techconsult
TECHNOLOGY MARKET ANALYSTS

30 YEARS ANNIVERSARY

THE GLOBAL USE OF COLLABORATION SOLUTIONS IN HYBRID WORKING ENVIRONMENTS

How companies manage security risks

On behalf of

HORNETSECURITY

Information about the study

Created by

techconsult GmbH
Baunsbergstraße 37
34131 Kassel (Germany)

Mail: info@techconsult.de
Phone: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Publication date

10/2022

Author

Ercan Hayvali

On behalf of

HORNETSECURITY

Contact

Hornetsecurity GmbH
Am Listholze 78
30177 Hannover (Germany)

Mail: info@hornetsecurity.com
Phone: +49 511 515 464 0

Find out more

Other Information
For reasons of better readability, the masculine form is used for personal designations and personal nouns in this study. Corresponding terms generally apply to all genders in terms of equal treatment. The shortened form of language is for editorial reasons only and does not include any rating.

Table of content

Introduction

Due to the establishment of hybrid workplace concepts in recent years, communication and collaboration solutions have also become increasingly integrated into operational processes. For many people, collaboration solutions such as Microsoft Teams are therefore among the key tools in terms of the completion of their work tasks. The internal discussions made possible by these solutions enable employees in groups to process projects and exchange messages and documents. Business-critical and sensitive content is increasingly being shared through collaboration solutions. As a result, IT managers aren't only required to ensure the protection of the IT infrastructure and the company network, but to also guarantee accessibility to the contents of collaboration solutions.

However, it is often the case that collaboration solutions only communicate in a limited number of channels. Despite the possibility to use private and public channels or groups, employees tend to carry out most of their communication via direct messages. It is frequently the case that highly sensitive, private or confidential files and information are sent. This includes IT-relevant details and passwords. Moreover, some 75 percent of employees also use the in-house collaboration solutions on their private end devices, such as their smartphones or tablets. In the long term, this fusion of the private and business spheres as well as the shifting of private conversations into the digital world, presents a major challenge – not just for employees, but also for IT departments.

How do employees use the collaboration solutions and which content is shared particularly often? What impact is shadow IT having on company security, and how can IT managers manage this? What are the risks and challenges presented by these solutions, and what are the future trends? These questions, and others, are analyzed and presented as part of this detailed study. An international survey of 540 IT managers and users of collaboration solutions from companies with at least 50 employees provides the basis for the data.

Hybrid work as a workplace model for the future

Companies and employees have been presented with major challenges, not least because of the coronavirus pandemic. Workplaces, workflows and methods of communication have changed and adapted to the new circumstances in a very short time. Less than three years after the start of the pandemic, however, the changes, which were initially considered temporary, have become the norm. This change is also reflected in the current configuration of workplaces.

Accordingly, approximately 46 percent of respondents don't just work in the office but also from home as part of a hybrid working model. This newer model tends to be used more frequently in larger companies. Accordingly, only a quarter (25 percent) of respondents from companies with 50 to 99 employees work both from home and in the office, while in companies with 5,000 or more employees, the proportion is approximately 58 percent.

In addition, some 40 percent of respondents work exclusively in the office or have returned to the office-based model. However, specific differences relating to company size can be seen here as well.

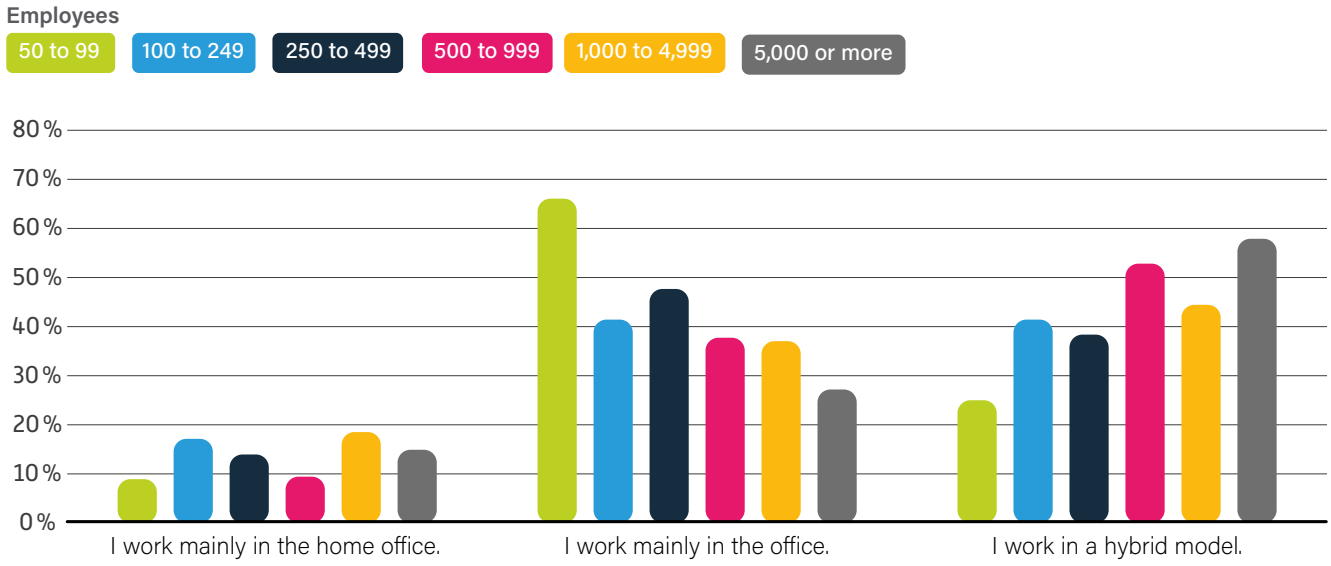
Accordingly, two-thirds (66 percent) of respondents in smaller companies with 50 to 99 employees work entirely in the office, while the percentage in large companies with 5,000 or more employees is only 27 percent. Overall, only 14 percent work from home on a permanent basis.

