

The State of Collaboration in the Digital Workplace: Building a Safe Sharing Environment and Optimal Employee Experience

Presented by:
eSHARE
and
reworked

In our digital world, external collaboration must balance the fine line between excellent security and high ease of use. But Digital Workplace and IT leaders don't necessarily understand how to accomplish this delicate balance. How can they best work together?



Introduction

Collaboration with external parties requires careful security protocols to ensure that assets are shared safely outside the organization. However, even though collaboration tools have come a long way in the past few years, the current collaboration environment is not working the way it should. It's becoming more complex, which is putting a strain on productivity and security.

Employees in many organizations are sharing in insecure ways that cause big risks, such as by using personal email or [shadow sharing](#). If a tool is used for internal collaboration, it's probably also being used for external collaboration. This presents a challenge when employees must work within security settings that limit them from being able to collaborate externally in a seamless, efficient way. This is an issue for both Digital Workplace (DW) and IT professionals, who need to be on the same page to ensure that they're giving employees the right tools, resources and education to collaborate safely and with ease.

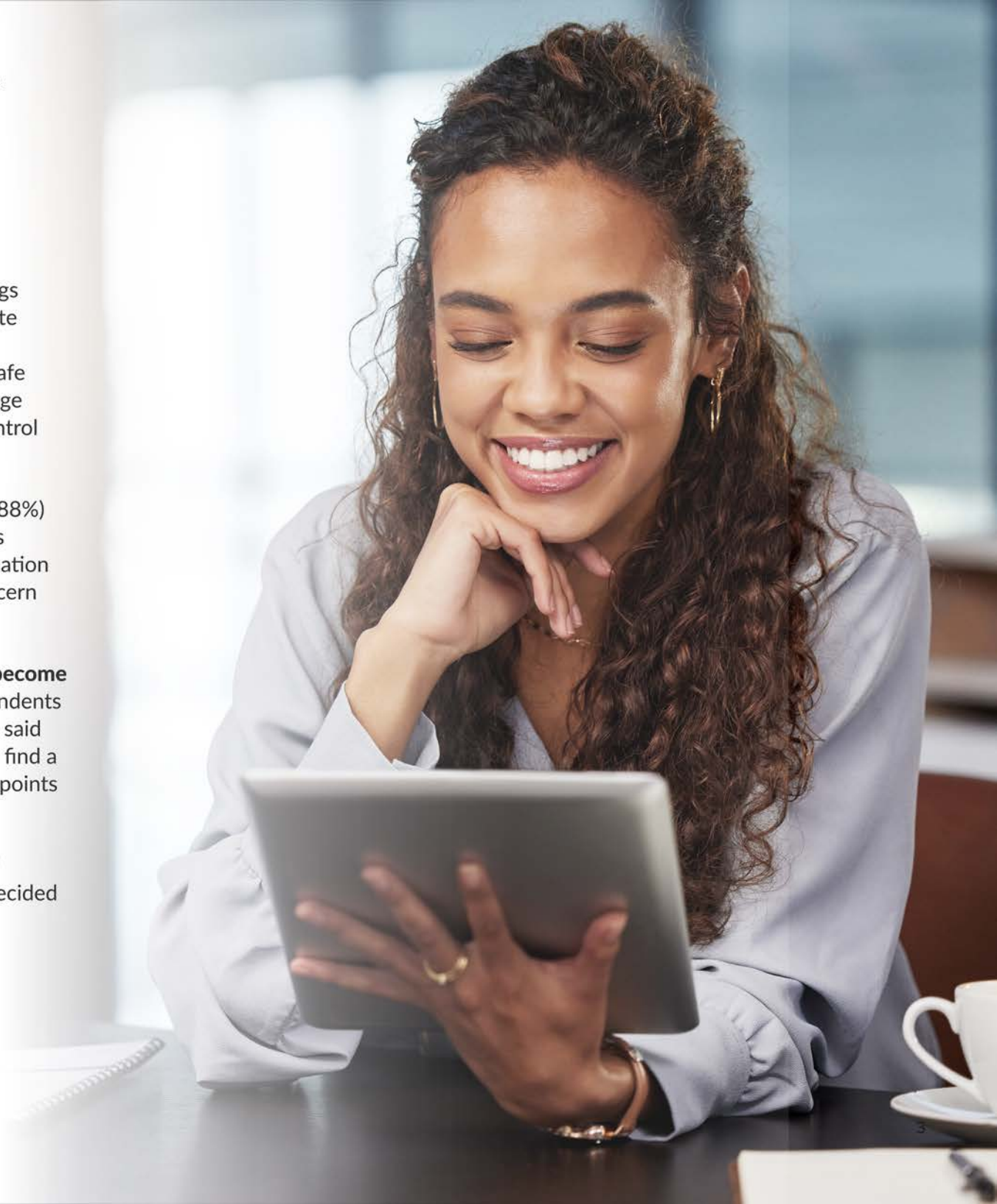
Meanwhile, changes in Microsoft 365 sharing restrictions have created even more friction in the external collaboration environment. As M365 is a relatively common toolset that organizations use, employees' reactions to the new restrictions show a troubling trend in unsafe sharing practices.

eShare, in partnership with Reworked Insights, surveyed more than 400 leaders (director level and above) who either work in IT or DW. eShare sought to understand the current state of external collaboration, where there are challenges and where opportunities exist to create a safer sharing environment. How can IT and DW professionals better balance the people side and the tech side of external collaboration?



Key Findings

- **If organizations are using a tool for internal collaboration, odds are they're also using it for external collaboration:** However, security settings often limit the ability for employees to collaborate externally with the same ease they collaborate internally, and they may end up resorting to unsafe sharing methods. This presents a serious challenge for Digital Workplace and IT professionals to control access to information and maintain security.
- **Safe sharing is a big priority:** The vast majority (88%) of DW and IT leaders at enterprise organizations strongly agree that how they safely share information with external collaborators is a top-of-mind concern for their leadership.
- **Digital collaboration with external parties has become more complex over the past year:** 69% of respondents said it has become more complex, and only 19% said it's become less complex. Organizations need to find a solution that successfully addresses the friction points that come with increased complexity.
- **Enterprise organizations are generally aware of changes in M365 sharing** — but many haven't decided yet how they will respond to these changes.



