Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2021**
Sponsored by **Theta Lake**

Archiving and Data Protection with Microsoft Teams

Executive Summary

The number of people using Microsoft Teams exploded during 2020, driven primarily by the global health pandemic that forced most information workers to work from home. Teams became a seemingly perfect answer to urgent communication and collaboration needs as normal office-based rhythms were suddenly interrupted. User numbers leapt from 20 million in November 2019 to 115 million in October 2020 (and 145 million in April 2021). Users are drawn to the collaboration feature set in Teams, along with its integration into the wider productivity toolset in Microsoft 365.

As users have flocked to Teams, compliance officers, information governance professionals, and other risk management decision-makers are asking whether they have access to the right archiving and data protection capabilities for the many data types produced within Microsoft Teams. While Microsoft offers some native capabilities for archiving and data protection for Teams, third-party archiving and data protection solutions offer a range of elevated capabilities that enable firms to fully satisfy the compliance and privacy regulations to which modern organizations find themselves subject.

Does your organization have access to the right archiving and retention capabilities for the many data types produced within Microsoft Teams?

KEY TAKEAWAYS

Osterman Research conducted an in-depth survey of IT decision-makers specifically for this white paper. Here are the key takeaways from the research:

- **Concerns of Compliance and Legal Professionals Underrepresented**
  The health pandemic of 2020 resulted in rapid growth in usage of Teams and other similar tools. However, compliance professionals and legal staff were two of the three least influential groups in the decision to adopt Teams during the urgency of pivoting operational models and collaboration software in 2020.
- **Declining Confidence in Efficacy of Native Teams Archiving**
  The ability of native archiving capabilities for Microsoft Teams to meet archiving and compliance requirements is expected to wane over the next three years.
- **Compliance the Top Driver, But Legal and Internal Incidents More Common**
  Complying with external regulations is rated as the most important reason for archiving Teams data. However, access to Teams content for eDiscovery requests and internal investigations happened more frequently than producing evidence from Teams for a compliance audit.
- **Many Respondents Underplay the Importance of Capturing Data in Teams**
  Only one third to one half of respondents say it is highly important to be able to search and produce various content types in Microsoft Teams.
- **Top Reasons for Third-Party Archiving Solutions**
  Survey respondents ranked three reasons as the most important for using third-party archiving solutions with Teams: in-place search across multiple platforms and content repositories, capturing the full range of data types in Teams, and gaining a single platform for both Microsoft and non-Microsoft data types.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Theta Lake. Information about Theta Lake is provided at the end of the paper. This paper references data from an in-depth survey of 142 IT decision-makers in mid-sized and large organizations, all of whom are currently using Teams. The survey was conducted specifically for this paper.

Adoption of Microsoft Teams

In this section, we review the publicly available numbers on adoption of Microsoft Teams and similar platforms, and report on the growth in usage of Teams among survey respondent organizations from several perspectives.

ADOPTION OF TEAMS AND OTHER SIMILAR PLATFORMS

The adoption of Microsoft Teams and other similar platforms grew significantly during 2020, with the response to the health pandemic the main driver:

- **Strong Uptake of Teams by Organizations from 2017 to 2018**
  After one year in market in March 2018, Microsoft said Teams was used in 200,000 organizations in 181 markets and 39 languages.[1] Six months later, the number of organizations using Teams had grown to 329,000.[2] In order for an organization to be counted, however, only one person per organization had to be using Teams (although many organizations had many more than this).
- **Fight for Daily Active Users in 2019**
  Microsoft published its first daily active user statistic in July 2019: 13 million daily active users of Teams and 19 million weekly active users, in comparison to only 10 million daily active users for Slack.[3] By November, daily active users stood at 20 million.[4]
- **Surging Adoption in March-April 2020**
  And then COVID hit. In March 2020, Teams usage leapt from 32 million to 44 million daily active users in a single week. The rate of people using video in calls doubled and video call usage increased ten times.[5] By October, there were 115 million daily active users of Teams, almost six times as many as in November the year before.[6] In April 2021, Teams hit 145 million daily active users.[7]
- **Growth in Slack Usage**
  Slack usage increased 25% in two weeks in March 2020, from 10 million to 12.5 million simultaneously connected users.[8]
- **Growth in Zoom Usage**
  Usage of Zoom surged in March 2020 to 200 million daily meeting participants using Zoom for remote working and learning. In April 2020, Zoom claimed 300 million daily meeting participants, which is however a different metric to daily active users.[9] The pre–March 2020 usage level was approximately 10 million daily meeting participants at most.[10] Zoom's rapid uptake brought several security weaknesses and design oversights to light, which Zoom sought to address rapidly.

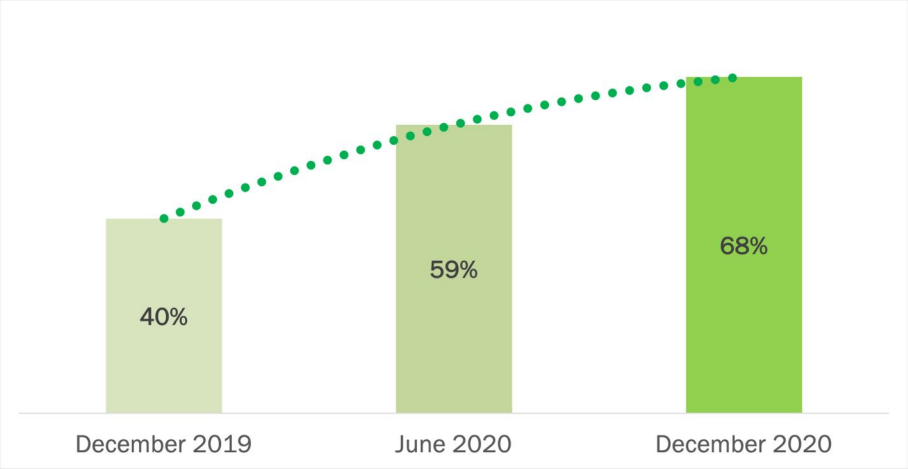
The health pandemic of 2020 had a rapid, significant, and unanticipated impact on the adoption of Teams and similar tools.

The pivot to hybrid work bodes well for ongoing usage of Teams and similar tools. Many organizations have reported meaningful productivity gains from Teams, and Microsoft is no longer offering Skype for Business.

INCREASING ADOPTION OF MICROSOFT TEAMS

The growing momentum behind Microsoft Teams globally was also evident among the survey respondents. Adoption increased by 50% in the first six months of 2020 during the height of the health pandemic. In the 12 months from December 2019 to December 2020, adoption increased from 40% employee coverage to almost 70% employee coverage. See Figure 1.

Figure 1
Employees Using Microsoft Teams for Day-to-Day Tasks
Percentage of employees

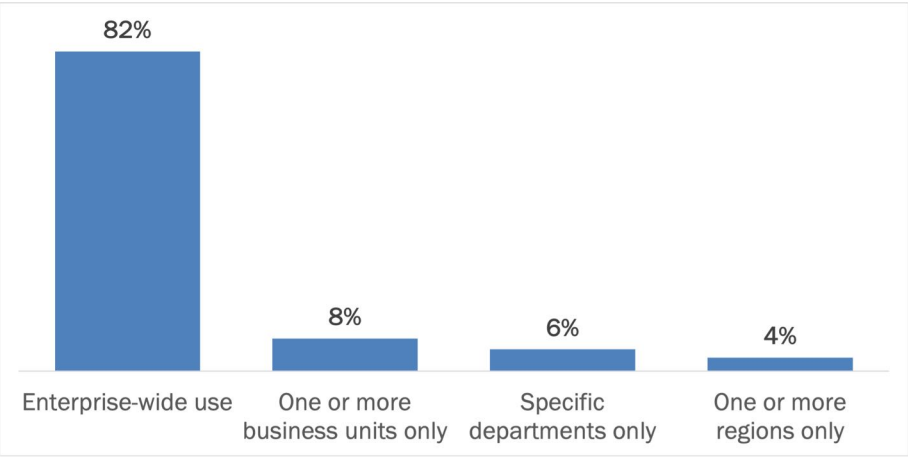


Source: Osterman Research (2021)

HIGH INTENT FOR ENTERPRISE-WIDE DEPLOYMENT

Most survey respondents are planning an enterprise-wide deployment of Microsoft Teams. Four out of five respondents are planning for a full roll-out to all employees. One in five are planning for lesser deployments, with a business unit–level deployment the most common of the three other options. See Figure 2.

Figure 2
Scope of Planned Deployment for Microsoft Teams
Percentage of respondents



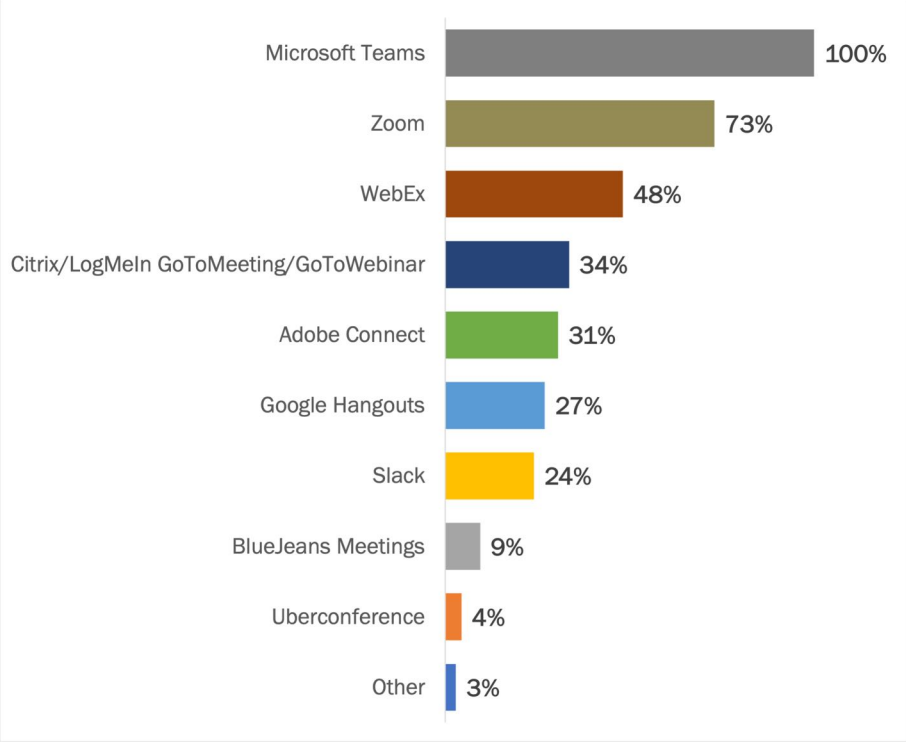
Source: Osterman Research (2021)

Adoption of Teams almost doubled during 2020, and most respondents are planning an enterprise-wide deployment.