Moreover, the new workplace culture has been accompanied by a change in the way we communicate. While direct discussions or email traffic were considered the usual communication channels before the pandemic, it is now collaboration solutions, such as Microsoft Teams, on which the exchange of information mostly takes place. In this respect, employees don't just use collaboration solutions for the purposes of exchanging information, but also for everyday communication with colleagues and also at the private level.

Only 14 percent of respondents work entirely from home while 46 percent work in a hybrid model

Current workplace model

Base: 540 Companies



Collaboration solutions as a key channel of communication

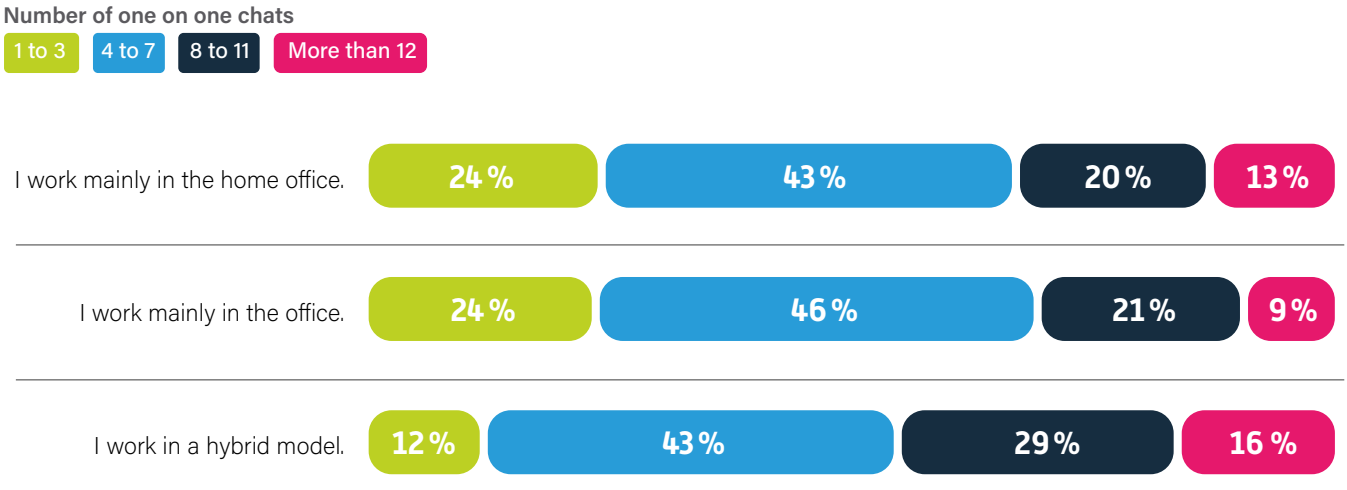
The change in the working world isn't just evident in terms of the places where the work is actually being done, but also in terms of the collaboration between employees. While before the pandemic, private conversations or work-related discussions took place next to the office coffee maker or over lunch with colleagues, this culture of communication has now almost completely shifted. Conversations or brief discussions are now mainly taking place at the digital level via Microsoft Teams, for example, and meetings are often held in the form of video meetings. For employees, collaboration solutions play a major role in maintaining the exchange of information with their colleagues. Accordingly, some 44 percent of respondents say that they communicate with four to seven people through Microsoft Teams on regular working days, and as many as a quarter (24 percent) have contact with eight to 11 people. Of course, the total numbers can vary depending on the company size, department and country. For instance, communication is particularly frequent in large companies that have 5,000 or more employees. In such organizations , approximately 45 percent of employees have contact with at least eight people each day via direct messages on Teams, whereas in smaller companies with 50 to 99 employees, the proportion is only 21 percent.

With collaboration solutions on private end devices, there is a tendency to exchange more messages

The workplace model itself also has a significant influence on the use of Teams as a means of direct communication, however. Surprisingly, employees who work from home tend to exchange fewer direct messages with colleagues than employees who work in the office or according to a hybrid working model. This could be due, in particular, to the fact that employees in the office see each other in person more often when they enter into discussions and continue their conversations digitally, whereas the initial contact with colleagues working from home takes place less frequently. In this sense, approximately 30 percent of employees who work from home and one in three (33 percent) who work in the office exchange daily messages with at least 8 colleagues, whereas for employees who work on a hybrid basis, the percentage is 45 percent.

Number of direct chats on average working days

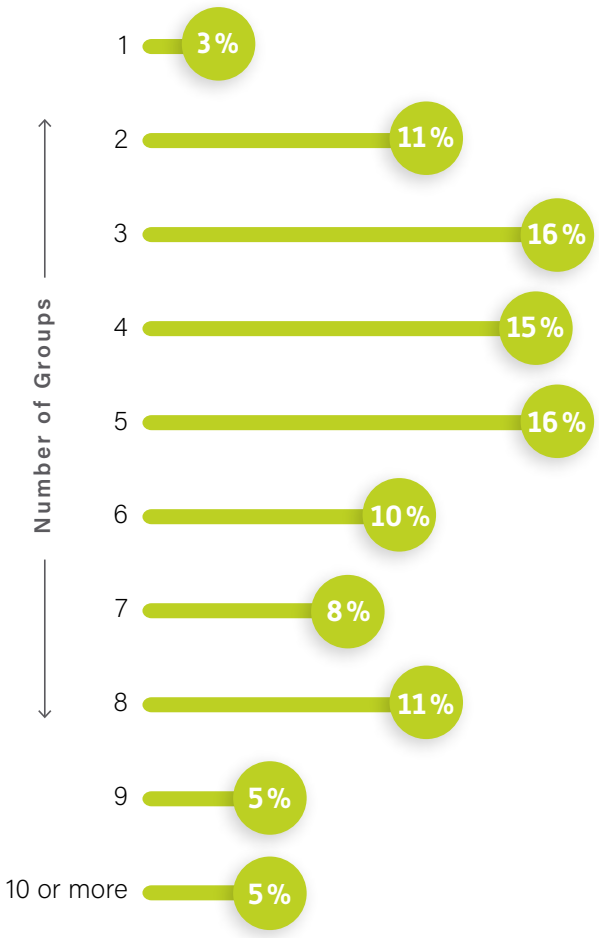
Base: 540 Companies



The exchanging of messages between colleagues is also influenced by the use of private end devices, though. Accordingly, employees are able to install the Microsoft Teams collaboration solution on their private devices and receive and send messages at any time. Approximately three quarters (74 percent) of respondents who do not install Teams on their private end devices send and receive messages with four or more colleagues. However, of the respondents who also use Teams on their private end devices, 84 percent exchange messages with at least four or more colleagues each day.