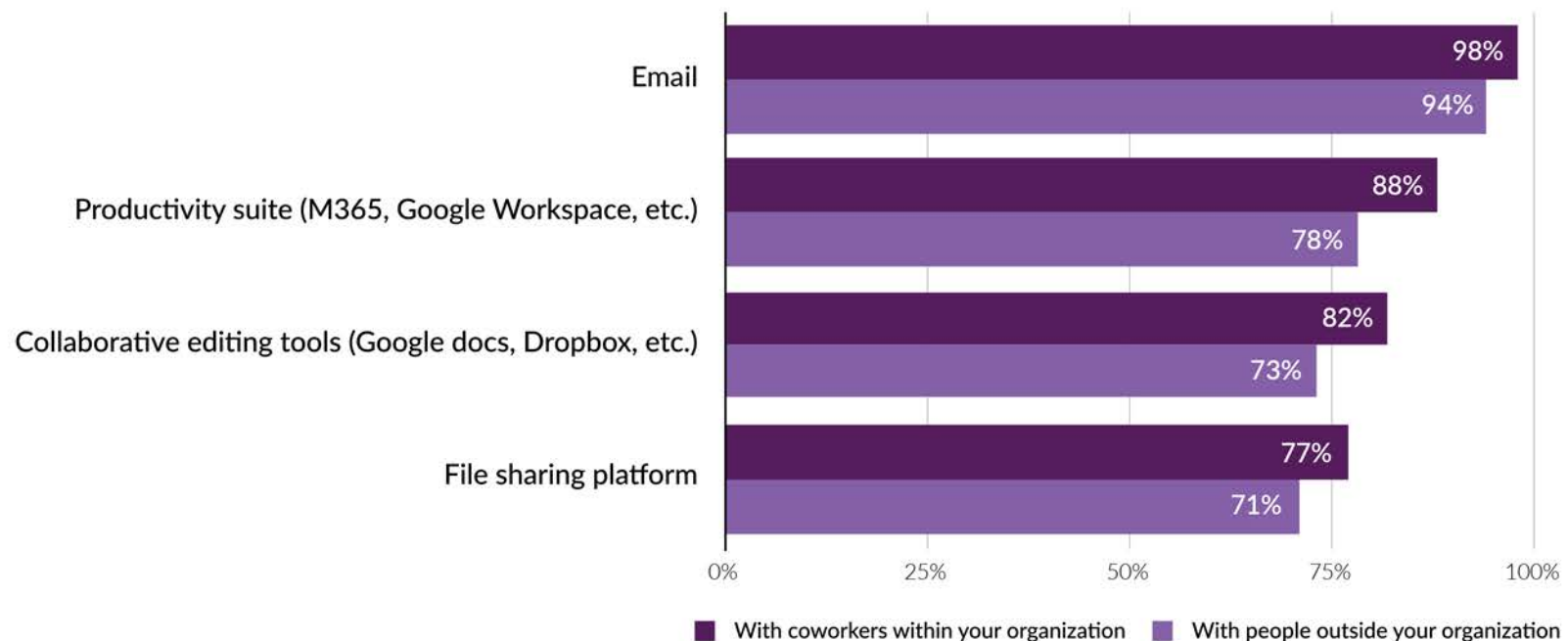
The Current State of Digital Collaboration Tools

The platforms and tools organizations use to collaborate internally are generally the same ones they use to collaborate externally. For example, 82% of organizations use collaborative editing tools like Google Docs or Dropbox for internal collaboration. Also, a hefty 73% say their employees use these same collaborative editing tools for collaboration with people outside of their organization (Figure 1).

This trend is a double-edged sword for organizations. These collaboration tools are helpful and accessible to employees. Yet at the same time, the degree to which employees use these tools externally may be something IT is not prepared for. Employees may respond to external security settings by working through a cloud-based app or shadow sharing, both of which increase security risks. And if IT loosens security protocol to make sharing more seamless, that also increases the company's exposure to risk.

This presents a problem for organizations that have not properly thought through external sharing security protocols for all these tools. Proper security for each of these solutions takes a lot of time and consideration, and given the sheer volume of tools that employees use to collaborate externally, that's a lot of work. In fact, for the most commonplace collaboration tools, 70% or more of enterprise organizations say that their employees also use them to collaborate outside of their organization.

Figure 1: Which collaboration tools do employees use to collaborate? (all organizations)