WIDESPREAD USAGE OF OTHER SIMILAR TOOLS

Almost all respondents indicated one or more similar tools to Microsoft Teams were also in use in their organization, with several online meeting, webinar and video conferencing services the most highly used. Four out of ten respondents used three or more additional tools. Note that the survey did not gauge the extent of employee coverage for each of these tools, only whether they were used within the respondent's organization. See Figure 3.

Figure 3
Usage of Other Tools Similar to Microsoft Teams
Percentage of respondents



Source: Osterman Research (2021)

Almost all organizations use other similar tools as well as Microsoft Teams.

Zoom and Slack are often positioned as the two key competitors to Teams. Among the respondents to this survey, Teams is sometimes used in conjunction with Slack (24%) and frequently used in tandem with Zoom (73%).

REASONS FOR INCREASING ADOPTION

Supporting employees working from home was the most critical reason for increased adoption in 2020 (77% of respondents). Faced with the sudden loss of face-to-face modalities afforded by office-based operations, many organizations scrambled to recreate the semblance of office-based working in an era of forced shelter-in-place orders and work-from-home edicts.

Two other reasons for increased adoption of Microsoft Teams during 2020 deal with more fundamental transformation of work processes, and these were less important drivers for the adoption curve in 2020. Interacting with customers and clients was highly important to 45% of respondents and working with supply chain partners was highly important to 37% of respondents.

IMPLICATIONS OF INCREASING ADOPTION

The pattern of adoption of Microsoft Teams and other tools has several implications for archiving and data protection. Implications of concern from this research are:

- **Data Requiring Archival Flows from Multiple Tools**
  Organizations that archive and protect data must deal with a heterogeneous landscape of content sources, even just from the perspective of Microsoft Teams and similar tools. Almost all organizations represented in this survey have two content sources from this category producing content that may be subject to archival requirements, and almost three in five organizations have three content sources from this category to deal with.
- **Handling Modern Attachments**
  Legal teams are struggling with the concept of modern attachments. By default, a link to the attachment is preserved, not the content in the attachment at the time of sharing the link.
- **New Features Deployed by Microsoft as On by Default**
  Microsoft often deploys new features in Teams as on by default, sometimes without sufficient notice to customers. Compliance teams must scramble to address the new challenges. Microsoft's release of native compliance capabilities often lags behind the release of productivity capabilities.
- **Growing Data Volumes from Microsoft Teams**
  As goes employee adoption so goes data volume, and the increased use of new video and audio features have an exponential impact on data volumes. More employees using Microsoft Teams results in growing volumes of data that may be subject to archival and data protection requirements.
- **Tool-Based Approaches to Archiving Do Not Scale**
  With organizations using multiple tools, even within the same category grouping as Microsoft Teams, the strategy of using tool-based information governance capabilities becomes an approach that is not scalable nor fit for purpose. Different tools will offer varying capabilities and approaches for archiving, data protection, legal hold, supervision, and eDiscovery, making it difficult to gain unified controls across all content.
- **Content Residue in Teams from 2020**
  It remains to be seen if the rapid uptake of Microsoft Teams during 2020 to support employees working from home during the health pandemic translates into ongoing usage as the threat of the pandemic subsides and people head back to the office. If usage does continue—and hybrid work designs would support ongoing usage—organizations will need to play catchup on archiving and data protection requirements. Regardless, content generated in Teams during 2020 must be retained and protected in compliant ways.

Tool-based archiving approaches do not scale; organizations are already using multiple tools within the same category as Microsoft Teams.

Archiving and Data Protection Mandate

Many organizations face archiving and data protection requirements that extend to content in Microsoft Teams. In this section, we consider the mandate.

A NOTE ON TERMINOLOGY

Microsoft offers two native capabilities in Microsoft 365 to address archiving and compliance for Microsoft Teams: workspace archiving and retention policies.

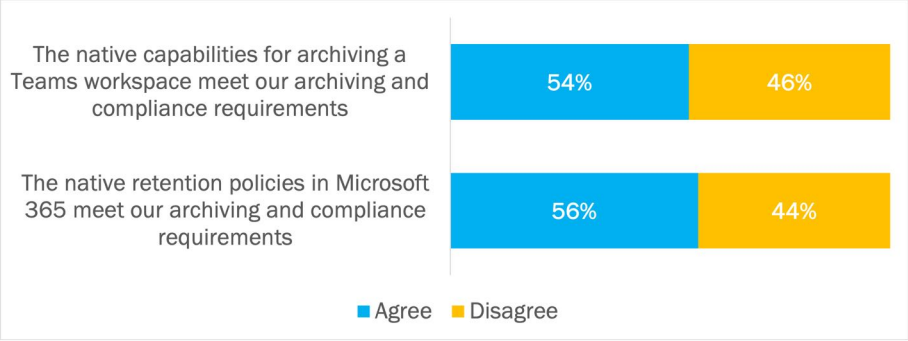
- **Archiving a Teams Workspace**
  The native capability in Microsoft 365 to archive a Teams workspace locks it from further activity. It is intended for use when a workspace reaches end of life because the project or initiative has ended. However, a workspace owner or a Microsoft 365 administrator with the appropriate rights can still permanently delete the workspace and all associated content. There are non-compliance and eDiscovery spoliation risks with this capability. It can assist with user-level workspace management, but not with regulatory compliance requirements.
- **Retention Policies Over Teams Content**
  Microsoft's native retention policies provide some capabilities to prevent deletion, modification, and unauthorized access to data in Microsoft Teams. Conceptually, what retention policies offer is a closer fit with the archiving and data protection requirements of compliance professionals. Retention policies can be configured to cover some—but not all—of the data in Teams.

LOW EFFICACY OF NATIVE ARCHIVING AND RETENTION POLICIES

Just over half of survey respondents assessed the native archiving and retention capabilities in Microsoft 365 for Microsoft Teams as meeting their requirements. Slightly more assessed native retention policies (56%) meeting their needs compared to native capabilities for archiving a workspace (54%). See Figure 4.

Just over half of respondents believe Microsoft's native capabilities for archiving and data protection for Microsoft Teams meet their requirements.

Figure 4
Assessment of Native Archiving and Retention Capabilities for Microsoft Teams
Percentage of respondents indicating strong agreement vs. weak agreement and disagreement with each statement



Source: Osterman Research (2021)

While respondents felt native retention capabilities were more suitable than native archiving capabilities—a perspective we agree with—the ratings for both are low.

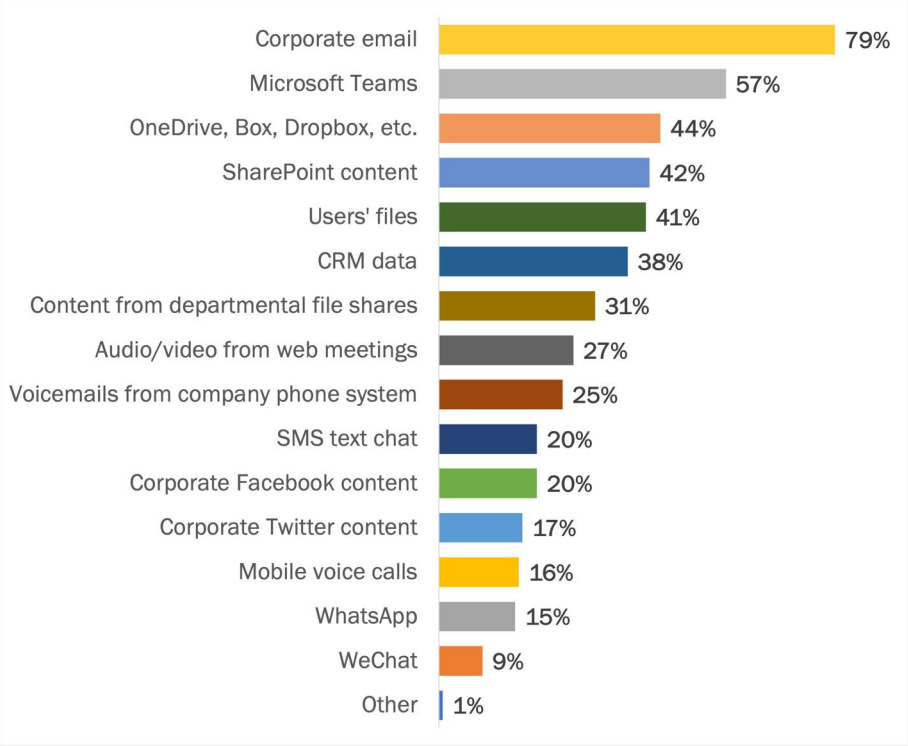
ORGANIZATIONS ARE ALREADY ARCHIVING ELECTRONIC CONTENT

Almost all the organizations reflected in this survey are already archiving electronic content. Three out of four organizations are already archiving content from three or more sources. Archiving was defined as:

- Archiving is the use of an on-premises or cloud-based system that places content into secure, immutable storage to satisfy regulatory or internal records retention requirements, indexes content, and provides robust search tools to find and produce this stored and indexed content.
- Archiving is different from backup. Backup systems enable data recovery in the event of a system failure or data corruption.

