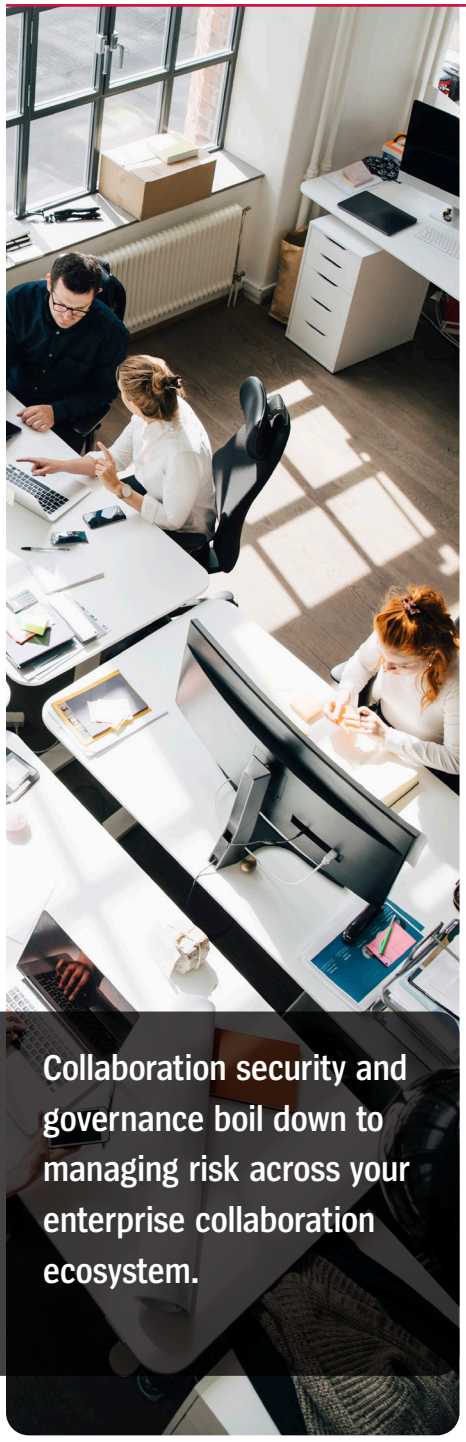
UNISYS

The Secret Buffer to an Economic Downturn? Collaboration Platform Governance

By Alan Shen



Two and a half years after the onset of the COVID-19 pandemic, we again face uncertainty with record-high inflation and a daunting economic forecast. Companies with hybrid or remote workforces are challenged to optimize their existing employees and fast-track productivity amid this tumultuous landscape. Forward-thinking organizations are tackling a heavily neglected area within the digital workplace as one buffer against the economic downturn: collaboration governance.

The collaboration governance challenge can be divided into two areas. The first is stopping and shrinking digital sprawl — referring to the staggering amount of data and documents businesses produce every day. Daily, workers waste hours searching for or duplicating existing work that is impossible to find amid uncontrolled workspaces, impacting both employee efficiency and retention. The right collaboration governance strategy can control and minimize digital sprawl, freeing up your team for high-value projects.

The second challenge is instituting strong yet flexible governance policies that do not hinder productivity. When first adopting a collaboration platform, enterprises often enact the strictest collaboration governance settings to ensure tight data security. After users push back when these excessive security measures hinder their ability to work, companies may select more relaxed native collaboration governance policies. This can open them up to security vulnerabilities. Some organizations have embraced bespoke collaboration governance policies provided by collaboration monitoring tools to strike a balance between securing enterprise data and facilitating the highest levels of workforce productivity.

Now more than ever, companies can no longer afford to operate without a solid collaboration governance strategy fueling their digital workplaces. Below, you'll find the key elements of collaboration governance and how they enable a more productive and positive end-user experience.

Tackling Digital Sprawl

While having many teams and channels working within your collaboration tool may not sound like a significant problem, digital sprawl can quickly snowball into a major security threat and productivity roadblock. Too many workspaces impact productivity as end users struggle to find the correct materials. Even worse, they may abandon their search and recreate an existing file, wasting hours of effort that could have been spent supporting other business outcomes.

A properly governed file-sharing environment, such as SharePoint, can save workers from hunting down historical documents and resources hidden throughout an organization's labyrinth of files. Even more gains can be found when valuable files left behind by prior employees are instantly identifiable, preventing the duplication of work by newer colleagues.

Risk can originate from several points within an enterprise collaboration platform, including files, chat streams, comments and meeting transcripts.

On the flip side, abandoned teams and channels also contribute to digital sprawl. Little oversight of these forgotten workspaces increases security risk, with seemingly lost data still accessible to many. Organizations can discourage data theft simply by containing their digital sprawl.

