smarsh®

THE DEFINITIVE GUIDE TO ELECTRONIC COMMUNICATIONS CAPTURE

IM & Collaboration

THE DEFINITIVE GUIDE TO ELECTRONIC COMMUNICATIONS CAPTURE

IM & Collaboration

Like email, instant message and collaboration technologies are well-suited for organizations of any size and across industries. Unique from email, however, are the multiple combinations of communication modalities offered by each platform. These include persistent chats, document sharing and co-authoring features, custom emojis, video and screen sharing and AI-enabled bots and services. These can each create distinct challenges for compliance teams.

Today's most popular platforms are Microsoft Teams and Slack, complemented by a dizzying array of functional favorites including Jira, Atlassian, Wrike and many others. These tool preferences differ across departments and functions. Add in common organizational changes and corporate acquisitions, and most enterprises are using an average of 3.8 collaborative platforms at a time.[1]

The 12 to 18 months leading up to 2020 witnessed a dramatic growth in the IM and collaboration technology space. This growth was led by Slack and Microsoft Teams, joined also by Cisco WebEx Teams, Workplace by Facebook and Symphony. Microsoft reported during this time period that more than 500,000 organizations were using Teams compared with 200,000 organizations a year ago, with 13 million daily active users (DAUs)[2], surpassing Slack's 10 million.[3]

The benefits of enabling collaborative technologies

The reasons behind this explosive adoption are clear: real, tangible ROI. Brian Hill, Principal at Wellington Consulting and long-time expert on the collaboration technology market, notes that users of these tools have realized many benefits that have fueled the category's growth.[4]

Benefits include increased productivity, improved business cycle times and improved service delivery. These all contribute to a reduction in cost and the ability to positively impact revenue based on increased business agility and responsiveness.

These points are supported by an April 2019 study led by Forrester Research.[5] In this study, users of Microsoft Teams reported a 17% reduction in daily email volume and a 19% reduction in weekly meetings. A similar study conducted by IDC[6] in 2017 noted that users of Slack saw a 32% reduction in emails and 23% fewer meetings.

SLACK

32% less email

21% faster response time to sales lead

23% fewer meetings

86% say it's easier to share key learnings

(Source: The Business Value of Slack, IDC Research, 2017)
Slack: 12 million daily active users

MS TEAMS

17% reduction in emails received per day

18% improvement in time-to-decision

19% reduction in meetings per week

832% ROI over 3 years

(Source: The Total Economic Impact of Teams, Forrester, 2019
Teams: 13 million daily active users

Then the world changed...

A newly remote workforce

COVID-19 abruptly and urgently drove virtually every organization into the market for collaborative and conferencing technologies, many for the first time. Firms that had previously operated with mostly in-office staff were suddenly thrust into a new paradigm. They had to consider how to supply remote workers with equipment and secure means of connectivity to corporate IT resources. Organizations have had to provide tools that allow remote workgroups to continue to stay on track with key deliverables and customer commitments.

The expansion in use of these tools has been nothing short of remarkable. Slack reported a 25% increase in users in a one-month period (March 2020).[7] Microsoft noted that the use of video within Microsoft Teams increased by 1,000% in that same time period.[8]

This tremendous spike in usage has been experienced not only by established market leaders, but also by new and more niche applications. Google Meet, Houseparty, Discord, Marco Polo and other downloadable apps have gained significant traction.

But the fast adoption of collaboration tools hasn't been without challenges. Many collaborative applications offer free versions. These are typically lacking either in key features or in the controls required to capture the communications activity occurring on those platforms. Absent explicit guidance, employees are using collaborative tools with which they are already familiar or those that were easy to obtain. These are not necessarily the tools that have been approved by management.

Unfortunately, some collaborative tools and versions are not suited to meet the demands of regulated businesses. The same goes for organizations that are subject to frequent litigation and investigative demands.

The unique challenges of capturing IM & collaborative content

As noted previously, collaboration platforms consist of multiple communication modalities, and each platform offers its own unique combination:

Conversational

Discussions typically occur over a series of asynchronous messages or posts. Understanding the context of a conversation is difficult when capturing individual messages unless message ordering is preserved. This includes noting items that may have been modified or deleted since they were originally posted.

Multiple participants

Conversations on collaboration platforms often consist of multiple participants. Any one of those participants may have policy restrictions for accessing specific subjects. For example, many firms have barriers or "ethical walls" that must be enforced between broker and advisory groups. Determining which participants should be on record — as well as capturing what can be hundreds of participants in a meeting — can be challenging on some platforms.

Interactive

Conversations can persist over configurable time periods. This requires firms to monitor changes to conversations that could be relevant to compliance tasks, including noting multiple versions of a document created by co-authoring features.

Activity oriented

Unlike email, collaborative content typically behaves more comparably to a virtual meeting room. Email is the transcription of notes from a meeting versus a collaborative event, which is the actual in-person meeting experience itself. The difference can be very significant from a content capture perspective. It may be relevant to understand who has joined or left a meeting, as well as noting the identity of a meeting participant known only as "call-in user 2."