Corporate email is the leading content type to be archived (by four out of five), followed by Microsoft Teams (by three out of five). Note that Microsoft Teams in this question was included as a singular data type, although in reality, Teams is a framework for a dynamic set of multiple intertwined complex data types. See Figure 5.

Figure 5
Electronic Content Being Archived Currently
Percentage of respondents



Source: Osterman Research (2021)

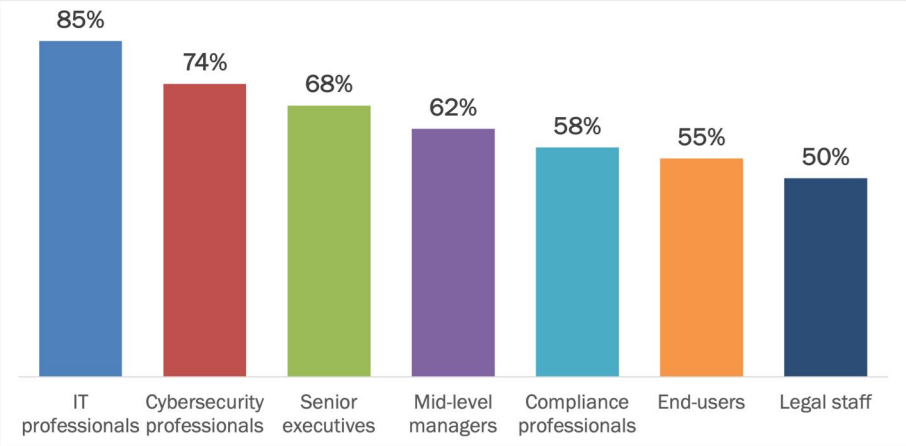
Three out of four organizations are already archiving content from three or more sources.

The difference between current practice and full compliance with archiving mandates is concerning, although this comment must be moderated by the observation that not all respondents were necessarily using all of the electronic content sources listed above. For this research, we can state that although 100% of respondents are using Microsoft Teams, just under 60% believe they are currently archiving at least some of the content types in Microsoft Teams properly.

LEGAL AND COMPLIANCE PROFESSIONALS UNDERREPRESENTED

Compliance professionals and legal staff were two of the three least influential organizational groups in the decision to adopt Microsoft Teams. IT professionals held the highest level of influence across the organizations represented in this survey. See Figure 6.

Figure 6
Adopting Microsoft Teams: Influence by Group
Percentage of respondents indicating "Very influential" or "Extremely influential"



Source: Osterman Research (2021)

The challenge of low participation in the decision-making process is that the concerns of those in compliance and legal roles are underrepresented, which raises risks associated with non-compliance and legal exposure. The rapid drive to adopt Microsoft Teams in 2020 to support work-from-anywhere arrangements has typically been made without adequate consideration for archiving and data protection concerns.

Compliance professionals and legal staff were two of the three least influential organizational groups in the decision to adopt Microsoft Teams.

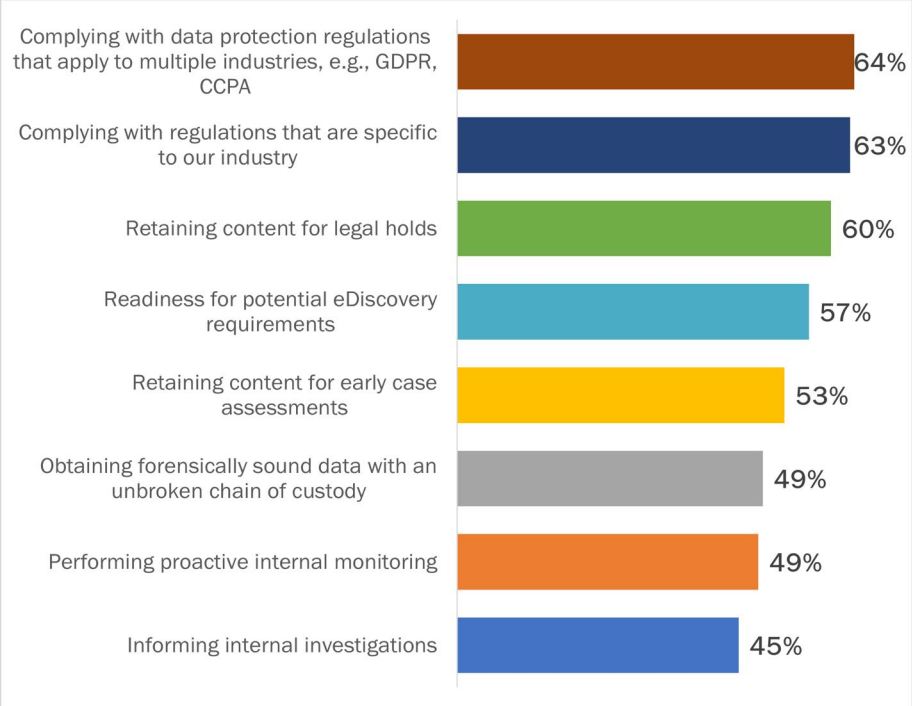
REGULATORY COMPLIANCE, LEGAL AND EDISCOVERY DRIVERS

Complying with general data protection and industry-specific regulations are the two highest-ranked reasons for archiving and protecting data in Teams, with several legal and eDiscovery concerns in third, fourth and fifth places. Internal monitoring and internal investigations were the least important drivers for archiving. See Figure 7.

In looking at the wider context of the answers to this question:

- **Half of Respondents Ranked Five or More Reasons as Highly Important**
  49% of respondents to the survey said that five or more of the eight reasons in the list were very or extremely important to their organization. For 26% of respondents, all eight reasons were very or extremely important.
- **Industry Matters**
  The industry in which the respondent worked was correlated with the answers to this question. For 67% of respondents in life sciences and 52% of respondents in financial services, five or more of the reasons were highly important. By comparison, only 15% of respondents in the insurance industry said the same.

Figure 7
Drivers for Archiving and Data Protection in Teams
Percentage of respondents indicating "Very important" or "Extremely important"



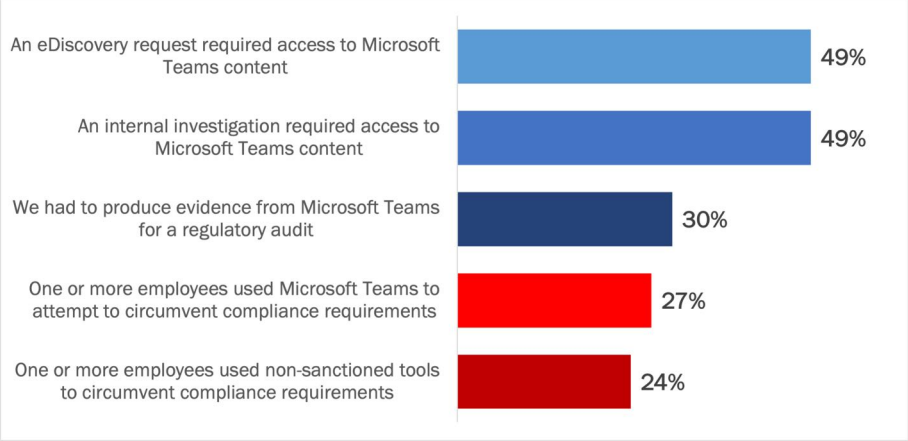
Source: Osterman Research (2021)

INCIDENTS OVER THE PAST 12 MONTHS

Three out of four respondents experienced at least one of the five incident types below at their organizations over the past 12 months, with just under half seeing two or more of the incidents. It is interesting to observe that the first-equal incident type—an internal investigation requiring access to Microsoft Teams content—was the least important driver for archiving content in Teams. See Figure 8.

Informing an internal investigation was the least important driver for archiving content in Teams yet is the first-equal incident type over the past 12 months.