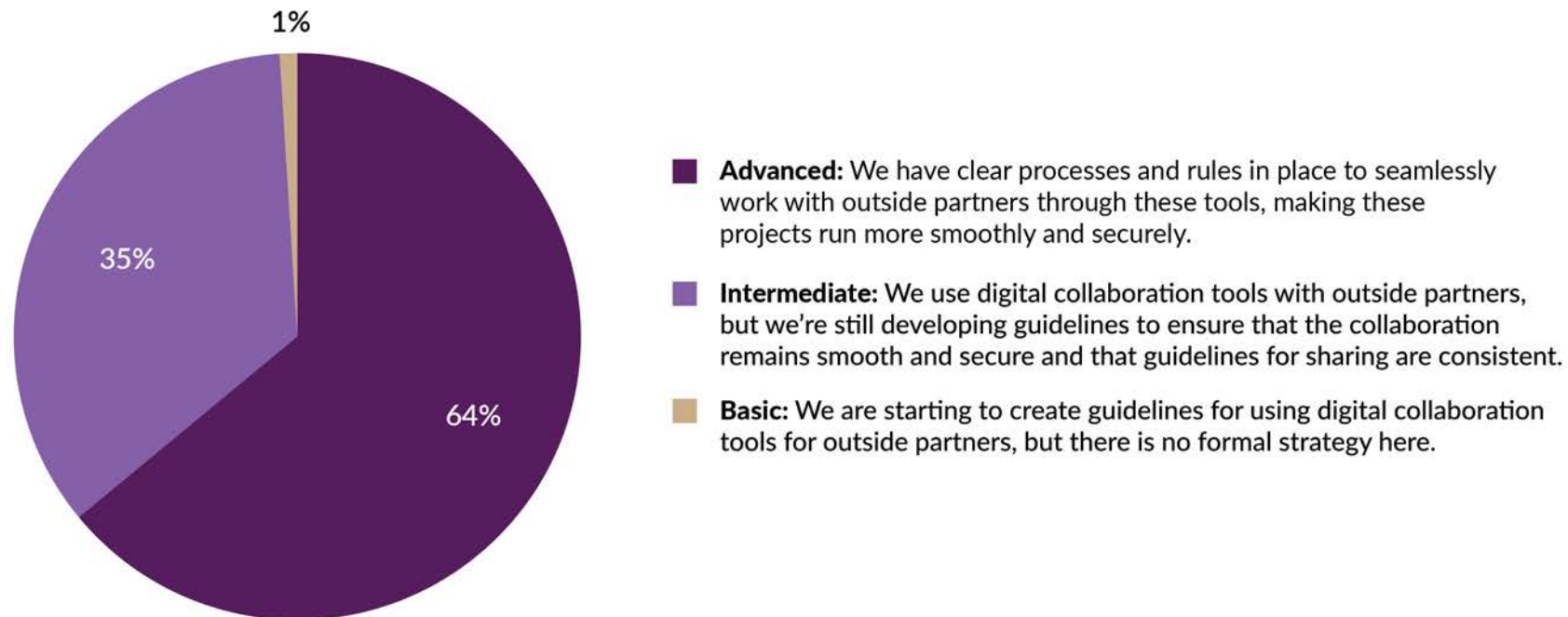


Pursuing Better Security in Collaboration

Luckily, safety is top of mind for most organizations and their decision-makers. The vast majority (88%) of DW and IT leaders strongly agree that how they safely share information with external collaborators is a top-of-mind concern for their leadership. Given this level of leadership support, it's likely that IT teams will receive enough resources to accomplish their goals related to the safety of collaboration tools.

Still, safe sharing is not yet the norm. A lot of progress must be made to accomplish the state of security that organizations strive for. While many DW and IT leaders say they've adopted advanced, formalized guidelines for collaborating with external stakeholders, a whopping 36% say they're still developing guidelines for secure and consistent sharing (Figure 2).

Figure 2: How formalized are your organization's guidelines for collaborating with external stakeholders (i.e., clients, customers, vendors, supply chain) via digital collaboration tools? (all organizations)



Different Attitudes for Different Leaders

We looked at the differences between DW leaders and IT leaders to see if they deviated on any beliefs or attitudes related to collaboration. They come from different perspectives, and comparing their answers showed that they have some differing views on the current state of digital collaboration tools.

IT leaders have a slightly rosier perspective. They're more likely to strongly agree that "our employees are well supported by IT to deliver a frictionless and smooth digital collaboration experience with external stakeholders" (72% vs. 64%). They're also more likely to say that their IT team works hard to make conducting business as easy as possible (78% vs. 71%). Finally, more IT leaders said that IT implements security measures to support their organizations' external digital collaboration efforts

There are a few potential reasons for this trend. For one, DW leaders are likely not as aware of the technical gears behind the tech stack as IT leaders are. On the other hand, DW leaders are closer to the employees actually using the digital collaboration tools, and they've likely directly heard frustrations from the people using the collaboration solutions more often.

Essentially, both IT and DW have a blind spot here. IT leaders are not as aware of the state of the user experience with these tools, and DW leaders are not as aware of the details on the technical side, especially where security is concerned. Luckily, IT leaders want to help DW leaders succeed, and DW leaders understand the importance of security. Both groups understand how the other is paramount to the success of the company.

As organizations seek out stronger technology solutions to their problems, it's important that they don't ignore the user-related aspects of success.

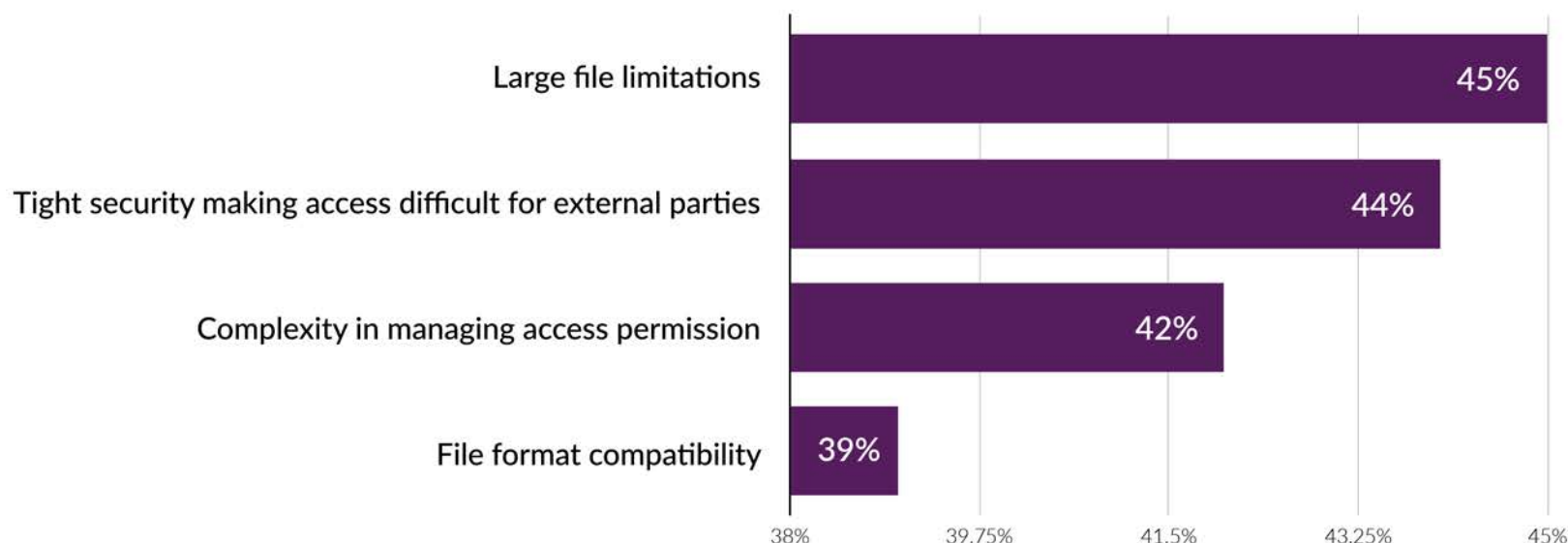


Different Attitudes for Different Leaders

Most (69%) organizations say that the complexity of digital collaboration with external parties has become more complex over the past year. With increasing levels of complexity comes an increasing need to maintain security standards and educate employees on proper sharing.