Activity in groups on average days

Base: 540 Companies



This demonstrates that private end devices contribute to an increased degree of internal communication. The use of private end devices could also lead to security risks, though. This is because privately used and unprotected end devices can become infected with malware, which they can then distribute to the company network via the collaboration software. In this case, IT departments are required to prevent the risk of what is commonly referred to as "shadow IT", and to backup the data, messages and content of the collaboration solutions.

Collaboration solutions can also be used for the purpose of working in groups, in which multiple employees are able to share workflows, projects or other topics.

Virtual collaboration in groups enables an efficient and productive level of communication, and improves the quality of the results. Almost a third (31 percent) of respondents are active in up to three groups on average working days, and 71 percent in up to six groups. Despite the specific differences in terms of size category and industry, the dispersion of the results indicates that the group activities are consistently used on a company-specific basis.

As with direct messages, the influence of private end devices can also be determined in terms of the intensity of group usage. Accordingly, three-quarters (75 percent) of employees who use Teams on their private end devices are active in three or more groups. By contrast, just over one in two respondents (53 percent) who do not have Microsoft Teams on their private end device are active in more than three groups. The use of private end devices can therefore result in a greater degree of use and collaboration in groups. In this context, it is also necessary for IT departments to ensure that content, files and chats within the groups are protected against the possible loss of data.

User Chats as a preferred method of communication

The communication behaviour of employees has also changed significantly due to the shift in working activities into the digital environment. In this context, as a widespread collaboration solution, Microsoft Teams offers a variety of possible forms of collaboration. It enables employees to contact each other via direct messages, exchange files and content or make direct telephone calls - these are known as Teams User Chats. Channels - or Teams Group Channel Conversations - can also be created for specific projects and workflows which are accessible to a restricted user group only or open to all employees in the form of an open channel. Group Channel Conversations can be used to share files, create content and meetings, or exchange project-specific messages.

Overall, however, it appears that employees tend to communicate directly via User Chats, which they prefer over other channels. For example, 70 percent of respondents agree that they exchange more direct messages with colleagues via User Chats than Group Channel Conversations. Therefore, in terms of the collaboration solution Teams, bilateral communication is one of the most widely used and widely used forms of communication. This can be seen at a similarly high level across all company size categories.

Employees are also able to exchange ideas in project-related groups. Here too, the majority of respondents prefer direct bilateral communication via User Chats. Accordingly, 61 percent of respondents agree with the statement that they prefer to write to colleagues using User Chats, despite the availability of groups.

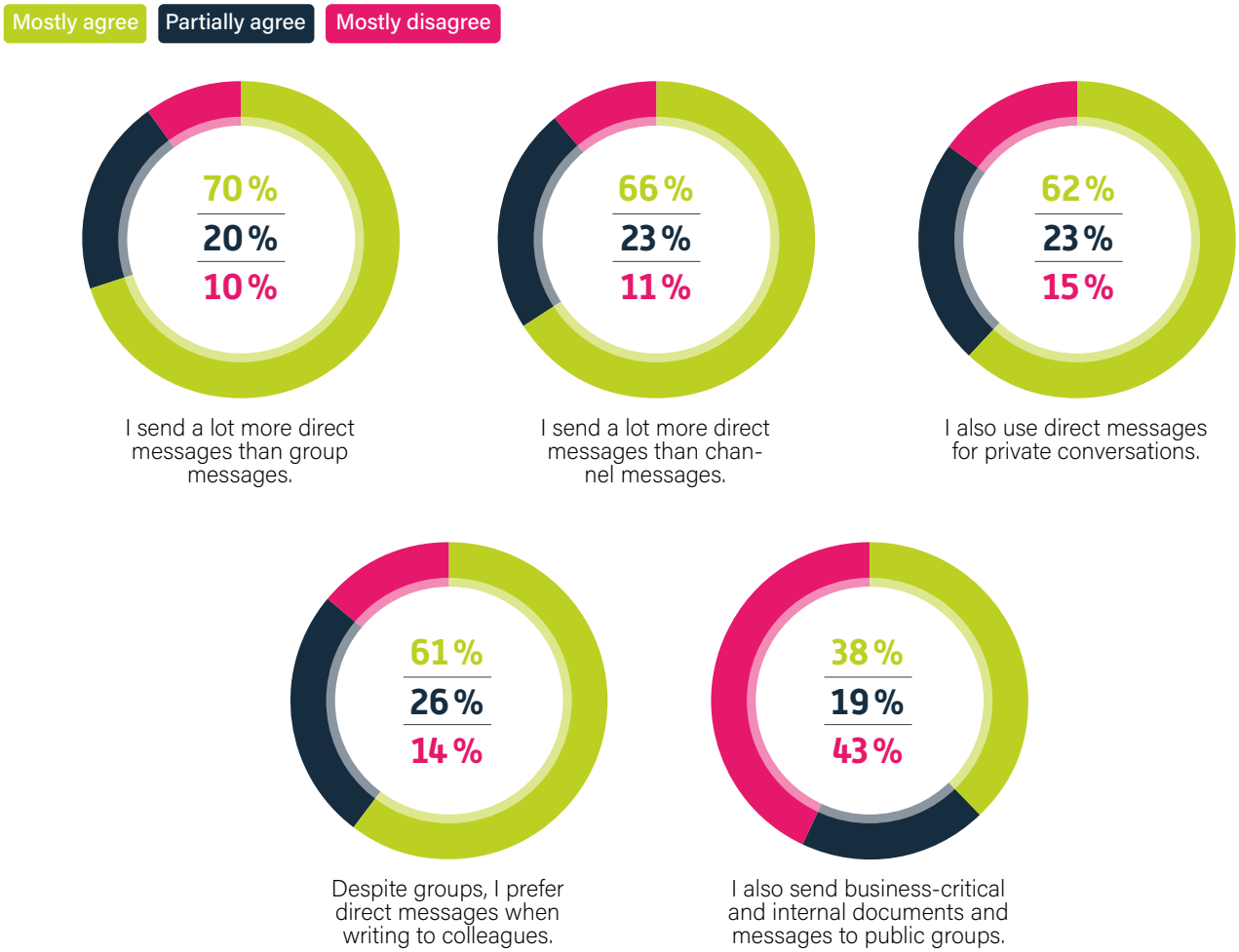
Accordingly, User Chats aren't only used for the purpose of communication if the topics only relate to the communicating persons, but also with other parties in the case of topics that are directly related to the project. This is particularly pronounced in larger companies. For example, more than two-thirds (67 percent) of employees in companies with 5,000 or more employees prefer User Chats over Group Channel Conversations, whereas the proportion in small businesses with 50 to 99 employees is only 57 percent.

