idm.
information & data manager

Home | Magazine | Enterprise Guides | Imaging Service Bureau | About Us | Events

Study identifies Teams Data as Compliance Concern

Friday, May 21, 2021 - 11:48

Microsoft Teams adaption skyrocketed in 2020; however, IT decision-makers remain split as to whether they are managing this data compliantly

ZL Tech, a developer of information governance and compliance solutions, has announced the results of a study investigating Microsoft Team's native arching and third-party compliance systems capabilities. Conducted by Osterman Research, the study surveyed 143 IT leaders at mid- and large-scale enterprises, all of whom are currently using Microsoft Teams.

Due in large part to the global pandemic that mandated virtual collaboration, Microsoft Teams adoption has skyrocketed in recent years, with over 145 million daily users in April 2021. However, this decision was often made without fully considering how usage would affect legal and regulatory compliance.

The survey found that when considering whether to incorporate Microsoft Teams, compliance and legal professionals were two of the three least influential decision-makers.

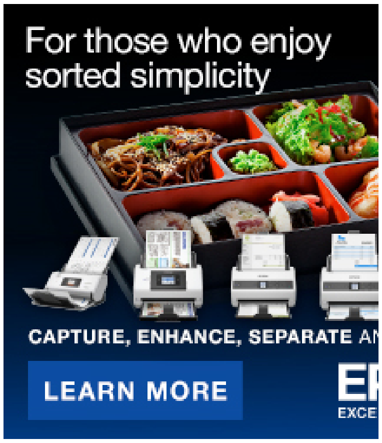
When asked whether Microsoft Team's native archiving capabilities were sufficient to meet their compliance requirements, only 54% of respondents fully agreed.

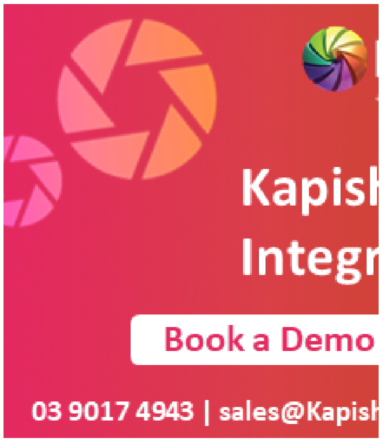
Some leading concerns are Microsoft Teams' inability to capture source files and documents (48%), quotes (36%), and audio in meetings (35%) and calls (35%). Looking to the future, only 40% of respondents think Microsoft Teams' native archiving tools will meet their various requirements in the next three years.

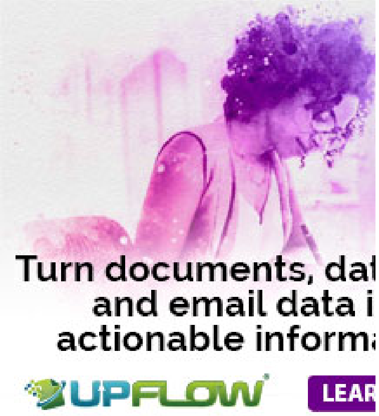
Regardless of whether the respondents' Microsoft Teams archiving capabilities were sufficient for their needs, Microsoft Teams data has already been required in the last year for eDiscovery (49%), internal investigations (49%), and regulatory audits (30%).