With uncontrolled workspaces leading to employee frustration and enterprise-level vulnerabilities, it's important for IT teams to get a better handle on governing digital sprawl by:

- **Setting permissions on who can create teams or channels**: Defining who can create workspaces nips the sprawl problem in the bud. Some organizations add a step in the workspace creation process by requiring IT's approval, preventing the proliferation of unnecessary teams and ensuring new teams are appropriately configured.
- **Performing workspace audits**: Even if a team or channel starts out as necessary, there is no guarantee it will be needed in the future. To prevent file-sharing sites and teams from spiraling out of control, enterprises should audit workspaces frequently to ensure they still provide value. Likewise, unused workspaces should be reviewed to decide if they should be archived or deleted, depending on your organization's data retention policy. Some organizations choose to have all teams and channels undergo a scheduled renewal process, while others simply review those that are inactive. To save time, organizations can leverage collaboration platform governance tools that flag unused or duplicate teams, streamlining the audit process.

Gaining control of your sprawling enterprise collaboration and file-sharing systems can significantly impact your team's productivity. With a few extra tools, you can optimize your digital workplace and employee experience, all while ensuring data security.

Navigating and Securing Workspaces

When grappling with enacting the right level of collaboration governance policies, it can be difficult to balance your employees' access demands with strong data security requirements. Governance policies for workspace configuration help ensure your collaboration platform applies the necessary levels of security in addition to the consistent organization of teams and channels. Here are key settings to consider adopting to prevent digital sprawl and strengthen governance:

- **Workspace naming conventions**: Enforce proper naming conventions to make it easier for end users to find the suitable workspace and to know whether guests are in a group. Standard methods include adding a prefix or suffix to denote an external-facing workspace or incorporating location or department names.
- **Minimum and maximum number of owners**: Each team has designated owners who control basic settings and oversee workspace activity. Given the importance of this role, companies should set policies to ensure a workspace has at least two owners. It's also important to prevent an excessive number of owners, as no one may step up to actively oversee the workspace.
- **Workspace classification**: Beyond configuring a workspace as private or public, classification denotes the sensitivity level of the data accessible to team members. Workspace classification can be based on team membership, expected topics of discussion and shared content types. For instance, teams classified as highly sensitive may restrict external guests, such as partners or customers.

Alan Shen
Chief Technology Officer,
Unisys Digital Workplace Solutions

Alan drives technical strategy and thought leadership across Digital Workplace Solutions. Building on his former role as head of Unify Square consulting and on his leadership in introducing key AI/ML technologies into Unisys' PowerSuite Management and Security Suite, Alan brings a wealth of customer experience to bear as he steers ongoing technology investments across the company's consulting, SaaS and managed services offerings.

He can be reached at
alan.shen@unisys.com

Exploring the Complexity of Guest Access

While it may sound simple, guest access is one of the most complex collaboration security issues. Employees might invite external guests to a team workspace, not realizing they have indirectly given that guest user access to a channel containing sensitive documents. Post-project, it's easy to forget to remove guest users, leaving them with unneeded access to data.

Beyond choosing whether to enable or disable guest access, IT and business leaders should decide who can be a guest, what they can access and how long they will have access. While cybersecurity teams may prefer to disallow guests entirely, this approach can introduce more problems, as guest users can be critical collaborators on projects that drive business outcomes. Here are questions to consider when establishing guest privileges:

- **Who should be allowed as a guest?** One recommended practice is to whitelist or blacklist certain domains to distinguish guests from known contractors. This prevents competitors from gaining access to valuable information. IT teams can also consider limiting users from public domains, as this type of guest will be able to access the workspace at any time — regardless of their employer. Aside from guest domains, it's also important to think through the general process of adding a guest: What approvals are required and from whom?
- **What should guests be able to access?** Your organization will likely want to restrict guest access to some workspaces, particularly highly sensitive ones. Carefully consider guest default settings and develop granular policies. Automated workflows can reduce the burden on IT teams to manually monitor, optimize and enforce these policies.
- **How long should guests retain access?** One common issue with guest access is that once a project ends, team members often move on to the next deliverable and forget to terminate guest access. Consider a periodic audit process for guests to protect and secure your data. The review should be mapped to the sensitivity level of the workspace and be conducted monthly, quarterly or biannually. For ease of guest tracking and management, organizations can leverage collaboration platform governance tools to streamline the process.

Companies can no longer afford to overlook the importance of an effective collaboration governance strategy. In the face of a challenging economic forecast, IT teams must now join forces across departments and business units to develop collaboration governance policies that support employee productivity and remediate your enterprise's data security vulnerabilities.

Unisys' PowerSuite™ Governance tool empowers organizations to streamline collaboration governance strategy creation and implementation. PowerSuite Governance is an all-in-one software solution that allows IT teams to easily identify and resolve digital sprawl and to set custom, flexible security policies that optimize employee experience.

Master collaboration governance in your organization with a free trial of Unisys PowerSuite Governance: www.unisys.com/powersuite-free-trial.

unisys.com

10/22 22-0346