Additionally, User Chats via collaboration solutions such as Microsoft Teams is also used for private conversations. Accordingly, the widespread hybrid working and home working models mean that employees keep in touch with their colleagues and maintain relations with them via Teams. In this context, it isn't only private messages, but also private documents, files and images which can be exchanged. Approximately 62 percent of respondents say that they use User Chats in Teams for their private conversations. This is evident across all size categories, but increases with the size of the company.

70 percent of employees prefer direct messages – or User Chats – for company communications

Use of collaboration solutions

Base: 540 Companies



62 percent of employees use direct messages for private conversations

It can also be seen that the use of Teams on private end device leads to a higher volume of User Chats through private conversations. The respective proportion for employees with Teams on their private end devices is 64 percent, while just 58 percent of employees who do not have Teams on their private end devices share private messages with colleagues. This entails company-relevant security risks, especially if the private content is distributed on an unchecked basis and malicious software is sent to employees, who then pose a risk to the company network.

For this reason, IT managers are required to ensure that all collaboration interfaces are monitored by security solutions, and that all content is protected against loss by backups.

When using groups and channels on collaboration platforms, it is evidently the case that they are not used as frequently as User Chats. This trend is particularly clear in the case of channels that are used in order to coordinate and process projects. For example, more than two-thirds (67 percent) of respondents say that they send User Chats rather than channel messages. On a similar basis to the use of groups, employees tend to seek direct contact with colleagues via direct chats for the purposes of exchanging information or content.

Backups of collaboration solutions are critical to success

For many companies, collaboration solutions have evolved from being a location-independent approach into a platform for project management and collaboration. In this context, it isn't just business-related and private messages that are exchanged, but also data relating to everyday work as well as confidential and business-critical files. Accordingly, some 39 percent of respondents don't just share business-critical and internal documents and messages through direct messages, but also through public groups. Where employees use Teams on private end devices, they are more likely to send critical documents via public groups (43 percent) than those who only use Teams on the work equipment with which they are provided (22 percent).

In the case of the messages that are sent, in addition to private content, it is possible to distinguish between data and messages relating to business operations, and those of an internal and business-critical nature. In this context, it can be seen that employees mainly use Teams in order to share internal and business-critical data.

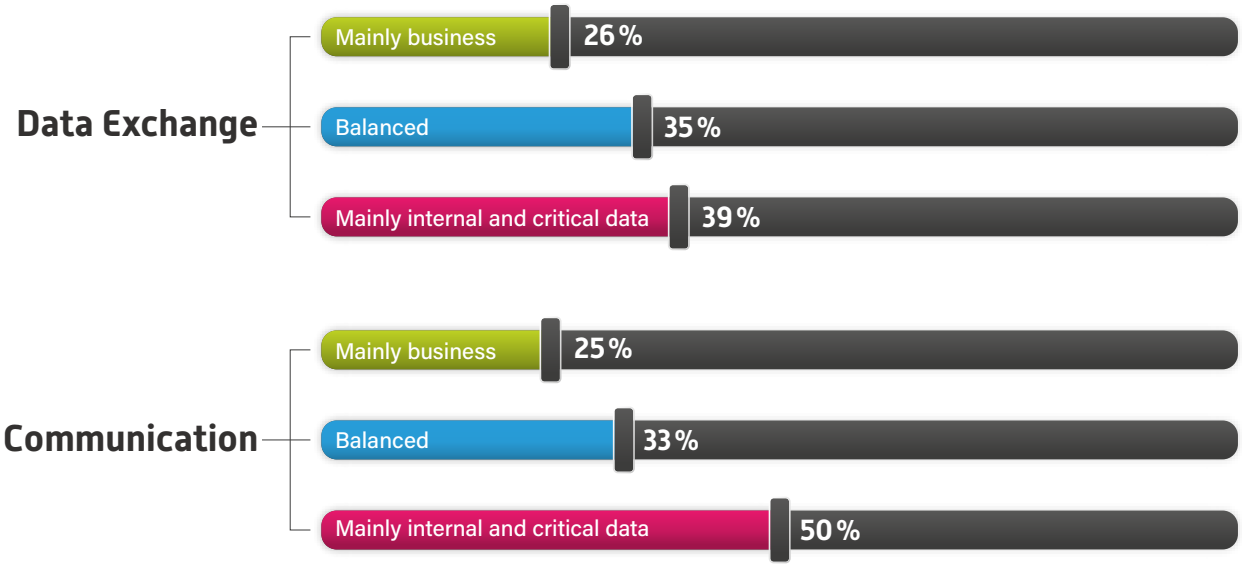
Accordingly, 39 percent of respondents primarily use Teams to send business-critical files, while one in two respondents use it for sending internal and business-critical messages. Only one in four respondents (25 percent) uses Teams to exchange business messages, while 27 percent use it to share business files.

Employees also use Teams as a storage medium for business-critical messages and files, which means it is also important for backup copies of all content to be created.

As regards this sensitive data, it is necessary for IT managers to pay particular attention to security measures within the Teams solution and the company network. After all, security vulnerabilities arise on a regular basis which allow hackers to access not just all the Microsoft services, but also shared business-critical and internal messages and documents.

