** Users are frequently uneducated on day-to-day data handling. Where user awareness training is offered, it is often infrequent, meaning that users don't translate it into everyday behavior.
- **Blame culture:** A culture where users are blamed for policy violations makes them nervous about self-reporting. It creates the same kind of adversarial relationships found with fake phishing exercises designed to test user awareness.

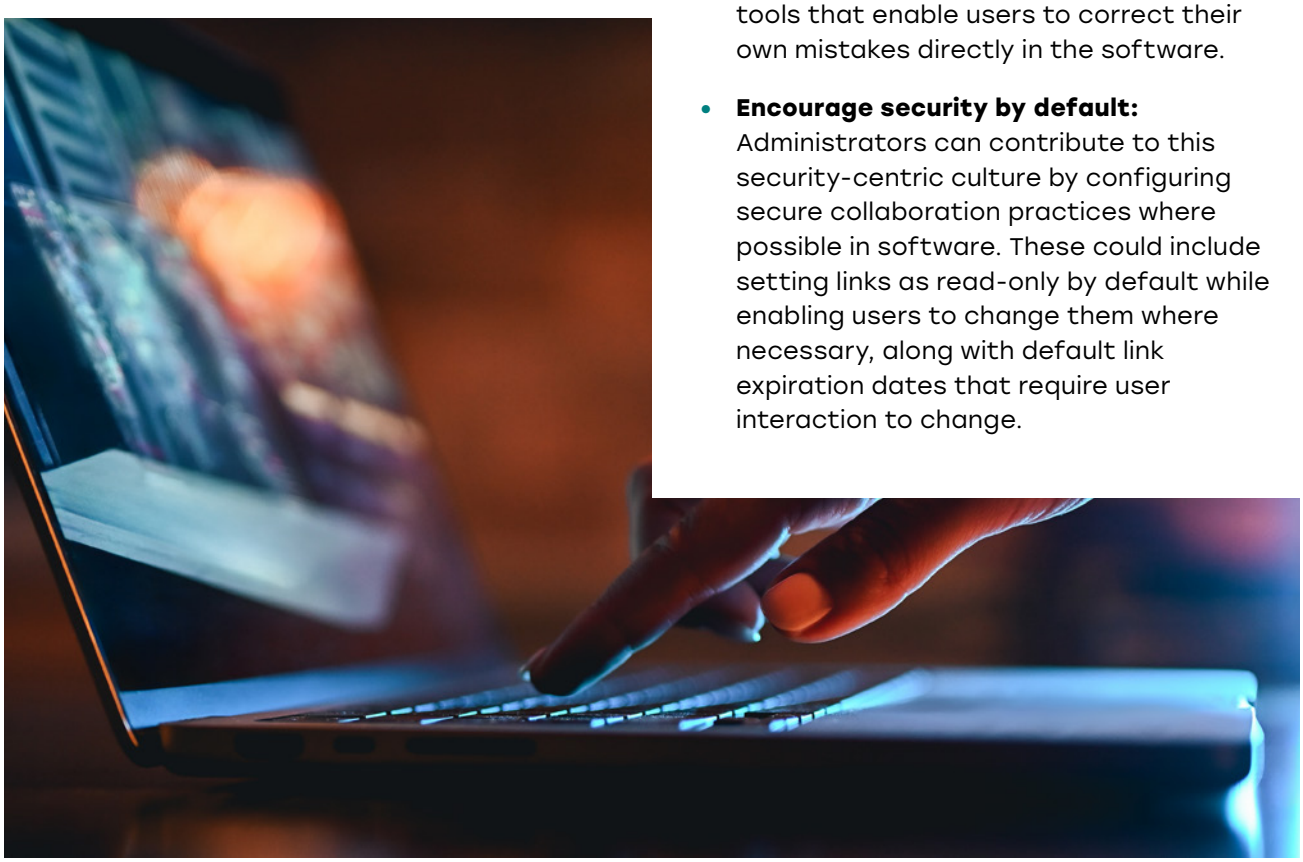


A Shift in Cybersecurity Approach

To bridge governance gaps like these, companies must change the way they think about information security and the role employees play.

Administrators can avoid many information-sharing and access problems by ensuring that users have the right permissions. They can routinely monitor privileges to ensure they're appropriate for user roles and revoke excessive permissions.

Beyond this, organizations must rethink their perceptions of users. Rather than dismissing them as part of the problem when it comes to information governance, it's time to view them as part of the solution. This means creating a collaborative culture of collective risk management in which users share responsibility for risk.