The most common kinds of friction that organizations experience in external file sharing are large file limitations (45%), tight security (44%) and complexity in managing access permission (42%) (Figure 3). All of these are inconveniences that can add unwanted tension in client communications and employee experience.

Figure 3: What types of friction does your organization experience in external document sharing? (all organizations)

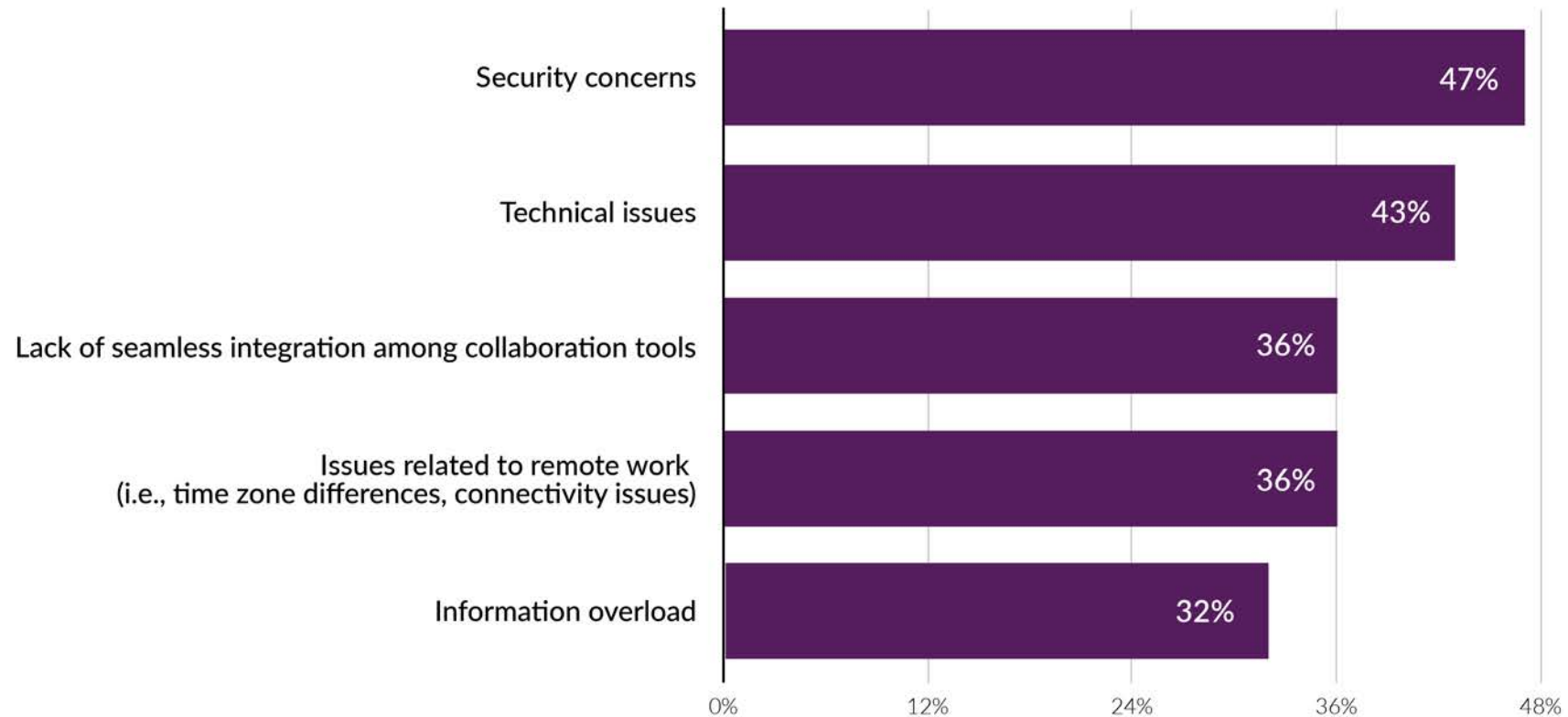


Friction Leads to Negative Consequences

Increasing complexity means more complicated security, as well. Almost half (47%) of DW and IT leaders say that their employees face security concerns when using digital collaboration tools (Figure 4).

Other common challenges include technical issues (43%) and the lack of seamless integration among tools (36%). This highlights a few important factors. For one, technical issues put a wrench in the employee experience as they try to create a pleasant, smooth working relationship with clients and partners. When technical issues or integration issues occur, both employees and outside partners may become frustrated.

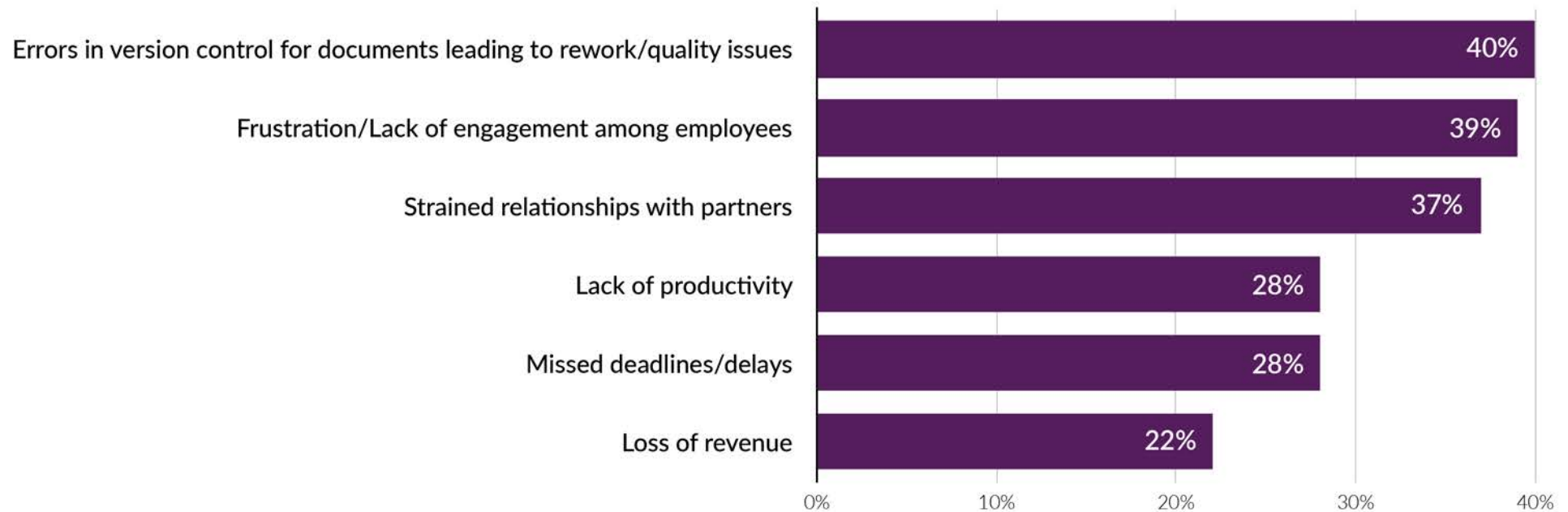
Figure 4: What challenges do your employees face when using digital collaboration tools? (all organizations)