Mainly use of collaboration tools

Base: 540 Companies



Security vulnerabilities of this kind also allow hackers to erase entire chats, documents and other stored files. If companies use the Teams channels and groups within the solution as a storage medium for company- or project-specific content, the erasure of the stored content can cause considerable damage within the company. For this reason, the principle of the backup also applies in this respect. It is necessary for IT managers to ensure that all of the communications and content within the collaboration solution is saved, and that it can also be restored.

75 percent of respondents also use Microsoft Teams on their private end devices, such as their smartphones or tablets.

In addition to combatting these external threats, backups also provide protection against potential internal threats. After all, cases of accidental or intentional erasure can apply rapidly throughout the entire network, which means that critical data can be lost or even completely destroyed. The results clearly show that such cases of erasure are not uncommon. For example, 42 percent of respondents confirm that their IT managers have already had to restore Teams data through backups. In this case, the related use of private end devices may influence the risk to the data. Almost one in two respondents (47 percent) with Teams on their private end device has had experiences with data recovery using Teams, whereas the percentage of respondents who don't have Teams on their private end device is only 26 percent. It is therefore clear that in this case, the combined use of private and business end devices may pose a security risk within the company.

This is reinforced by the fact that a large proportion of employees are also able to access and use the collaborative solution Teams outside their working hours. 75 percent of respondents also use Microsoft Teams on their private end devices such as their smart-phones or tablets. This high level can be observed equally in almost all size category of company and every country. This mixing of personal and business data is associated with many risks which should be taken into account in the context of the security and backup strategy. In this sense, it may be the case that if permissions are set extensively enough, privately-used apps can also access business-critical data from Teams. Since the IT department has no control over the privately-used end devices, a proactive form of protection cannot be ensured. And in the event of the loss or theft of private end devices, it isn't only possible for data protection breaches to occur, but also risks to the corporate network.

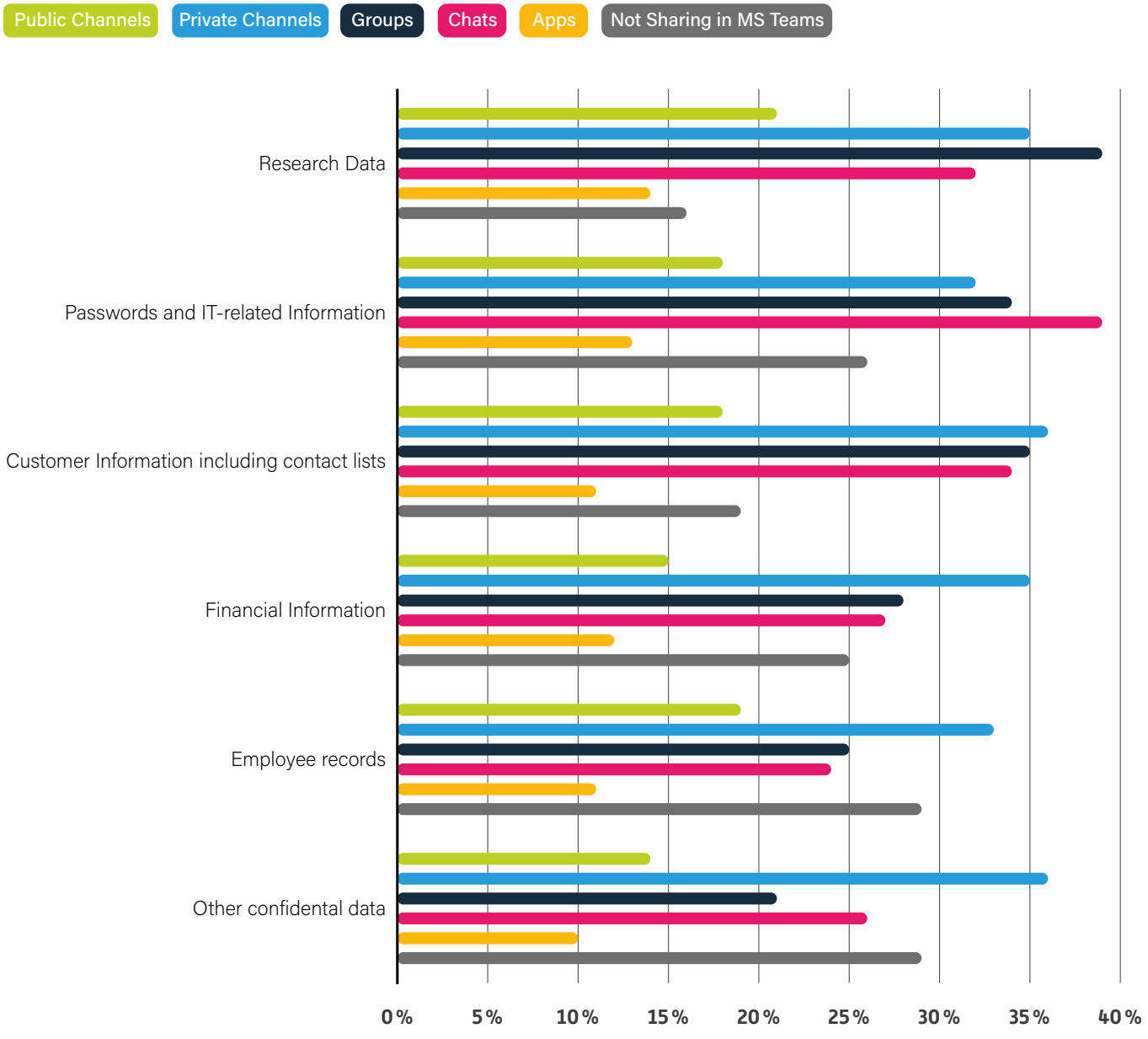
Employees share sensitive data via chats

The exchanging of messages and files via collaboration solutions can include a wide variety of different content. In this respect, it isn't only possible to exchange business-relevant messages, but also sensitive, and in some cases, confidential messages. Accordingly, 39 percent of the employees surveyed send confidential passwords and IT-relevant information directly to colleagues via Teams chats.

As working methods have moved into the digital world, the handling of sensitive information has also changed. For this reason, it is important for Teams content and devices to be secured as part of a comprehensive IT security strategy.