Nurturing a culture of security and collective risk management involves making several changes:

- **Empower users:** Involve users in making risk decisions about the information they're sharing.
- **Reduce friction:** Make it easy for users to follow best practices for secure information sharing at the point of sharing. Consider using tools that encourage behavioral change (see sidebar).
- **Reward, don't punish:** Rather than punishing users for their mistakes, reward them for positive action. Gamification is a powerful tool to help people celebrate their successes, but be careful that you don't use it to shame failures.
- **Focus on learning from mistakes:** Better still, use low-friction, secure collaboration tools that enable users to correct their own mistakes directly in the software.
- **Encourage security by default:** Administrators can contribute to this security-centric culture by configuring secure collaboration practices where possible in software. These could include setting links as read-only by default while enabling users to change them where necessary, along with default link expiration dates that require user interaction to change.

The AI Factor: How and Why To Govern AI and Microsoft 365 Copilot

AI has become so ubiquitous in M365 that in January 2025, Microsoft renamed the suite to Microsoft 365 Copilot. Implementing that technology brings powerful new features, particularly in areas such as information discovery. These features also carry potential risks.

How AI amplifies information risk

M365 Copilot's heavy reliance on graph data and semantic search makes it a powerful information-finding tool. It can surface data a user didn't realize they had access to based on their membership to different teams, and their relationships with others. Its ability to search for meaning within unstructured documents further advances its capabilities to find sensitive data, such as financial documents or HR records. That opens up a vast array of old, sensitive shares to inadvertent discovery.

Without effective governance, the potential for data leakage grows in line with this new functionality, making it all the more important to explore risks tied to broad misconfigurations, such as access across the entire organization.

Foundations for safe AI adoption

Like most enabling technologies, AI can be either a liability or an asset. With the right governance measures (see sidebar), it can help to supercharge productivity. The far-reaching nature of this technology requires guidance from senior leadership in its implementation.

Checklist: Your Guide to Fast-Start Governance Actions

Information governance can be daunting, but breaking it down to its constituent parts can make it more manageable. Consider the following steps in your strategy:

- **Risk management:** Align your compliance needs with your organization-specific risk management needs under a single, unifying information-governance strategy.
- **Build an information inventory:** Inventory current shares, and identify sensitive data.
- **Define policies:** Validate correct policies in areas including access and link expiration, data classification, and automated policy enforcement. Scale these policies in line with the volume and sensitivity of the data they protect.
- **Introduce collective risk practices:** With policies in place, begin to share responsibility for information governance across departments.
- **Build secure collaboration mechanisms:** Establish high-impact, low-friction user training at the point of risk for secure collaboration.
- **Adopt AI in stages:** With a strong governance-focused strategy for AI, begin a phased approach to adopting the technology in M365.
- **Monitor and improve:** Finally, create a culture of continuous improvement through regular evaluations and user-centric adjustments. Choose appropriate metrics to measure behavioral change.

What's next?

Microsoft 365's collaborative strengths can easily become liabilities without the proper governance measures. Effective governance must embrace people as a critical part of the security culture. That works best when those people receive contextually appropriate prompts to do the right thing, rather than penalties for making mistakes.

Organizations planning to take advantage of AI in M365 must implement a governance regime early, because this technology will magnify configuration gaps in the software. Many organizations won't even know their users have started using AI, so they will already be behind the curve.

Talk to WeActis today for a demonstration of how it can help you to strengthen your data hygiene in M365, de-risk AI adoption and protect your organization by empowering employees to adopt safe behaviors. Learn about WeActis features, such as positive nudges to encourage secure behavior, automated tagging of potentially risky shares and sensitive-data removal.

What behavior-driven security looks like in practice:

A chief financial officer accidentally shares a salary spreadsheet containing all employees' sensitive compensation details. He forgets to limit access to the HR department, instead allowing anyone with the link to view the data. The widespread leak causes a drop in morale and HR headaches.

A behavioral information security tool could have reminded the CFO to limit sharing permissions to specific people and to set an auto-expiry on the link.

The Importance of Behavior-Driven Security Programs

Behavior-driven security programs help to engage users at the point of risk for positive security outcomes. Here's how it works:

- **Context is key:** Behavior-driven security uses contextual nudges and micro-interventions at the point of risk. These include messages reminding you to set expiration policies.
- **Policy is baked in:** Delivering these messages and suggestions lets you enforce security policies in context, adapting to specific business scenarios while making the process easier on users.
- **Better metrics:** Collecting more meaningful behavioral metrics, such as the number of revoked links, or per-user engagement, provides a richer picture of performance than simply measuring click rates via fake phishing tests.

WeActis
by Mondata

About WeActis

WeActis revolutionizes cybersecurity by turning employees into active defenders and making security a shared responsibility rather than an IT burden. Integrated into Microsoft Teams, it seamlessly embeds security into daily workflows, guiding employees to mitigate risks in under five minutes per week. By improving data hygiene in Microsoft 365, strengthening governance, and streamlining risk reduction, WeActis helps organizations build a Cybersecurity Resilience Culture—enhancing compliance, reducing data exposure, and driving measurable, lasting security improvements.

WeActis.com | info@weactis.com | 1-833-666-3282