Figure 8
Incidents Over the Past 12 Months
Percentage of respondents



Source: Osterman Research (2021)

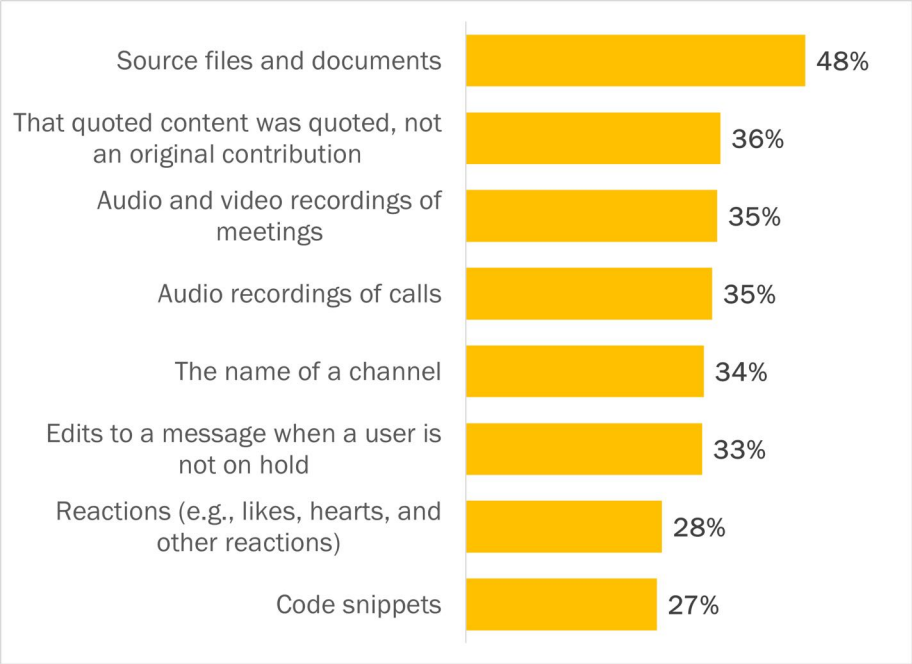
About a quarter of respondents have experienced two types of deliberate insider actions by employees over the past 12 months to circumvent compliance requirements, including via the use of Microsoft Teams. A tool like Teams offers multiple ways for insiders to cover their tracks, such as creating a chain of innocuous-sounding messages dispersed across multiple channels, creating and editing or deleting messages so they would not persist, using unmonitored whiteboard, voice, or screen sharing features in an attempt to circumvent archiving controls, using Teams in combination with other message formats (e.g., text messages), using code words to obfuscate intent, or leveraging capabilities in Teams that are not archived nor subject to eDiscovery searches (e.g., code snippets). People have proven adept at finding creative ways to attempt to conceal their tracks when necessary.[11] While a quarter of respondents had the optics to detect such insider actions, it is likely that many other organizations have also experienced insider actions which have gone undetected.

NATIVE CAPABILITIES IN TEAMS EXCLUDE CONTENT TYPES

When an eDiscovery search in Microsoft 365 is executed for content in Microsoft Teams, certain content is excluded from the search results even if full native archiving and retention capabilities are used. Half of respondents are highly concerned that source files and documents are excluded, and about one third of respondents are highly concerned about the other excluded types, such as the name of a channel in which a conversation happened. See Figure 9.

27% of respondents said one or more employees used Microsoft Teams to attempt to circumvent compliance requirements.

Figure 9
Concern About Excluded Content Types in eDiscovery for Microsoft Teams
Percentage of respondents indicating "Very concerned" or "Extremely concerned"

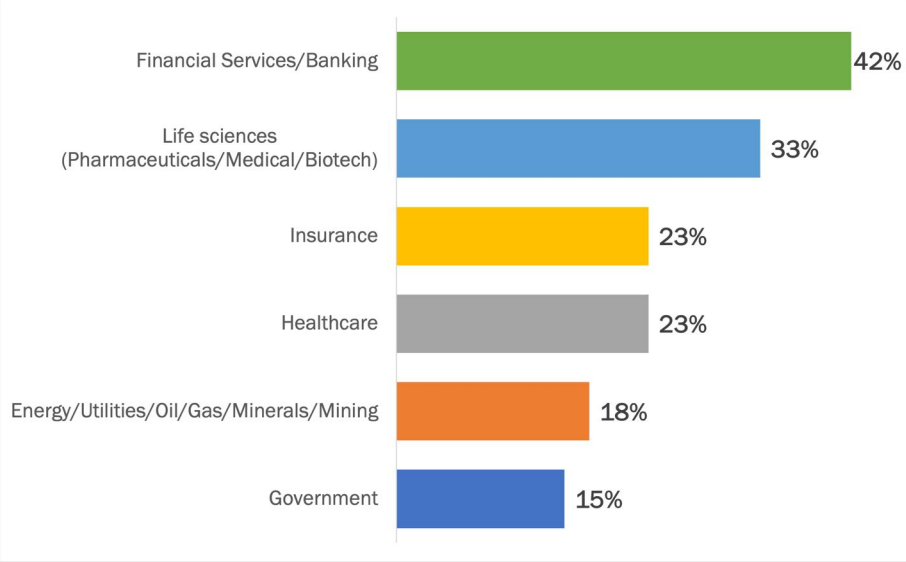


Source: Osterman Research (2021)

The inability to find responsive content should be of high concern to organizations under both legal proceedings and internal investigations. However, there is also an industry influence at play in how this question was answered. Respondents from

two industries—financial services and banking (42%) and life sciences (33%)—registered higher levels of concern on at least five of the eight exclusions than respondents in the other industries covered by this research. See Figure 10.

Figure 10
Industry Concern About Excluded Content Types in eDiscovery for Teams
Percentage of respondents by industry indicating five or more "Very concerned" or "Extremely concerned" rating on excluded content types



Source: Osterman Research (2021)

Among financial services respondents, 27% registered high concern on all eight exclusions, and 17% of life sciences respondents did the same.

Respondents from the financial services and life sciences industries register higher concern about excluded content than respondents in other industries.

THE DATA PROTECTION MANDATE

Survey respondents ranked complying with data protection regulations that apply to multiple industries, such as GDPR and CCPA, as the top ranked driver for archiving and data protection in Teams (see Figure 7 earlier). Specific regulations that impose data protection mandates include:

- **General Data Protection Regulation (GDPR)**
  Europe's GDPR introduced sweeping changes to how personal data on European data subjects had to be protected, afforded a new set of rights to data subjects, and eliminated the geographical factor in defining which organizations had to comply with the regulation. Falling afoul of GDPR is costly. Complying with GDPR includes an emphasis on aligning technological solutions with organizational and administrative ones, which by nature should include taking a strong approach to information governance (including archiving).
- **California Consumer Privacy Act (CCPA)**
  The CCPA incorporates several of the data protection principles of the GDPR into California state law, including access, disclosure, and deletion rights by data subjects. Organizations subject to the CCPA—including businesses outside of California's geographical boundaries that buy, receive, sell, or share the personal data of 50,000 or more Californian consumers, households, or devices per year—must implement organizational and technical measures to ensure data protection for personal information.

- **Health Insurance Portability and Accountability Act (HIPAA)**
  Health care providers, health plans, and healthcare clearinghouses—along with other covered entities in the United States healthcare system, e.g., business associates—are required to securely retain and protect health records for six years under the Health Insurance Portability and Accountability Act of 1996 and its subsequent updates. The HIPAA Privacy Rule covers all individually identifiable health information in electronic, physical, and oral formats. The requirement to protect individually identifiable health information from data breaches, inadvertent access, and inappropriate usage is part of the data protection mandate. The requirement to securely retain such data could also be listed separately in the next section.

Archiving data from Microsoft Teams using third-party solutions also has data protection benefits, for example:

- **Reducing Unauthorized Access Through Phishing Attacks**
  Workspaces in Microsoft Teams that are no longer needed can be deleted because complete archived data is available in a third-party system. A successful phishing attack, therefore, will be able to access fewer workspaces and less data.
- **Reducing Credential Compromise Through Various Means**
  Credentials compromised through any form of attack, including phishing, brute force, and the purchase of breached credentials on the dark web, will result in a reduced breach space if non-current data has been moved to a third-party archival system.

Archiving data from Microsoft Teams using third-party solutions also has data protection benefits.

THE ARCHIVING MANDATE

Regulations that impose strict requirements for archiving include:

- **FINRA Rules 3110, 3120, 4511 and 11-39 (Social Media)**
  The Financial Industry Regulatory Authority (FINRA) in the United States imposes strict archiving and supervision rules on financial services firms to protect markets against insider trading and misconduct. Rules 3110 (Supervision) and 3120 (Supervisory Control System) require the creation of a supervision system for reviewing "incoming and outgoing written (including electronic) correspondence and internal communications relating to the member's investment banking or securities business."[12] The system needs to capture all communications in their original form, with capabilities to enable supervision. Data must be retained for eight years on indelible media—per Rule 4511—with immediate access to all communications during the first two years of data retention. Firms are required to keep a duplicate copy of all communications at an offsite location during the eight-year retention timeframe. Rule 11-39 imposes an obligation to preserve social media communications when the content is a business communication.
- **SEC Rule 17-a4**
  The Securities and Exchange Commission (SEC) in the United States imposes archiving and data protection requirements on financial services firms. Rule 17-a4 requires the orderly preservation of electronic records in a way that prevents editing or deletion. The efficacy of the media recording process must be verified, and a duplicate copy of records must be stored separately from the original content. Content must be retained for between three and six years, depending on the type of record.

- **SEC Rules 204 and 206**
  The SEC imposes archiving and data protection requirements on investment advisors, hedge funds, and private equity firms. Under Rule 204(2), various records must be retained for five years and preserved using immutable storage. These records must be arranged and indexed to support search, retrieval, and access. Rule 206(4)-(7) requires the creation of a supervisory system to protect the privacy of client records, monitor disclosures by advisors, and preserve records from unauthorized changes, among other requirements.

- **MiFID II**
  In Europe, the Markets in Financial Instruments Directive II (MiFID II) imposes elevated and harmonized requirements on record-keeping for transactions and communications in the financial services industry. All communications from brokers and financial consultants must be recorded and archived in tamper-proof storage, a requirement which explicitly includes phone and video calls.

- **FinVermV**
  The Ordinance on Financial Investment Mediation in Germany—or the *Finanzanlagenvermittlungsverordnung*—applies to banks, liability umbrellas, some asset managers, financial investment brokers, and some financial investment advisors. From August 2020, covered entities must record certain communications to clients regarding financial investments, including communications by phone. Immutable storage is required for up to 10 years, with accessibility at all times from the business premises. Transcripts of voice calls must be produced and analyzed for mandatory compliance statements, fraud detection, and categorization. FinVermV transfers the protections afforded to consumers in MiFID II into Germany's regulatory framework.