DW and IT leaders also cited many common consequences that their organizations have experienced due to friction in collaboration. “Errors in version control leading to quality issues” was the top answer here (40%) (Figure 5). Collaboration tools are supposed to make it easier to form an efficient, smooth working relationship with outside parties, and it’s not an acceptable outcome for version control issues to decrease the quality of work.

Similarly, 39% of leaders said that frustration and lack of engagement among employees is an outcome they’ve experienced – yet another trend that can lead to less-than-satisfactory experiences for clients and other outside parties.

Figure 5: Which of the following negative consequences has your organization experienced due to friction in collaborating with external partners via internal digital collaboration tools? (all organizations)



Finding the Path Forward

DW and IT leaders have put up more security controls to protect information, but they've experienced mixed results here. Luckily, they're generally aware that they've put up so many controls that employees feel they have to go around them to avoid friction in the external collaboration experience.

Employees aren't keeping their frustrations quiet. Most IT and DW leaders (67%) say that employees have expressed frustration over how difficult it is to share files externally due to external parties' email or security filters. And 63% say that employees have expressed frustration due to collaboration tools that don't work as well as they should. Given this environment, it's no surprise that a whopping 75% say that when working with external stakeholders, employees often prioritize information sharing over security.

It's a good sign that DW and IT leaders are aware of the problem. A solid majority (76%) agree that their organization's security protocols are cumbersome enough that employees sometimes share files externally through personal email or other unauthorized means. And more than a third (37%) of leaders say that they themselves have used personal emails to extend digital collaboration to external stakeholders. Luckily, almost all organizations (93%) are exploring ways to make it easier for employees to balance security and external collaboration.

Most (71%) DW and IT leaders say their employees have access to a sufficient number of collaboration tools to make external collaboration easy and safe. This means that, in general, access to the right tools isn't the issue. The immediate challenge is employees knowing how to use the tools correctly and securely. Moving forward, employees will more often expect collaboration tools to be easily accessible solutions rather than complicated distractions that impact their productivity.

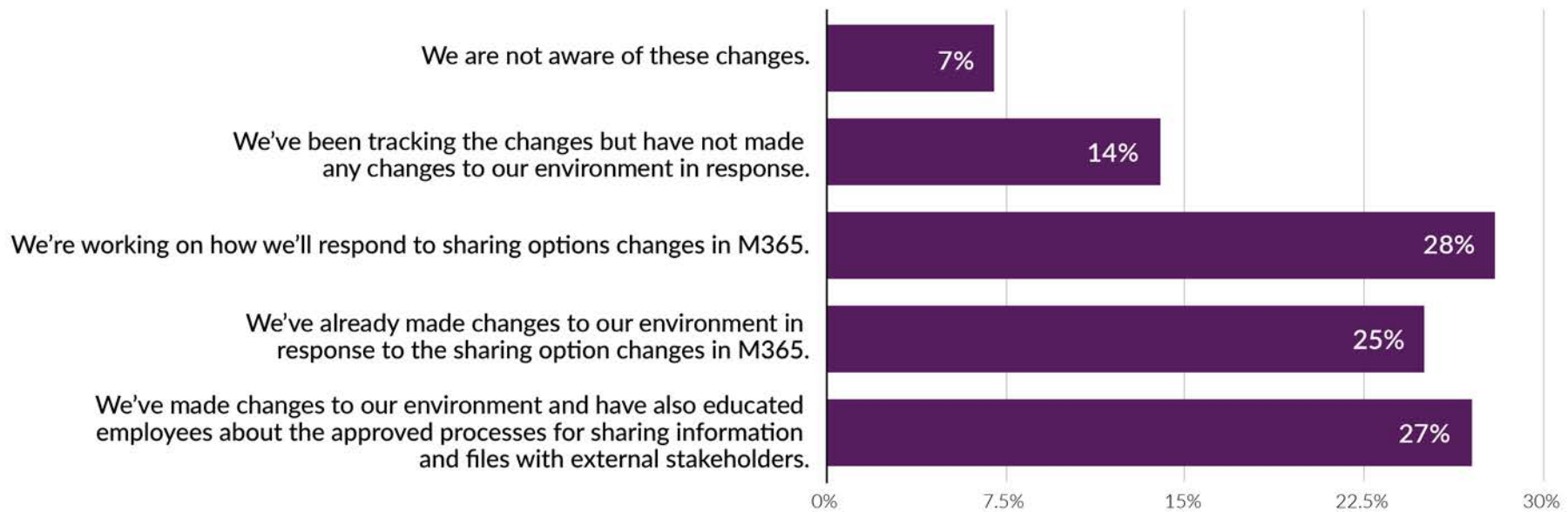


Changing M365 Sharing Restrictions and Changing Strategies

Microsoft 365 is a common enterprise collaboration tool that organizations use — and one for which new sharing restrictions were recently released. Exploring organizations' usage of the platform provides a solid example of common collaboration successes and concerns.