Sending messages and data

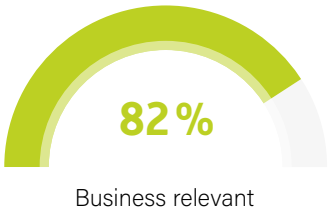
Base: 540 Companies



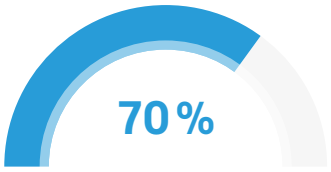
In addition to this, customer data and contact lists are also shared in Teams, especially in private Group Channel Conversations (36 percent). Private or public channels of this kind are particularly suitable for exchanging departmentally-specific information, for example, between the employees in the sales department. However, research data and the associated findings are also shared in Teams groups by 39 percent of the respondents. Overall, depending on the content, requirements and target group, different information is sent within the Teams communication channels. This presents IT managers with the challenge of securing all the content in Teams at all times and restoring the files if necessary.

Frequency of sending different types of data

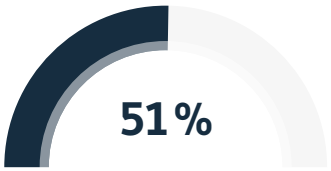
Base: 540 Companies



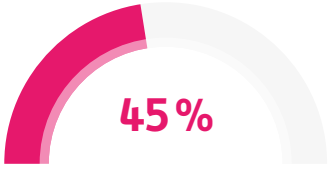
Business relevant



Internal



Business critical



Restricted and confidential

A perspective from a meta level illustrates the different classifications of the exchanged messages. Overall, some 82 percent of respondents send business-related information and messages using Teams frequently to very often, and 70 percent send internal information and messages via Teams. This includes everyday exchanges on the basis of work-related tasks and workflows that affect the company or departments.

In addition to this, more than one in two respondents (51 percent) share business-critical content through Teams. This may include specific operational data, metrics or competitive information that has an impact on the decision-making and strategic direction of the company. In this context, it is striking that respondents with Teams on their private end devices (56 percent) are significantly more likely to share business-critical content than employees without Teams on private devices (36 percent).

The content shared can also be of a confidential nature. In this context, 45 percent of the respondents send confidential information via Teams on a frequent to very frequent basis. Similar to business-critical content, such information is withheld from the company itself and would pose a high risk if it were published or fell into the hands of competitors. Information of this kind tends to be shared more often via Teams in smaller companies than in larger companies. Accordingly, the proportion for companies employing between 50 and 99 people is 54 percent, while in large companies employing 5,000 or more people, only 41 percent of employees share confidential information frequently or very frequently. The effect of private devices can also be seen with this type of content. Accordingly, more than one in two employees (51 percent) with Teams on their private end device share confidential information, whereas the percentage for employees without Teams on their private end devices is only 29 percent. In the event of loss or theft of the private end devices, restricted and confidential data may become public and harm the company. This means that the IT departments have to be proactive and prepared accordingly.

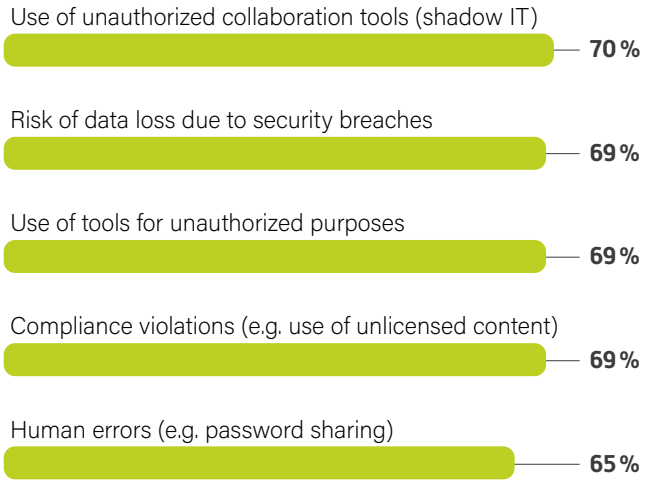
Loss of data as a risk factor when using collaboration solutions

Although the use of collaboration software offers many advantages, it is also possible for risks and challenges to be identified which should also be taken into consideration. Accordingly, 70 percent of respondents perceive the use of unauthorized collaboration solutions alone, and 69 percent, the use of tools for unauthorized purposes, to pose a security risk to the company. Unauthorized software or end devices which are connected to the corporate network as shadow IT can present a risk to security due to security vulnerabilities and remote access.

In addition to this, 69 percent consider the risk of the loss of data due to security vulnerabilities to be a major challenge when using collaboration solutions. Unforeseen security vulnerabilities and cyber attacks can lead to the failure of the deployed collaboration solutions and affect the key information and data of the company. To address these challenges, a proactive backup strategy is required in order to secure and restore all the content from these solutions as required.

Security risks and challenges

Base: 540 Companies | Sum of top 1 and top 2



Other stated risk factors are compliance violations e.g. through the use of unlicensed content (69 percent) and human error (65 percent). Due to carelessness, it is also easy for relevant content and information to be erased in the company network or on collaboration platforms. This can cause considerable damage to the company or cause paralysis.

What companies do to minimize risks:

- **56%** Regular security awareness training
- **49%** Organizational measures
- **45%** Increased use of additional security software
- **34 %** Only use services with advanced security features
- **29 %** Choose providers that comply with data protection
- **25%** Use best practices for Bring Your Own Device
- **4%** We don't know how we can minimise the risks.

To address these potential risks and challenges, 57 percent of companies rely on regular training in order to increase the awareness for security. After all, many risks arise in-house and can be minimized by raising the appropriate awareness amongst the employees, e.g. regarding the use of unauthorized hardware and software. More than two-thirds (67 percent) of the respondents say their awareness has already been raised on the use collaboration solutions and they have received training. In relation to this, almost one in every two companies (49 percent) applies organizational measures and guidelines to control the use of software solutions and to counteract possible risks on a proactive basis.