- **SOX**
  The Sarbanes-Oxley Act in the United States introduced elevated recording and reporting standards for public company boards in the United States, executives, and public accounting firms. Records of various financial transactions and related communications at covered entities must be retained securely for up to seven years—including protections from modification and unauthorized access—and be available on request for review by the SEC. Since more than 80% of respondents to this survey were planning an enterprise-wide deployment of Microsoft Teams (thus covering financial processes), any respondents covered by SOX who are using Teams for financial processes will need to ensure compliance with its archiving and data protection provisions.

- **FERC**
  In the energy market, the Federal Energy Regulatory Commission (FERC) imposes record retention and protection requirements for various types of documents and communications. For example, service contracts must be retained for four years, and the minutes of several types of corporate meetings have to be retained for five years.

Regulations in Europe and Germany are explicitly requiring capture and archiving of voice and video calls, including transcript production and analysis for fraud.

The above sampling of regulations imposes strict external requirements for the retention and protection of various types of data. Any organization subject to these regulations must archive Teams content. But in addition, the two most common incident types that organizations have experienced over the past year (per Figure 8) requiring access to Teams content were for eDiscovery and internal investigations, e.g., for an internal discrimination claim, harassment allegation, or for early case assessment. These are universal needs, and therefore organizations must archive Teams content in order to satisfy eDiscovery and internal investigation demands.

CONFLICTING USER PREFERENCES AND COMPLIANCE REQUIREMENTS

It is not uncommon for users of a product to seek capabilities that conflict with the compliance requirements governing the use of the product. Recent history shows that the productivity argument more frequently wins in the battle with compliance. In the majority of cases, productivity features that conflict with a compliance mandate reduce friction and streamline adoption for users, although in a minority of cases, people will use such capabilities to intentionally cover wrongdoing. Firms need to meet both productivity and compliance requirements, which often requires specialized compliance tools alongside the collaboration infrastructure.

For Microsoft Teams, many users have requested the following capabilities that create challenges for meeting compliance mandates covering archiving and data protection.[13] Figure 11 lists three items from UserVoice along with our analysis of the tension between the user benefit and the compliance challenge.

Figure 11
High-Ranked User Requests for Teams That Introduce Compliance Challenges
Number of votes by registered users on UserVoice

Title (Votes, Rank)	User Benefit	Compliance Challenge
Move a project (channel) from one team to another 30,234 votes 3rd highest	A workspace in Teams always shows only current and relevant projects. Projects (in a channel) can be started on one team and easily moved to another.	Loss of wider point-in-time context when analyzing the conversations in a Teams workspace. Conversations in a channel that has been subsequently moved could potentially be responsive.
Delete private chat threads 19,209 votes 6th highest	Old and unnecessary conversations can be removed from the private chat window.	Destruction of potentially responsive evidence, either solely in private chat or as part of a multi-tool obfuscation.
Move conversations to different channels 11,104 votes 11th highest	A channel in Teams always shows only current and relevant conversations. Users do not have to worry about starting a conversation in the perfect channel initially, because it can always be moved later.	Loss of wider point-in-time context when analyzing the conversations in a Teams workspace. Conversations in a channel that have been subsequently moved could be potentially responsive, and the conversation could be moved to a workspace that can be deleted.

Source: Three Items from UserVoice, with Analysis by Osterman Research (2021)

Users of Microsoft Teams are requesting capabilities that conflict with the compliance requirements governing the use of Teams.

Over 67,000 requests have been lodged by users for new features in Microsoft Teams, and while many move the product forward in a beneficial way, others raise significant compliance challenges. If Teams becomes a system that supports high fluidity in movement and reorganization of people, conversations, and projects across Teams workspaces, being able to pinpoint wrongdoing in a regulatory compliance situation—or even for an internal investigation—will become increasingly difficult without strident retention of data elements and the ability to re-create an accurate and complete point-in-time view.

ARCHIVING OF MICROSOFT TEAMS IN SMALLER BUSINESSES

Archiving of Microsoft Teams in small businesses—those with 50 or fewer employees—was beyond the scope of the survey conducted for this research. How should small businesses approach the issue of archiving content in Microsoft Teams? Considerations and perspectives include:

- **Industry Requirements for Compliance**
  Industry and organizational size are independent factors. For example, financial services firms of any size that must comply with FINRA and SEC rules will need data archiving capabilities beyond what is offered natively in Microsoft Teams.
- **Potentially Fewer Platforms and Platform Variations**
  Smaller firms are likely to have fewer sanctioned and official data-producing platforms than larger firms, because there are fewer people and therefore less room for variation in preferences. However, the easy availability of mobile apps has clouded this situation due to easy accessibility to rogue and unsanctioned applications that employees self-select for critical work processes.
- **Greater Potential for Extensive Data Exfiltration, Deletion, and Leakage by Rogue Employees**
  Administrators, executives, and employees are likely to have access rights to a broader selection of data than at larger firms. Such rights increase the risks of intentional or inadvertent sharing, leakage, or deletion of sensitive confidential information by employees. The ability for a single employee to disclose or delete information through Teams that would result in severe regulatory, privacy, security, or reputational harm to the firm must be managed appropriately. Managing every capability of Teams—webcams, screen shares, file transfer, and chat—for potential exposure is essential. At a small business with a single IT administrator, for example, one person has full deletion rights over all business systems and data. If that administrator—or an executive with a similar span of control—were to go rogue, the consequences would be dire.
- **Greater Reliance on Fewer Employees**
  Smaller organizations do not have the personnel to support the division of duties and interchangeability through co-training that is available in larger organizations. Fewer employees, therefore, have broader responsibilities, and without strong archiving controls, the ability to rebuild a comprehensive understanding of a department-of-one or business process run by one person is compromised when an employee leaves or dies unexpectedly.
- **No Immunity from Legal Challenges and Internal Misconduct**
  Being small does not grant immunity to legal challenges and eDiscovery requests, insider threats, misconduct, or allegations of harassment.
- **Fewer Resources for Information Governance**
  Being a small business is more likely to mean the financial resources to hire a full-time information governance professional are harder to allocate than for a larger firm. While this can appear like a sufficient reason to ignore the information governance challenge, it more accurately signals the need to select archiving, data protection, and supervision tools that reduce complexity and run automatically without requiring a high degree of manual effort to get right.

While a small business may decide that native capabilities in Teams are suitable to their archiving and data protection requirements, being a small business does not automatically mean that high-fidelity archiving is unimportant.

Being a small business does not automatically mean that high-fidelity archiving is unimportant.

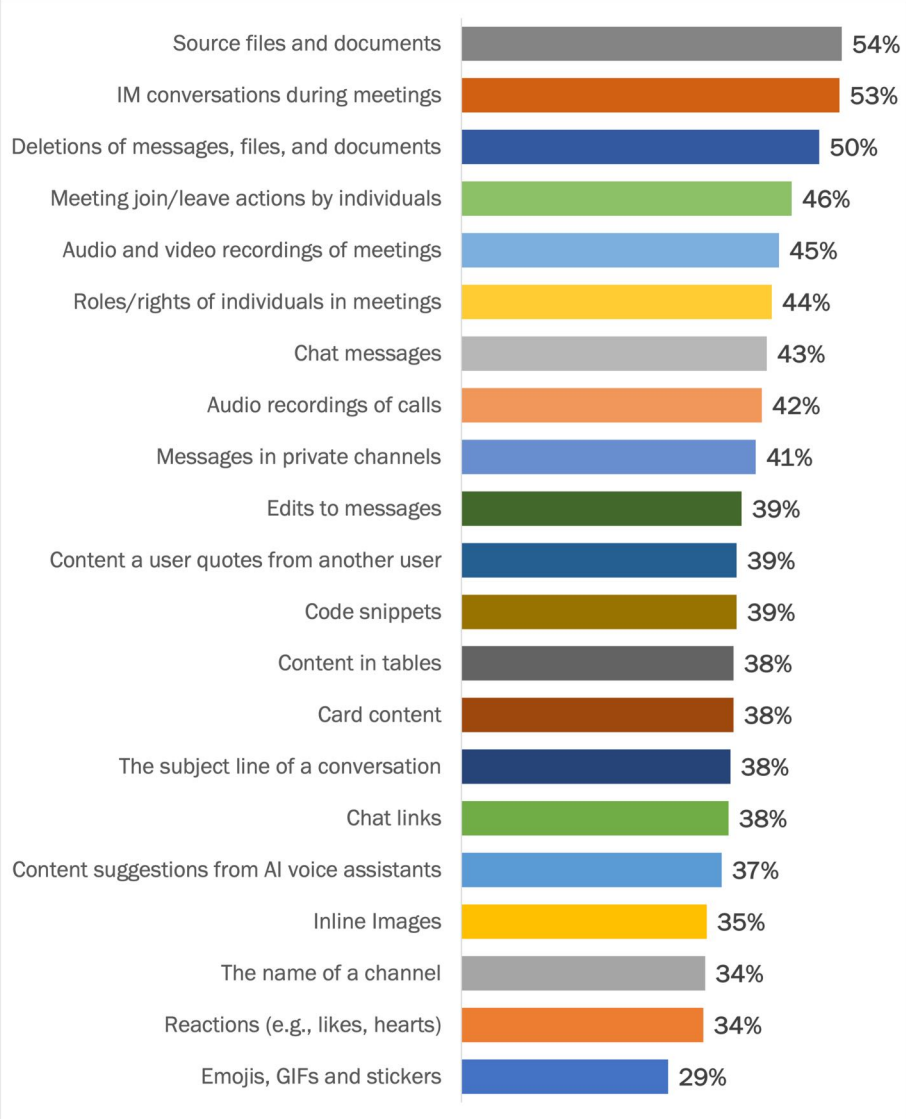
Teams Content to Capture

Microsoft Teams brings together many content types from Microsoft 365 and third-party apps. From an archiving perspective, there is much that could be captured.