The platform introduced new restrictions on sharing externally in 2023, and many organizations have still not figured out how to use the tool effectively with these new limitations. In fact, even though 93% of DW and IT leaders are aware of the changes Microsoft has made, only 52% say that they have made any changes to their environment in response (Figure 6).

Figure 6: In the past year, what has been the response of your organization to the restricted sharing options changes for Microsoft 365? (all organizations)

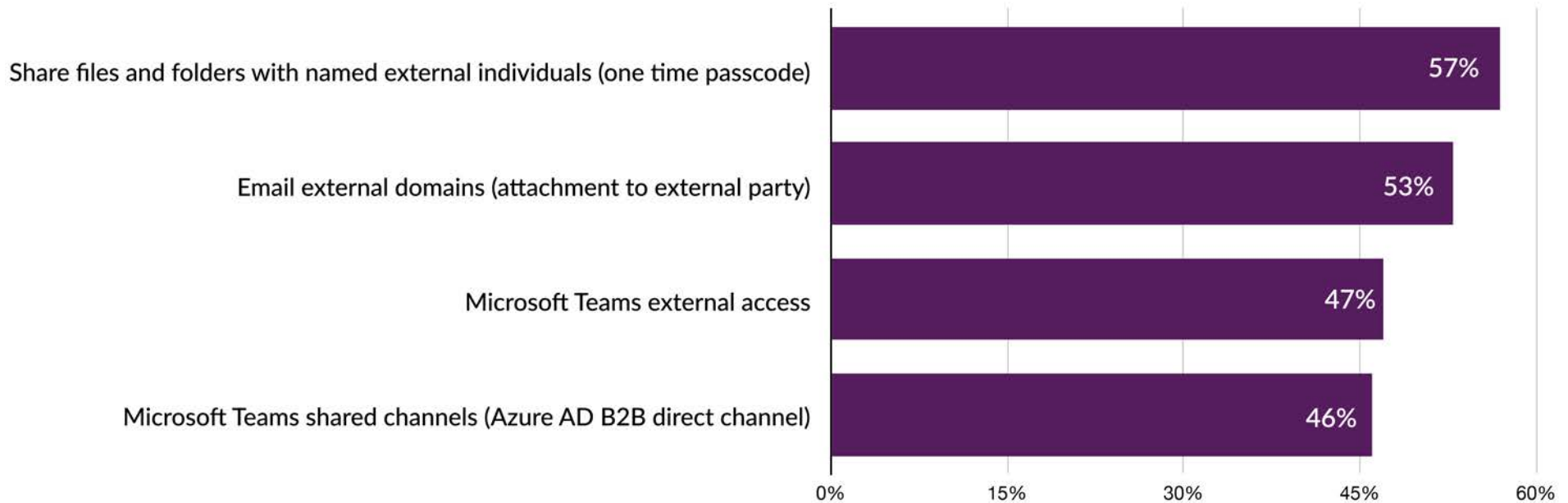


Meanwhile, organizations are facing certain negative consequences to these changes, like employees becoming uncertain which sharing options are the most secure/safe (46%) and links to clients being blocked by security measures (45%). Another 38% say that external sharing on their platform is more difficult to manage. These answers further support the fact that DW and IT leaders say security concerns (47%) are the most common challenge their employees face when using digital collaboration tools.

How Organizations Are Using the New M365

Currently, organizations rely on some Microsoft 365 options more than others. More than half (57%) said they share files and folders with named external individuals using a one time passcode, and 53% said they email external attachments (Figure 7).

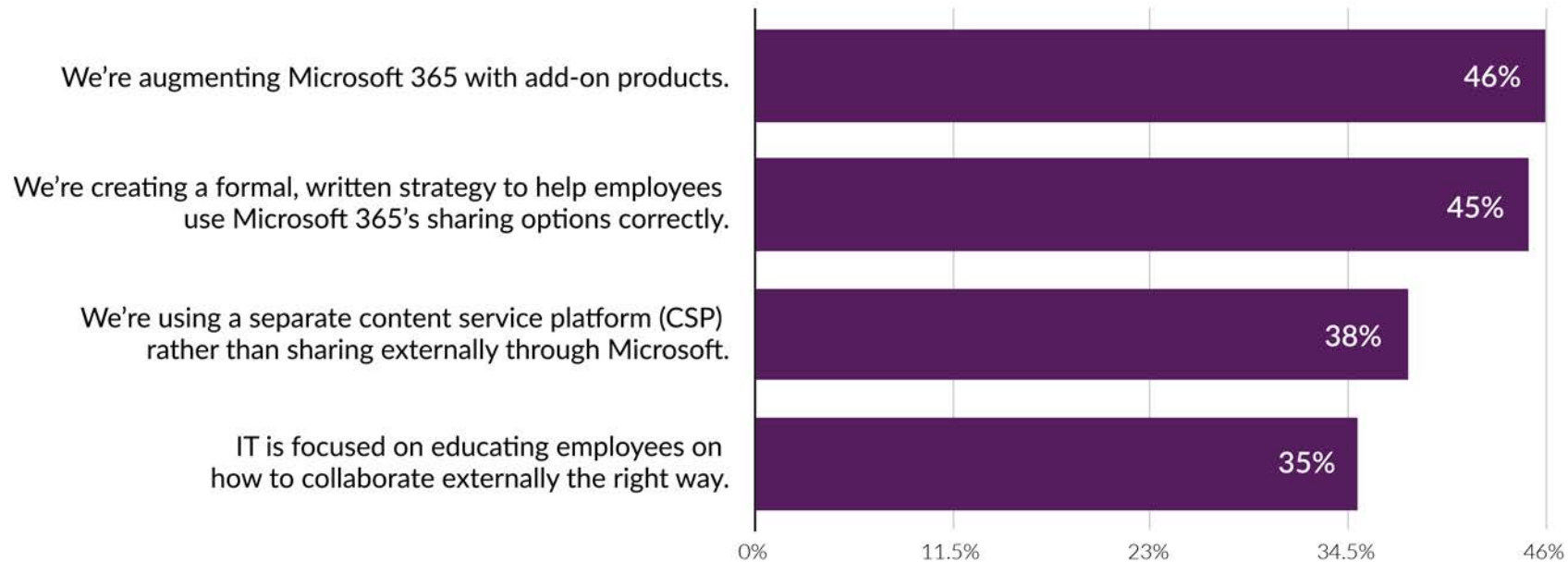
Figure 7: What restricted sharing options on Microsoft 365 does your organization use? (all organizations)



They're also making certain strategy changes due to the new restricted sharing options. Most commonly, they plan to augment Microsoft 365 with add-on products (46%) and create a formal, written strategy to help employees use Microsoft 365's sharing options correctly (45%) (Figure 8).