Another approach is to extend the software-based security architecture. Accordingly, some 45 percent of the companies surveyed are making increasing use of additional security solutions to eliminate the risks and challenges associated with collaboration solutions.

Collaboration is more than just a trend

The results presented show clearly that software-supported collaboration forms an important part of modern working environments. On a daily basis, employees use solutions such as Microsoft Teams to communicate with their colleagues, to complete projects or in order to exchange information or files.

In particular, direct messaging (or User Chat) is preferred over bilateral communication, even where the messaging is possible in groups or channels (or Group Channel Conversations). In addition to this, increasing numbers of messages and files with sensitive content are being shared. Employees don't just use Microsoft Teams to exchange business-related messages at work, but also to share sensitive, business-critical, and classified content. Such an intense and extensive use of solutions like these can lead to falls in productivity or cause greater damage to the company.

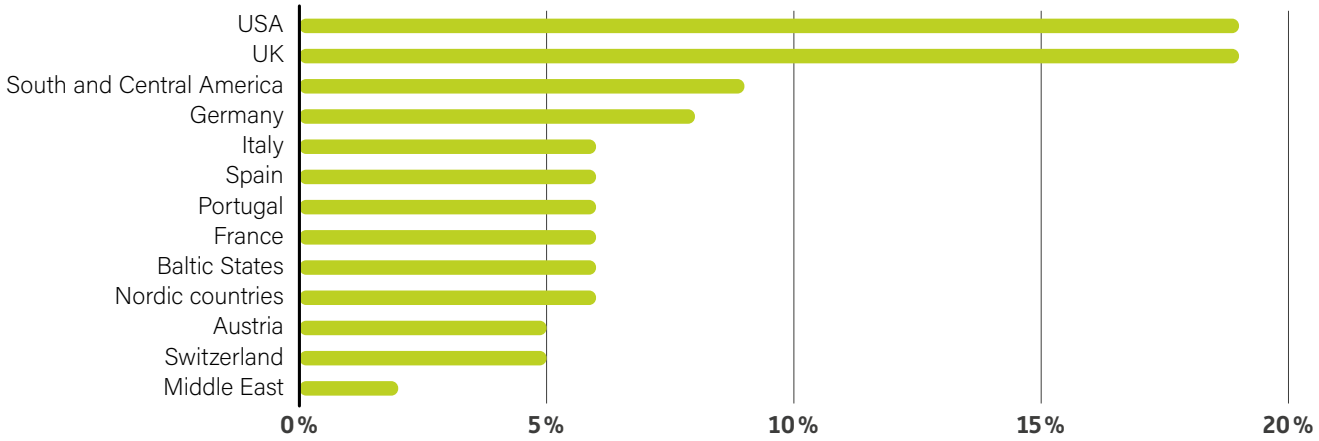
As part of their proactive security strategy, it is therefore necessary for IT managers to ensure that all messages, files and content from the collaboration solutions used are protected with backup solutions. This requirement is reinforced by the fact that company software for workplace collaboration is increasingly being used on private end devices. This increases the risk of cyber attacks, security vulnerabilities or the loss of data due to potential human error.

The use of collaboration solutions will continue to be a part of working life in the future, and is set to be integrated even more closely into workflows and processes. As hybrid working models continue to expand, these solutions will become more important than ever. Accordingly, two-thirds (66 percent) of respondents predict that they will focus more on collaboration solutions in the future. Remote working will therefore continue to be an integral part of the modern working world, with the respective communication and collaboration solutions being decisive and relevant instruments.

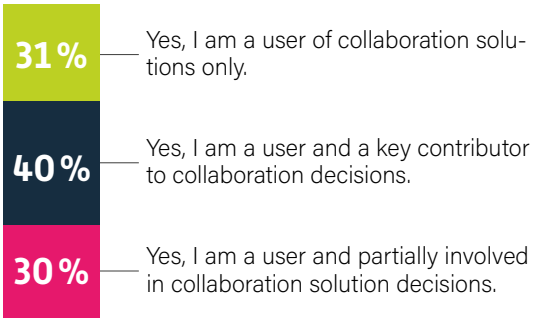
Sample

The study surveyed a total of 540 users of the Microsoft Teams collaboration solution in August 2022. The respondents are pure users, users with significant or conditional decision-making authority regarding the procurement and design of collaboration solutions. Only participants from companies with at least 50 employees from over 16 countries were included. All industries were considered.