MANY RESPONDENTS UNDERPLAY THE IMPORTANCE OF CONTENT TO CAPTURE IN TEAMS

Only one third to one half of respondents say it is highly important to be able to search and produce various content types in Microsoft Teams, with source files and documents (54%), instant messaging conversations during meetings (53%), and deletions of messages, files, and documents (50%) the three highest ranked content or action types. See Figure 12.

Figure 12
Importance of Being Able to Search and Produce Various Content Types in Teams
Percentage of respondents indicating "Very important" or "Extremely important"



Source: Osterman Research (2021)

Only one third to one half of respondents say it is highly important to be able to search and produce various content types in Microsoft Teams.

Teams generates a wide variety of content types, and the native archiving capabilities for Microsoft Teams preserves much of it for eDiscovery and content search. Not everything is captured, however, and the ignored content types provide space for employees to communicate with malicious intent or in inappropriate ways. Figure 13 lists some of the content types ignored by Microsoft's native archiving and eDiscovery capabilities for Microsoft Teams.

Figure 13
Examples of Content Types Ignored by Microsoft's Native Archiving and eDiscovery Capabilities for Microsoft Teams

Content Type	Microsoft's Approach	Compliance Challenge
Recordings of meetings and calls	Audio recordings were initially stored in Stream. From November 2020, recordings can be stored in OneDrive and SharePoint, and retention labels can be automatically applied to recordings.	Recordings stored in Stream were not searchable for eDiscovery. Historical content remaining in Stream is still not searchable. With the transition to OneDrive and SharePoint, retention is based on the type of content ("meeting"), not on the content in the meeting.
Edits to messages in Teams chat and channels	A user can edit their messages in Teams chat and channels. Earlier versions of the message are kept only if the user was on legal hold when edits were made.	Users can state unauthorized information in the first version of a message and then edit it to say something else after the recipient has read and acted on the initial version. Unless all users are perpetually on legal hold, such edits are invisible.
Chat reactions	Likes, hearts, and other reactions can be freely used in chat and channel conversations but are not captured for eDiscovery.	Newer non-textual methods of signaling agreement (and hence proving complicity) are excluded from re-created chat and channel conversations, therefore enabling only partial reconstruction of the thread and context of a conversation.
Code snippets	Code snippets using various languages can be sent in chat and channel messages. Code snippets are a specially formatted message type. Code snippets are not captured for eDiscovery.	The code snippet message type can be used to hide malicious, unauthorized, or unacceptable forms of communication. These are invisible when a conversation thread is subsequently reconstructed.
Content in Microsoft Planner	Microsoft Planner can be added to a Teams workspace for visual planning and coordinating task assignments. Planner content is not captured for eDiscovery.	Planner is a Microsoft-native app in Microsoft 365, but its content is invisible for compliance and internal monitoring purposes.

Source: Osterman Research (2021)

Unless all users are perpetually on legal hold, edits to messages in Teams chat and channels are invisible in compliance searches.

Figure 13 (continued)
Examples of Content Types Ignored by Microsoft's Native Archiving and eDiscovery Capabilities for Microsoft Teams

Content Type	Microsoft's Approach	Compliance Challenge
Drawing, annotations, and text shared using Microsoft Whiteboard	Microsoft Whiteboard can be used to share drawings, annotations, and text during meetings. None of this content is included in the video recording for the meeting, nor is it available for eDiscovery.	Malicious, suspicious, unauthorized, and unacceptable content can be shared using Microsoft Whiteboard. It is invisible for compliance and internal monitoring purposes.
Quoted content	Content that someone quotes in a chat or channel message is captured for eDiscovery, but not the fact that it was quoted rather than being an original contribution.	Misattribution of quoted content.
Content surfaced through tabs in Teams	Third-party apps can be surfaced in tabs in Microsoft Teams. Such content is generally ignored by the compliance capabilities in Microsoft Teams, and relies instead on the compliance capabilities offered by the third-party vendor.	Without strong archiving and compliance controls for third-party apps, employees could merely switch interaction to accessible apps that do not create compliance records.
Content shared via screen sharing or webcam interactions	Employees can use screen sharing to display desktops, applications, and cloud services, along with highly sensitive or privileged documents. Webcams can be used to show documents, physical whiteboards, etc.	Searches of visual content cannot detect sensitive information that is shared through screen sharing or a webcam. eDiscovery searches looking for such data would be incomplete.

Source: Osterman Research (2021)

Any enterprise-sanctioned tool that includes easy methods of avoiding supervision, policy adherence, and compliance requirements is only asking for trouble.

Releasing an enterprise-sanctioned tool that includes easy methods of avoiding supervision, policy adherence, and compliance requirements provides the opportunity for employees to do the wrong thing and cover their tracks. As examples of people using these ignored content types in Teams in non-compliant ways become more commonplace, we expect that more organizations will seek stronger archiving, data protection, and eDiscovery capabilities.

ROADMAP BY MICROSOFT

Microsoft's public roadmap for Microsoft Teams includes few upcoming changes that address the weaknesses in native Teams archiving for organizations subject to strict compliance requirements or internal monitoring policies. Item 68731 on the roadmap adds new capabilities for using Microsoft's Graph API for exporting messages, attachments, emojis, GIFs, and user @mentions from Teams, but does not offer these capabilities to the native archiving approach as such.[14]

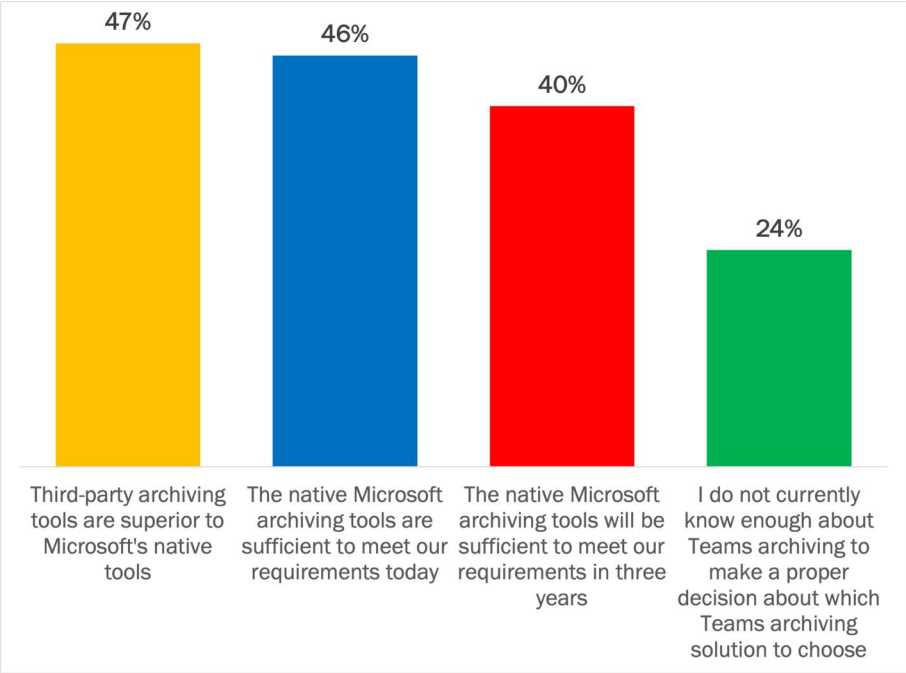
When to Consider Third-Party Solutions

Using the native archiving capabilities in Microsoft 365 for Microsoft Teams content is one option for organizations, but third-party archiving vendors offer an alternative pathway that better addresses the requirements for compliance and internal investigations. In this section, we consider the situations where using third-party solutions makes greater sense than relying on the native option.

EFFICACY OF NATIVE ARCHIVING FOR TEAMS EXPECTED TO DECLINE

Slightly more respondents believe third-party archiving tools are superior to Microsoft's native archiving tools for Teams (47%) than believe Microsoft's native tools are sufficient to meet today's archiving requirements (46%). See Figure 14.

Figure 14
Greenfields View of Approaches to Archiving Teams Content
Percentage of respondents indicating "Agree" or "Strongly agree"



Source: Osterman Research (2021)

Respondents expect the ability of native Microsoft archiving tools in Teams to be less effective in three years than today.

There are two additional interesting data points from Figure 14:

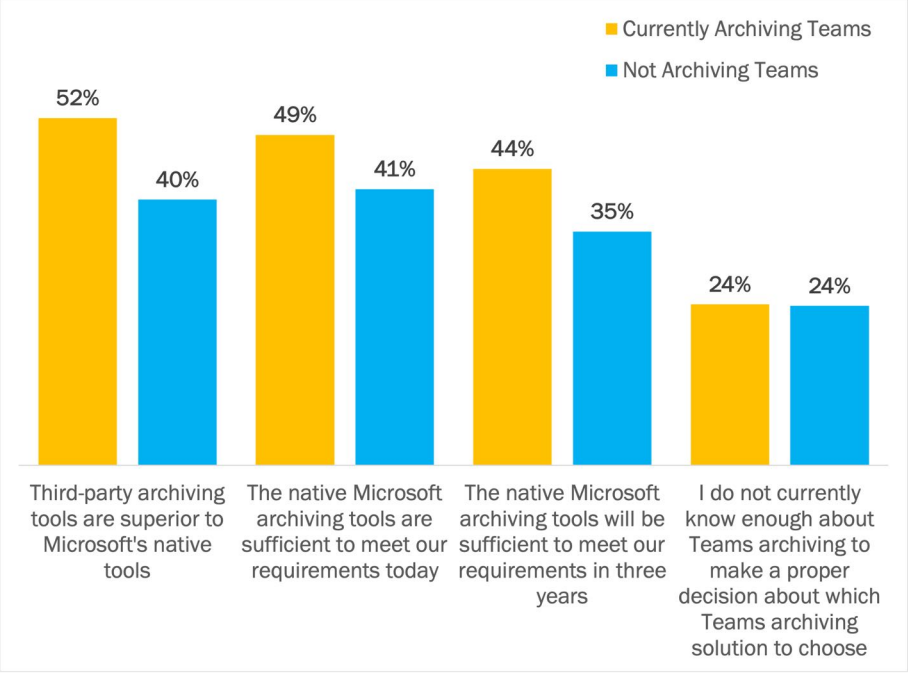
- **Degrading Sufficiency of Native Teams Archiving Over Next Three Years**
  Fewer respondents expect the native archiving tools in Microsoft 365 for Teams to be effective in three years than today—most likely due to increasing regulatory demands. Today's native tools already do not cover all data types, but many respondents believe Microsoft's actions with Teams archiving over the next three years will not improve the situation.
- **One Quarter Need More Education**
  24% of respondents indicate they lack sufficient knowledge about the native capabilities for archiving Teams content to decide whether native or third-party archiving is better suited to their organization.