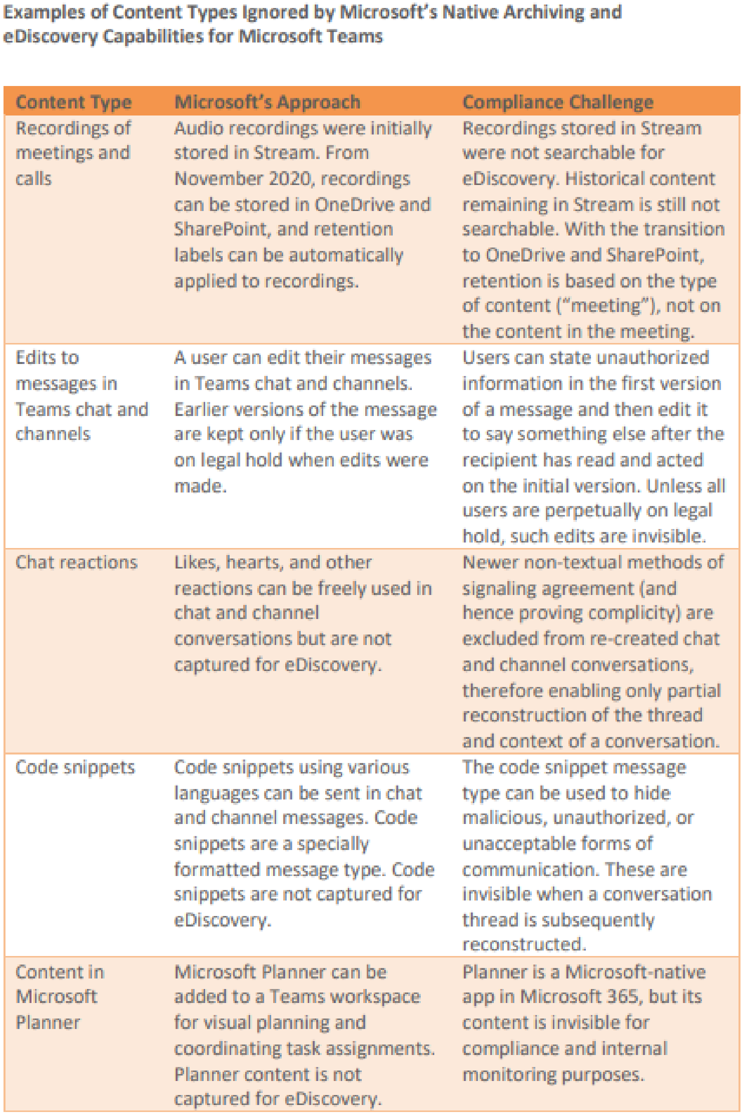
Of respondents currently archiving Microsoft Teams, over half (52%) believe that third-party archiving tools are superior to native capabilities. The leading reasons IT leaders considered a third-party solution were to search across multiple platforms in-place (54%), to capture all Microsoft Teams data (53%), and to have a single platform for archiving, eDiscovery, and compliance for multiple data sources (53%)

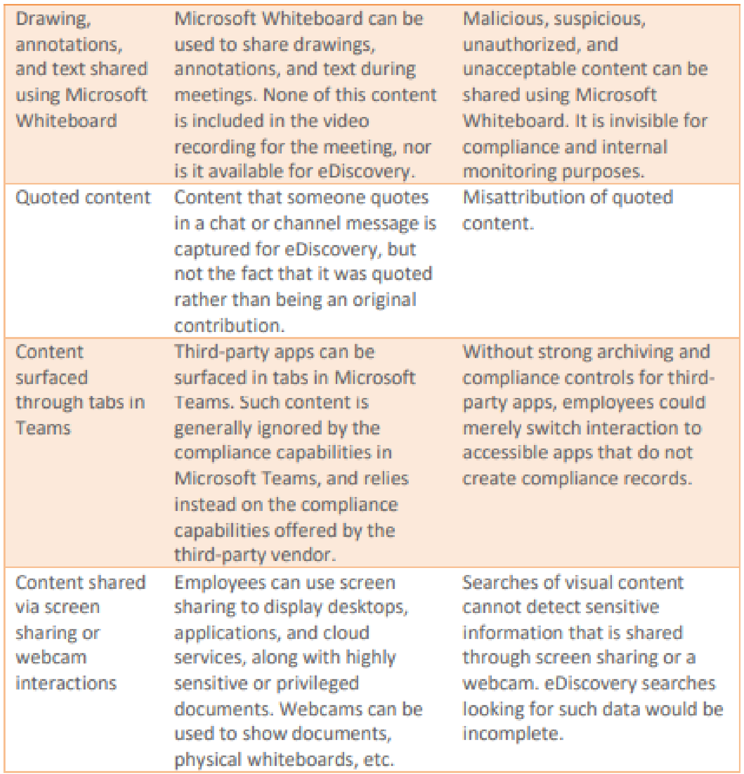
To read the entire report, click here.


For those who enjoy sorted simplicity
CAPTURE, ENHANCE, SEPARATE AN
LEARN MORE
E
EXCE









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.
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.

?? ?? 0

Email idm@idm.net.au Tel
+61 2 9043 2943

↑