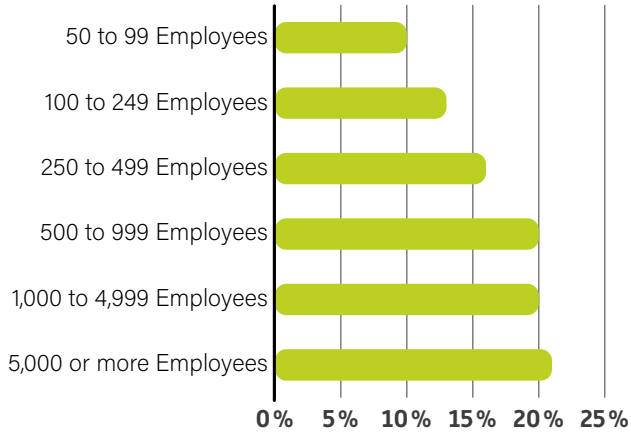
Location



Target group



Employees



Industry

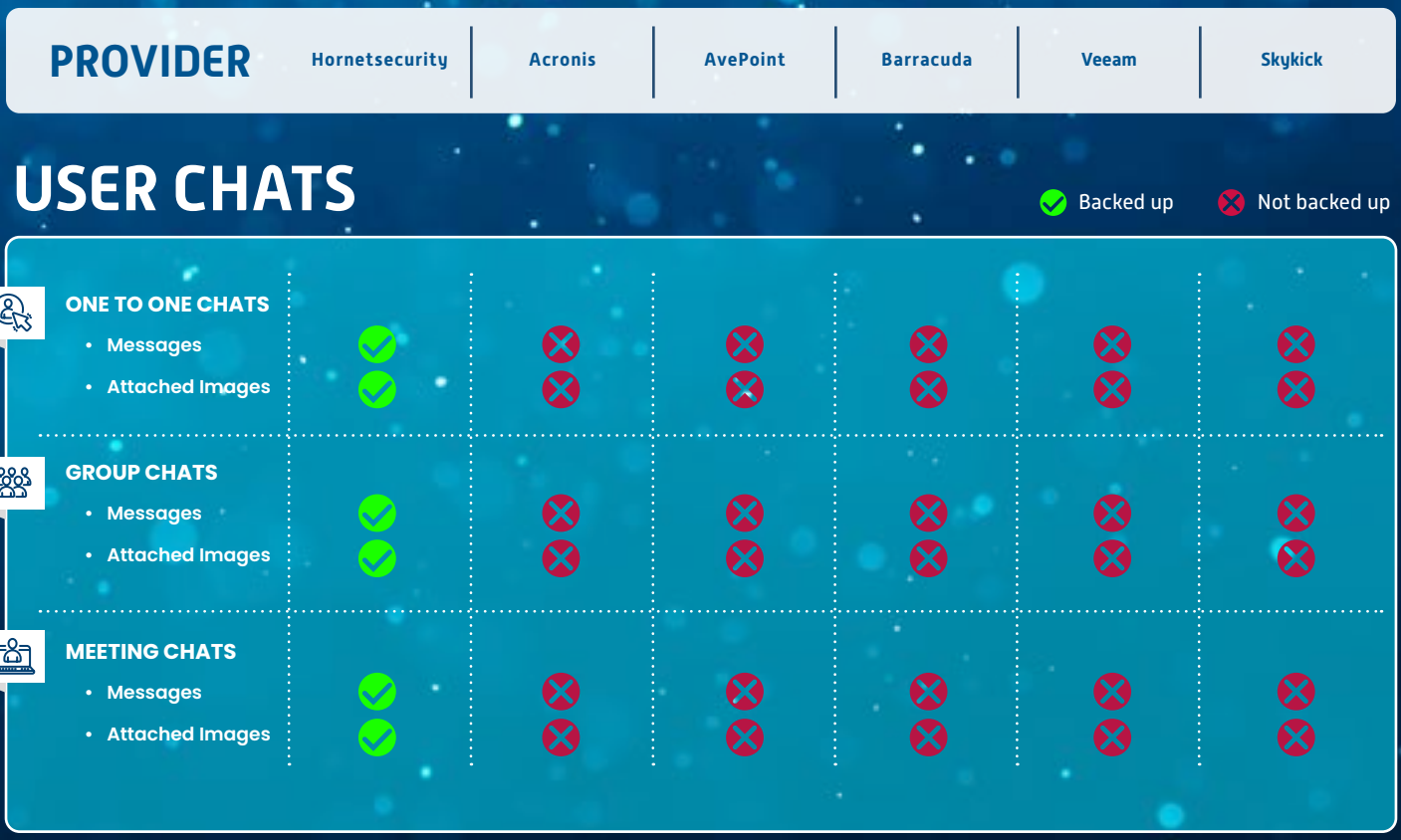
15% Information and Communication
13% Financial and Insurance Activities
9% Other Service Activities
9% Manufacturing
8% Professional, Scientific and Technical Activities
7% Wholesale and Retail Trade; Repair of Motor Vehicles
6% Human Health and Social Work Activities
6% Transportation and Storage
5% Education
4% Administrative and Support Service Activities
4% Construction
3% Public Administration/Defence; Compulsory Social Security
2% Electricity, Gas, Steam and Air Conditioning Supply
2% Accommodation and Food Service Activities
2% Arts, Entertainment and Recreation
2% Real Estate Activities
1% Water Supply; Sewerage, Waste Management
1% Agriculture, Forestry and Fishing
1% Mining and Quarrying

Due to rounding adjustments, some totals may not add up to 100%.

Provider comparison

Microsoft Teams Backup Solutions

A selective competitive review and analysis was also carried out during the quantitative investigation. The scope of services and components of Teams backup solutions from selected providers were examined. The following table shows whether and which Teams communication formats discussed in the study are supported by the backup solutions.



Creation date: 09/28/2022

More information

Contact for more information

Ercan Hayvali
Analyst

Phone: +49 561 8109 178
Mail: **ercan.hayvali@techconsult.de**

techconsult GmbH
Baunsbergstr. 37
34131 Kassel (Germany)

Phone: +49 561 8109 0
Fax: +49 561 8109 101
Web: **www.techconsult.de**

About techconsult GmbH

techconsult GmbH was founded in 1992 and is one of the most well-established analyst firms in Central Europe. The company's strategic consulting services focus on the IT and communications industries. Through long-standing standard and individual studies, techconsult has a unique collection of data in German-speaking countries, with respect to both the continuity and depth of information. It is therefore an important consulting partner for CXOs and the IT industry for product innovation, marketing strategies and sales development.

On behalf of

HORNETSECURITY

Contact

Hornetsecurity GmbH
Am Listholze 78
30177 Hannover (Germany)

Mail: **info@hornetsecurity.com**
Phone: +49 511 515 464 0

Find out more

About Hornetsecurity

Hornetsecurity is a leading global email cloud security and backup provider, which secures companies and organizations of all sizes across the world. Its award-winning product portfolio covers all important areas of email security, including spam and virus filtering, protection against phishing and ransomware, legally compliant archiving and encryption — as well as email, endpoint and virtual machine backup, replication, and recovery. Its flagship product is the most extensive cloud security solution for Microsoft 365 on the market. With more than 400 employees in 12 regional offices, Hornetsecurity is headquartered in Hanover, Germany and operates through its international network of 8,000+ channel partners and MSPs and its 11 redundant, secured data centers. Its premium services are used by 50,000+ customers including Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, and CLAAS.

Media inquiries

Please contact us on **press@hornetsecurity.com**.

A study by

techconsult
TECHNOLOGY MARKET ANALYSTS

Impress

techconsult GmbH
Baunsbergstraße 37
34131 Kassel (Germany)

Mail: **info@techconsult.de**

Phone: +49 561 8109 0
Fax: +49 561 8109 101
Web: **www.techconsult.de**

On behalf of

HORNETSECURITY