Splitting the responses by whether respondents are currently archiving Microsoft Teams data or not provides another view of the data (see Figure 15).

- **Currently Archiving Teams**
  For respondents who are currently archiving Teams data, slightly more agree or strongly agree that third-party archiving tools are superior to Microsoft's native tools (52%) than agree or strongly agree that Microsoft's native tools are sufficient to meet their requirements today (49%). The expected three-year drop in the rating strength of native Microsoft archiving tools among this cohort is 10%.
- **Not Currently Archiving Teams**
  For the respondents who are not currently archiving Teams data, slightly more agree or strongly agree that native Microsoft archiving tools will be sufficient to meet their requirements today (41%) compared to third-party tools being superior (40%). However, for this cohort, the expected three-year drop in the rating strength of native Microsoft archiving tools is 15%.
- **A Quarter of Both Cohorts Don't Know Enough Yet**
  Regardless of cohort, just under one quarter of respondents indicate they do not currently know enough about archiving Teams data to make a proper decision on third-party versus native archiving.

Respondents who are currently archiving Teams data rate third-party archiving tools more highly than those who are only thinking about it.

Figure 15
Greenfields View of Approaches to Archiving Teams Content—Currently Archiving Teams vs. Not Currently Archiving Teams
Percentage of respondents indicating "Agree" or "Strongly agree"



Source: Osterman Research (2021)

REASONS FOR SEEKING BETTER ARCHIVING CAPABILITIES IN TEAMS

There are many potential reasons why a firm will seek better archiving capabilities for Microsoft Teams than what is offered natively by Microsoft. We asked respondents to rank the importance of ten possible reasons they would consider third-party offerings. See Figure 16.

Figure 16
Reasons for Using Third-Party Archiving Solutions for Microsoft Teams
Percentage of respondents indicating "Very important" or "Extremely important"

Source: Osterman Research (2021)

Multi-repository search with in-place data was the highest ranked reason for seeking a third-party archiving solution for Microsoft Teams.

IN-PLACE SEARCH ACROSS MULTIPLE PLATFORMS AND REPOSITORIES

Respondents ranked the ability to perform searches for eDiscovery and other investigations with in-place data across multiple platforms and repositories—without first having to migrate data to a central repository—as the most important reason for using third-party archiving and data protection solutions for Microsoft Teams. With all the survey respondents currently using multiple systems and associated data repositories, gaining unified and integrated search for internal investigations, ongoing regulatory supervision, regulatory audits, early case assessment, and eDiscovery is critical.

CAPTURING THE FULL RANGE OF DATA TYPES IN TEAMS

Microsoft's native retention capabilities for Teams capture many but not all of the data types in Microsoft Teams. Third-party archiving solutions provide fuller capture of the multiple data types in Teams, along with advanced customizable workflows and legal hold and eDiscovery capabilities. For example:

- The standard data types that Microsoft already captures in its native retention approach for Teams, such as chat and channel conversations, instant messaging conversations in meetings, and messages in private channels.
- Reactions to messages (e.g., emojis, which can signal agreement or collusion without using an associated text fragment), versions of edited messages irrespective of whether a user is on hold, audio recordings, formatting options in conversations, and code snippets (which could be used to hide conversational data), among others.
- Capture and analysis for animations, images, files, audio, video, notes, and capture with analysis of files from SharePoint links at the point in time they were shared.

Respondents ranked the ability to capture the full range of data types in Teams as the second most important reason for considering third-party archiving solutions.

Third-party archiving tools either need to provide in-place search plus complete data type capture for Teams, or complete data type capture in a fit-for-purpose multi–data type enterprise archiving platform.

SINGLE PLATFORM FOR MICROSOFT AND NON-MICROSOFT DATA SOURCES

A single platform for archival, eDiscovery, and compliance across both Microsoft and non-Microsoft data sources was the third highest-ranked reason for using third-party archiving solutions for Teams. In comparison to the top-ranked reason of in-place search across multiple platforms and repositories (i.e., leave all data where it is but cohesively search and produce it), the single-platform reason takes the architectural approach of a single and separate platform for archival and compliance purposes.

Characteristics of this approach generally include:

- A separate copy of all covered data elements in a centralized platform that is different from any systems which created the data elements originally. This creates a secure digital memory with tight restrictions on access for the purposes of compliance, eDiscovery, and internal investigations.
- The ability to search across all data elements to respond to data subject access requests, data portability exports, and right-to-be-forgotten purposes under GDPR, CCPA, and other applicable privacy regimes.

- A unified policy engine for classifying, protecting, and setting retention timeframes on all covered data elements. Under this approach, the originating system becomes an additional element of metadata for determining classification and retention timeframes, not a limiting factor of capability.
- A comprehensive approach to preventing edits, unauthorized deletions, and other interference in the authenticity of captured data, using immutable storage technologies and techniques.

Some third-party vendors can additionally provide redacted views to protect personally identifiable information and sensitive data across chat, video, and voice from employees without the appropriate access rights.

REDUCING RISK OF USER CHANGES UNDERMINING COMPLIANCE CAPABILITIES

Microsoft Teams remains a dynamic and ever-changing offering. Microsoft's official roadmap for Teams currently lists 212 features in development, 29 rolling out, and 143 launched in recent months.[15] As stated earlier, more than 67,000 feature requests have been lodged in UserVoice for Microsoft Teams. Teams has only been in market for just over three years. It is still a relatively new and highly promising offering for Microsoft, and the cadence for both previous and upcoming change is significant.

However, it is highly likely that many valid use cases for Teams will conflict with compliance requirements for authenticity, accuracy, and completeness. Using a third-party archiving and data protection solution to capture point-in-time and point-in-context actions and signals enables organizations to embrace the newer features from Microsoft that address valid use cases without undermining the compliance requirements they are also subject to. Such an approach enables compliance officers to champion the use of new collaboration and productivity platforms while also knowing they have advanced third-party tools to manage all of these new ways of communicating.

The ability to have the best of both worlds in this regard was the fourth highest-ranked reason for considering third-party archiving solutions.

Respondents see third-party archiving solutions as offering the best of both worlds: access to new leading-edge user capabilities without compromising compliance mandates.

FEWER, CONSISTENT RETENTION POLICIES

Third-party archiving solutions are more likely to offer a unified approach to policy definition and enforcement that works across multiple data types from various products, services, and solutions. Fewer policies that cover a broader remit of data types can be created and managed under such an approach, decreasing the likelihood that important data types are inadvertently missed by falling between an unintended space in multiple different policies.

The ability to set fewer, consistent retention policies that cover more data types—irrespective of the source system—was the fifth highest-ranked reason for considering third-party archiving solutions.

FIVE OTHER REASONS FOR BETTER ARCHIVING CAPABILITIES IN TEAMS

Respondents ranked a constellation of five additional reasons for better archiving for Microsoft Teams. In ranked order, the additional reasons were:

- **Targeted Legal Hold Across Multiple Platforms and Repositories (6th)**
  The ability to set legal holds across multiple platforms and data repositories without having to migrate data to a central repository first was highly important to 49% of respondents, placing this reason in sixth place. This reason complements the top-ranked reason of being able to search in-place across multiple platforms with multi-platform legal hold capabilities. The ability to use a single legal hold across multiple platforms and repositories means that a collection of different legal holds per platform or repository can be avoided.
- **Faster Removal of Messages (7th)**
  The prompt removal of messages subject to a deletion retention policy is important to just under half of respondents. Data that can be deleted based on the correct retention timeframe should be deleted as soon as possible. Microsoft Teams can take up to seven days after the deletion timeframe has passed before a message is actually deleted.
- **Better Tools for Supervision (8th)**
  Supervision of communications enables proactive and automated flagging of messages that may violate external regulations or internal policies. For 43% of respondents, gaining access to better capabilities for supervision was highly important as a reason to use third-party solutions. While the supervision capabilities in Microsoft 365 have come a long way since Microsoft's initial attempts and its new Communication Compliance solution is able to address a wider range of risk scenarios, third-party offerings still offer better capabilities in multiple areas. These include lexical analysis, options for pre-delivery approval of messages that have been automatically identified as containing serious violations of policy, multi–data type support beyond just Teams and Microsoft 365, automatic echo cancellation, and the automatic inclusion of new data sources without having to manually update policies. Some third-party offerings offer remediation and removal of problematic content in Teams, along with real-time supervisory actions in meetings. Teams chat communications are persistent which means that violations and sensitive data stay live and exposed in Teams. When compliance teams discover such risks, modern supervision tools can remediate and delete offending data in Teams, while retaining a full audit log of that action as part of the review record. For meetings, modern supervision products can alert users in real-time of behavior that is potentially in violation of compliance requirements and capture all such activity in the archive as a searchable set of actions.
- **Separate Compliance Platform and Data Set (9th)**
  Separating the compliance platform and data set from the day-to-day system used by employees for communication and interaction was highly important to 43% of respondents. Using a third-party archiving solution in this way means that information governance and compliance professionals gain a specific fit-for-purpose platform for all information governance and compliance processes. Users, on the other hand, can use whatever connected platforms and systems they need for their day-to-day tasks. Data types from user platforms are captured by the compliance platform, thereby serving the needs of both constituencies.