However, while this is a step in the right direction, that's still fewer than half of organizations making these strategy changes. The lack of sufficient action here highlights the degree to which organizations are not quite prepared for these changes.

Figure 8: Is your organization making any strategy changes due to Microsoft 365's new restricted sharing options? (all organizations)



Looking at workforce distribution helps explain some of these shortcomings in Microsoft 365 strategies. Separating respondents by those in global or multinational companies and those in local or national companies shows some illuminating findings. Global and national companies are more likely to be aware of changes in Microsoft 365 sharing options and take action accordingly.

When asked what their response has been to the changing Microsoft 365 restrictive sharing environment, 38% of the multinational and global respondents said “We’ve made changes to our environment and have also educated employees about the approved processes for sharing information and files with external stakeholders” – the most advanced option – compared to only 16% of the National/Local group.

One potential reason for this is that companies outside the United States tend to operate in countries with stricter compliance and safety requirements. In order to be successful in a multinational or global company, it’s necessary to be more compliance-centric. Companies outside the U.S. could threaten not to do business with them if they’re not compliant.

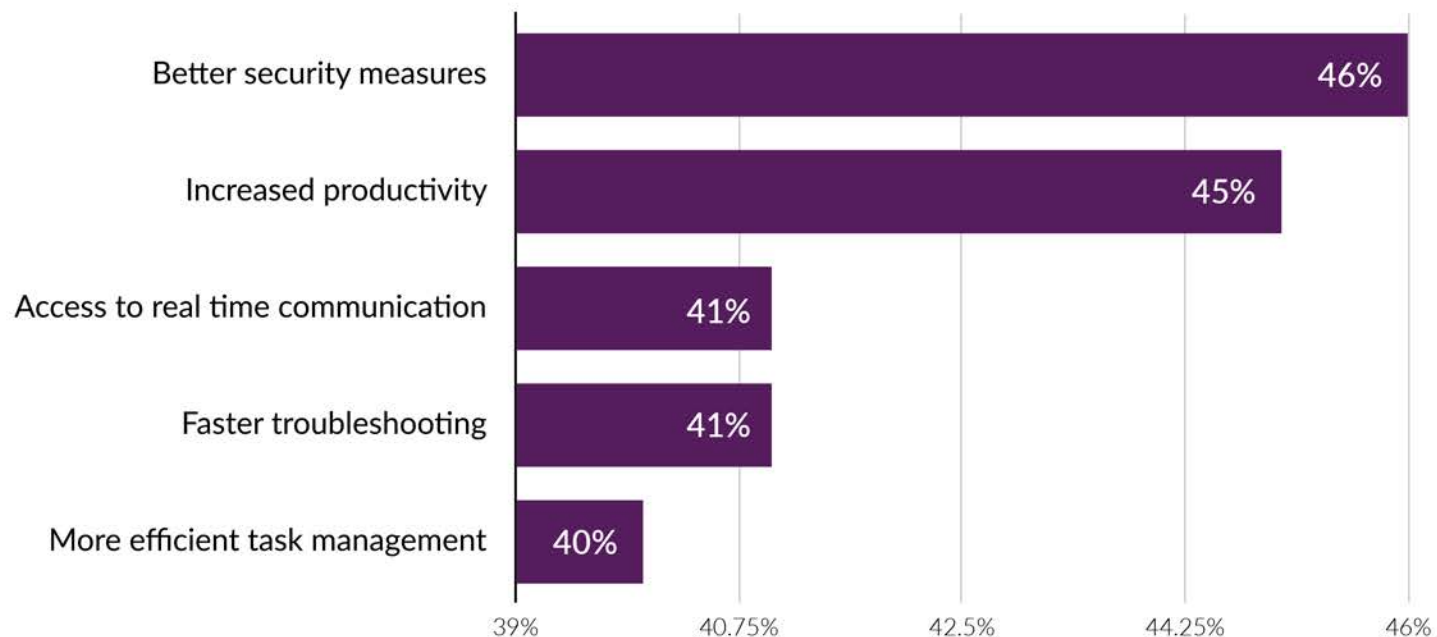
Another area of confusion for current Microsoft 365 users relates to their new AI assistant, Copilot, also released in 2023. Organizations are excited to have access to a generative AI tool that can accomplish a variety of tasks -- from creating charts to identifying trends to summarizing large amounts of information – and all of these are use cases that can help projects with external parties move forward more efficiently. But using this tool effectively also requires careful collaboration between IT and DW teams. While DW can focus on the potential benefits for how work is accomplished, IT will be more likely to know how to integrate the tool securely into the organization’s tech stack.

Improving the M365 Environment

While organizations are taking certain actions to ease the challenges in the current Microsoft 365 environment, there are still many issues left to address. A lot of employee training and education is still needed to make sure employees know how to use the platform safely. As shown in Figure 8, when asked how they're responding to changes in Microsoft 365's sharing options, only 35% of leaders said "IT is focused on educating employees on how to collaborate externally the right way." One reason for this could be that IT does not think training is the answer, and they're more focused on putting up guardrails and lessening the friction related to external collaboration.

Organizations that do figure out how to improve digital collaboration can expect many benefits, including better security measures (46%) and increased productivity (45%) (Figure 9). Better security measures is an especially desirable outcome in an environment where sharing safely is such a major concern.

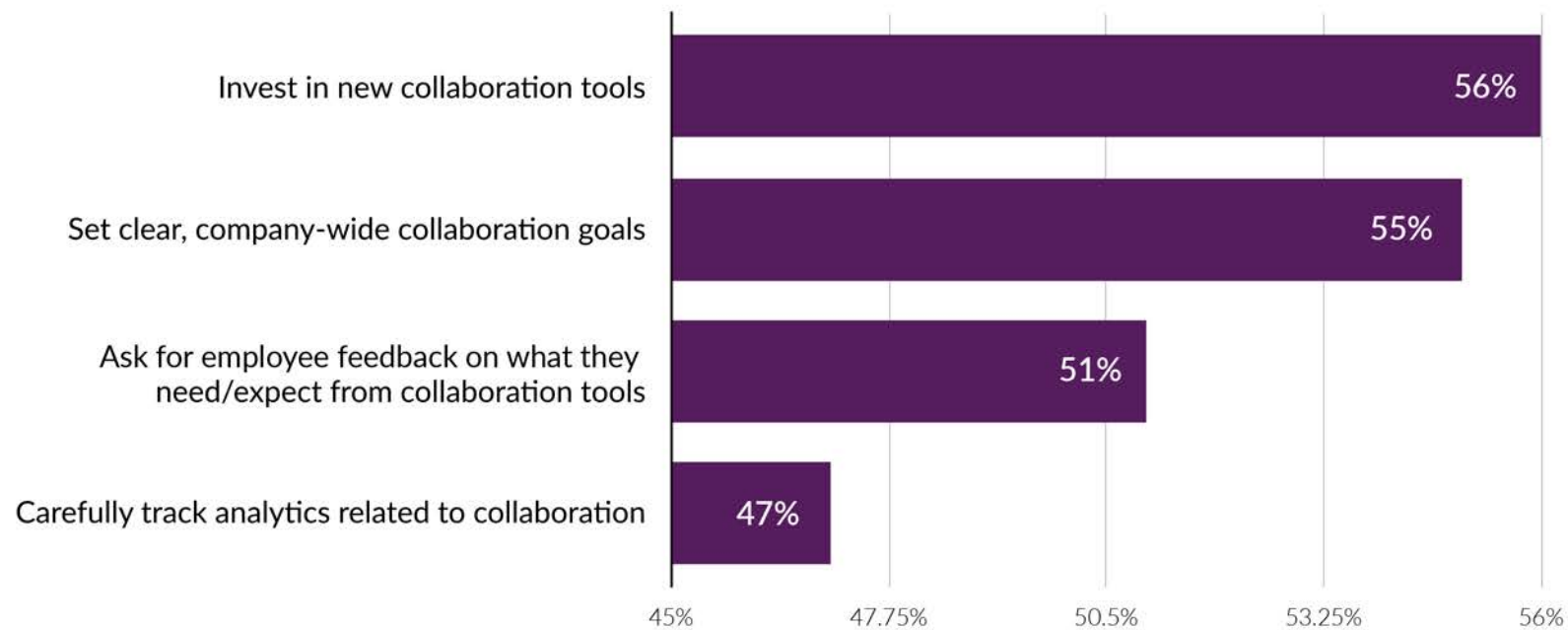
Figure 9: What benefits has your organization experienced due to efforts made to improve digital collaboration? (all organizations)



One solution that would address this problem and create these benefits is a more simple, manageable collaboration solution that allows both IT and DW to get what they want — IT to have more control over safe sharing and DW to know that employees are able to collaborate in a way that is easier, safer and less difficult to understand. In fact, investing in new collaboration tools was the most popular answer for organizations when they were asked how they plan to improve workplace collaboration in the next year (Figure 10).

Certain add-on solutions will allow organizations to keep their current collaboration platforms like Microsoft 365 or Google Suite — all while benefiting from advanced security features and smoother ease of use of the add-on solution.

Figure 10: How does your organization plan to improve workplace collaboration in the next year? (all organizations)



Conclusion

Many current external collaboration challenges are contributing to an environment in which sharing information externally is not safe or secure, nor is it as easy as collaborating internally. This is not good for either employees and the clients they're working with. The ideal balance for organizations is to reach the point where simplicity and friction are just as important factors as security and more tools.

To create a safer environment with minimal friction between employees and clients, organizations need a solution that avoids the common collaboration challenges they're currently facing. Now is the time for DW and IT to align in a more consistent, organic manner — before the growing complexity becomes too much to handle.

That's where eShare comes in. As a SaaS solution that is designed to augment Microsoft 365's external-sharing capabilities, eShare helps simplify the external collaboration process for both users and IT. It uses an organization's existing cloud file storage to provide virtual data rooms where authorized internal and external users can collaborate. This solution allows organizations to share files and collaborate externally as easily as they do internally, but without ever letting any data or files leave the security of the company's tenant. Learn more about how this platform allows frictionless collaboration and secure governance to co-exist in the link below!

[Learn more about eShare here!](#)



Appendix

Demographics

Title

“State of External Collaboration in the Digital Workplace:
Security and Productivity ”

Survey dates: March 2024

Respondents: 417

Organizational size

1,000-5,000: 85%

5,000+: 15%

Career level

C-Suite, owner, partner: 41%

Senior vice president: 7%

Vice president: 13%

Director: 40%

Distribution of the workforce:

Local: mostly located in one region: 18%

National: located in several regions within one country: 39%

Multi-national:

mostly located in one country with some global distribution: 24%

Global: highly distributed with locations around the world: 19%

Statistics may not total 100% due to rounding.

About

eShare

eShare is at the forefront of transforming external data sharing and collaboration for enterprises. Our platform enhances the digital employee experience while ensuring the utmost security and compliance by integrating with Microsoft 365 and Google Workspace, thereby removing the dependence on additional data repositories. Built around familiar tools like Teams, SharePoint, OneDrive, and Outlook, eShare makes external data sharing seamless and secure, allowing businesses to concentrate on growth with the assurance of secure, compliant, and efficient data sharing practices.

Reworked

Reworked, published by Simpler Media Group, is a native digital publication covering the r/evolution of work and the transformation of the workplace.

Simpler Media Group

SMG is a B2B technology information and research services company serving a 3 million+ strong community of global digital business leaders.

Our flagship publication, [CMSWire](#), is complemented by our [Reworked](#) and [VKTR](#) publications. Our research division produces a range of annual state of the industry reports, quarterly market segment guides and a range of focused industry insights briefs. We offer performance marketing, custom research, content development and custom event production services directly to our clients.

Our obsessions: next generation digital customer experiences, navigating the r/evolution of work and advancing enterprise learning.

eSHARE | **reworked**