Some third-party offerings offer better tools for supervision, such as remediation and removal of problematic content in Teams, along with real-time supervisory actions in meetings.

- **Reduce Point Solutions (10th)**
  Out of the ten potential reasons for considering third-party archiving solutions, the 10th most important reason was to reduce reliance on point solutions (by 42% of respondents). In other words, respondents would prefer not to use multiple platform-specific archiving and compliance solutions across a distributed and heterogeneous data landscape. Having to use multiple individual systems for archiving and compliance adds complexity and cost to regulatory, legal, and other internal processes that are already complex and costly enough.

Summary and Next Actions

Ensuring the right archiving and data protection capabilities are available to secure and protect content in Microsoft Teams—and other enterprise data sources too—is critical for every organization for compliance, legal processes, and internal investigations. We encourage readers to leverage this research and evaluate their own requirements:

- **What Drivers Are at Play?**
  Develop an understanding of the external compliance regulations your organization is subject to which impose strict archiving requirements on your use of Microsoft Teams. Additionally, examine the internal legal and governance drivers that are best served with tighter controls over the capture, security, privacy, and protection of archival data.
- **What Data Systems and Repositories Are Currently in Use, or Forthcoming?**
  Analyze your current data landscape to understand the systems, repositories, and platforms currently being used by employees. In addition, what new systems, repositories, and platforms are likely to be added over the next few years? There should be IT strategy documents available to review for such guidance.
- **Native Archiving Versus Third-Party Archiving**
  Match the archiving and data protection drivers with your picture of current data systems and repositories to gauge whether reliance on native archiving capabilities in Teams and other platforms will be sufficient, or if third-party archiving solutions are likely to offer better alignment with your requirements.
- **Third-Party Vendor Evaluation**
  If a third-party approach better fits your requirements, evaluate third-party vendors on their level of integration, partnership, and certification with Microsoft across all aspects of Teams directly and Microsoft 365 more broadly.

Ensuring the right archiving and data protection capabilities are available to secure and protect content in Microsoft Teams is critical for every organization.

Sponsored by Theta Lake

Theta Lake provides security and compliance for modern collaboration platforms using frictionless partner integrations with Cisco Webex, Microsoft Teams, RingCentral, Slack, Zoom, and more. Using patented machine learning and NLP, Theta Lake detects risks in video, voice, chat, and document content across what is shared, shown, spoken, and typed. Those risks are surfaced in an AI-assisted, patent-pending review workspace that adds consistency, efficiency, and scale for security and compliance teams. All of this enables organizations to safely realize the full ROI of a collaboration-first workplace while reducing the cost of security and compliance. Visit us at thetalake.com, LinkedIn, or Twitter at @thetalake.

With customer-driven data center and data residency coverage in the US, UK, EU, Canada, and Australia, Theta Lake's existing Microsoft Teams compliance integrations and capabilities include:

- **Microsoft Certified Teams Meetings Recording, Archiving, and Supervision –** as of May 2021, the only archive, supervision, and eDiscovery vendor to achieve Microsoft Certification for compliance recording and archiving with the only full analysis and supervision for video, voice, and chat meeting content. This includes follow-the-user recording enforcement where all chats and meetings can be captured for an organization's employee—even if the meeting host and meeting are initiated by an external party who is not an employee of the organization.
- **Microsoft Teams Chat Capture, Archiving, DLP, Supervision, and Remediation –** covering Teams Team Chat, Team Group Chat, and Teams Private, 1:1 chat—providing fully native capture (messages, images/GIFs, reactions, edited/delete messages, files, documents), SEC 17a-4 archiving (including third-party email archive integrations), supervision of compliance, acceptable use, data privacy risks, malicious URLs along with actual remediation capabilities in Teams. Theta Lake provides a native chat viewer of Microsoft Teams Chat, presenting messages, shared content, images, reactions to understand full context and history.
- **Security and Compliance Center Integration –** delivering advanced security configuration validation and enforcement reporting to ensure the key settings for Teams, like not being able to delete a Teams channel or message, can be set, enforced, and reported on globally for internal and external audit requirements.
- **Realtime Compliance Advisor for Microsoft Teams Meetings –** providing real-time and in-meeting compliance alerting and coaching with personalized resources for employees in live meetings as well as enterprise reporting on Teams meeting behaviors.
- **OneDrive Integration –** allowing compliance teams to capture, compliantly archive, and detect risks in content stored in OneDrive, including audio recordings, video recordings, documents, and other content.

www.thetalake.com

Twitter: @ThetaLake

LinkedIn: @ThetaLake

info@thetalake.com

+1 650 242 3900

- **O365 Archive and Third-Party Archive Integration** – extending beyond simply archiving Teams and other UC platform content from Zoom, Webex, Slack, RingCentral, and more, the integration adds Theta Lake risk and detection insights with reviewer and workflow audit history into the O365 archive with the ability to add views into Theta Lake's patented review workspace. This deployment mode can be extended to multiple other third-party archive and eDiscovery systems simultaneously.
- **Azure Integration** – providing the ability to move or archive content and analysis insights for content captured to Azure storage; underlying ability to use Theta Lake is deployed completely via Azure with robust security and compliance controls including 'bring-your-own-encryption-key' for customers.
- **Co-Sell Incentivized** – through the Microsoft One Commercial Partner program, Theta Lake joins a select group of ISVs to collaborate and closely align with Microsoft's sales organization and partners to further expand go-to-market initiatives and the global adoption of Theta Lake's Compliance and Security Suite running on Azure.

Theta Lake provides tight integration and value-add for Microsoft-centric customers of all sizes, while providing the extensibility to cover multiple other collaboration tools like Zoom and Cisco Webex while supporting flexible deployment modes to maximize investments in pre-existing archive and eDiscovery systems.

---

[1] Lori Wright, Microsoft Teams turns 1, advances vision for Intelligent Communications, March 2018, at https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/12/microsoft-teams-turns-1-advances-vision-for-intelligent-communications/

[2] Ron Markezich, 10 new ways for everyone to achieve more in the modern workplace, September 2018, at https://www.microsoft.com/en-us/microsoft-365/blog/2018/09/24/10-new-ways-for-everyone-to-achieve-more-in-the-modern-workplace/

[3] Jared Spataro, Microsoft Teams Reaches 13 Million Daily Active Users, Introduces 4 New Ways for Teams to Work Better Together, July 2019, at https://www.microsoft.com/en-us/microsoft-365/blog/2019/07/11/microsoft-teams-reaches-13-million-daily-active-users-introduces-4-new-ways-for-teams-to-work-better-together/

[4] Jordan Novet, Microsoft Claims 20 Million Daily Users for Teams, Extending Its Lead Over Slack, November 2019, at https://www.cnbc.com/2019/11/19/microsoft-teams-reaches-20-million-daily-active-users.html

[5] Tom Warren, Microsoft Thinks Coronavirus Will Forever Change the Way We Work and Learn, April 2020, at https://www.theverge.com/2020/4/9/21214314/microsoft-teams-usage-coronavirus-pandemic-work-habit-change

[6] Jared Spataro, Microsoft Teams Reaches 115 Million DAU - plus, a New Daily Collaboration Minutes Metric for Microsoft 365, October 2020, at https://www.microsoft.com/en-us/microsoft-365/blog/2020/10/28/microsoft-teams-reaches-115-million-dau-plus-a-new-daily-collaboration-minutes-metric-for-microsoft-365/

[7] Microsoft Investor Relations, Microsoft FY21 Third Quarter Earnings Conference Call, April 2021, at https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/TranscriptFY21Q3.docx?version=5000c435-108f-a064-0035-be555b8a57ff

[8] Slack, Slack CEO Stewart Butterfield Shares Updated Business Metrics During Tweetstorm on Impact of COVID-19, March 2020, at https://investor.slackhq.com/news/news-details/2020/Slack-CEO-Stewart-Butterfield-Shares-Updated-Business-Metrics-During-Tweetstorm-on-Impact-of-COVID-19/default.aspx

[9] Zoom, 90-Day Security Plan Progress Report: April 22, April 2020, at https://blog.zoom.us/90-day-security-plan-progress-report-april-22/

[10] Eric S. Yuan, A Message to Our Users, April 2020, at https://blog.zoom.us/a-message-to-our-users/

[11] Kimber Streams, Petraeus and Broadwell Attempted to Conceal Affair Using Gmail Drafts, November 2012, at https://www.theverge.com/2012/11/13/3642256/petraeus-broadwell-scandal-gmail-drafts

[12] FINRA, FINRA 3110. Supervision, November 2020, at https://www.finra.org/rules-guidance/rulebooks/finra-rules/3110

[13] Top requested items were extracted from the Microsoft Teams UserVoice page on April 26, 2021. The number of current votes and ranking of each request item will change over time. See https://microsoftteams.uservoice.com/forums/555103-public/filters/top?page=1

[14] Microsoft 365 Roadmap, Microsoft Teams: Microsoft Graph API for Teams Export (Preview), April 2021, at https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=&searchterms=68731

[15] The status of the Microsoft 365 Roadmap for Microsoft Teams was extracted on April 26, 2021. These numbers will change over time. See https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=Microsoft%20Teams