Mobile friendly

Most modern collaboration tools have been designed with a "mobile first" philosophy. Today's remote workforce may need to connect to colleagues from anywhere — including from their mobile devices while in transit. Capturing collaborative content should function independently of devices used, to ensure the complete record of a conversation has been preserved

The risks associated with IM & collaborative technologies

Clearly, collaboration tools are highly popular and are now critical to doing business. Whether measured explicitly or more broadly, organizations are seeing their value. Compliance executives seek to enable their business to use the tools with which their employees and clients are familiar and comfortable. If your firm does not allow these channels to be used, it's likely that your competitors do.

However, collaboration tools present potential risks that can impact nearly every function of the business. They require the participation of stakeholders from all functions to ensure that a complete view of possible vulnerabilities is examined before making an investment. Those risk areas include the following:

Regulatory compliance risk

Every firm regulated by FINRA, SEC, FCA, IIROC, MiFID II or other regulatory bodies has an obligation to meet books-and-records requirements by capturing all business-related communications. Those requirements do not distinguish one communications or collaborative source from another.

In fact, FINRA Rule 4511 and SEA 17a-4 both note the requirement that those records be "true, accurate, and complete," highlighting the importance that capture methods account for the multi-modal, interactive and conversational nature of collaborative technologies. As compliance executives have frequently stated, if a communications channel can't be captured, employees can't use it to conduct business.

Data privacy risk

One challenge unique to collaboration tools like Slack and Microsoft Teams is that they can look like places to socialize. Privacy complications can arise if collaboration tools are not used exclusively for business purposes. Content collected from those tools must be used by the firm for the stated business or regulatory purposes that are outlined in policies.

International and U.S. state privacy mandates such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in California continue to emerge. Firms should be aware of how each collaboration tool will impact their ability to fulfill Right of Access requests under applicable privacy laws.

Information security risk

InfoSec remains the most closely watched risk category, spanning a broad range of topics. These include breach, outages, spam and malware infection, susceptibility to advanced targeted attacks and other potential vulnerabilities. Today's major information security providers remain heavily invested in and focused on email and web-based threats.

The result has been an increase in the incidents of malware and ransomware targeting collaborative platforms such as Microsoft Teams[9] and Slack.[10] Inevitably, those with intent on doing harm are going to follow users to popular platforms. Firms are best served to monitor the InfoSec credentials, third-party attestations and accreditations and investments made by collaborative tool providers before investing.

Discovery review risk

Multiple communication modalities — along with the fact that conversations can be changed, modified or deleted — create new complexities for discovery programs that are designed for email. Familiar parent-child relationships of email are not as easy to decipher when there may be hundreds of participants in a persistent chat with consistently evolving content.

For firms facing frequent litigation, the risk of missing a critical conversational component is exceptionally high. Using capture tools unsuited for collaborative technology is an exposure that is catching the attention of an increasing number of legal teams.

Internal policy risk

A primary challenge in the deployment of collaboration tools is the lack of guardrails. Potential exposures can be introduced if communication policies guiding the appropriate use of intellectual property and other sensitive information are not extended to these platforms. "Zoom Bombing" and "Slack Bullying" are becoming familiar terms. They highlight the need for firms to consider HR and other code-of-conduct violations in their definitions and plans for communication risks.

Mitigating the risks of IM & collaboration technologies

For regulated firms, risk mitigation of collaborative tools has three main factors: 1) policy adjustments, 2) updated user training and 3) selection of the appropriate capture technologies.

1. **Policy adjustments:** These typically take multiple forms for firms seeking to change the way they collaborate and communicate. Here are some of the most common:

Retention policies: Regulated firms have retention policies driven by mandates such as FINRA 3110 and SEA 17a-4. These must apply to all communications tools used for business purposes. Firms do not typically tie policies to specific tools, aside from the use of mobile devices. However, they do need to examine whether the types of activities conducted on collaboration tools would constitute "business records" as defined within their records classifications. Given the recent spike in usage of Microsoft Teams and Slack in particular, it will become increasingly difficult for firms not to retain those communications. At minimum, firms should inspect existing retention policies to ensure there are no implicit biases toward established communication technologies. Policies must apply equally to collaborative tools.

Communications policies: Similarly, employee communications policies should be updated to outline acceptable and prohibited usage of collaborative tools. This should be done in coordination with business stakeholders who are familiar with how those tools are being used by internal groups, as well as how they are shared with customers and partners. It is safe to presume that more explicit guardrails should be established for modalities including voice, video and app sharing than were required for email.

Supervisory policies: FINRA, SEC and other regulatory bodies do not differentiate one communications tool from another. If business is being conducted on behalf of the firm, it must be captured and supervised. Firms should evaluate existing supervisory workflows and policies to make sure they can preserve and review the interactive, multi-modal activities taking place on collaborative tools.

RECOMMENDED READING:

Managing Global Compliance: What to Do About IM and Collaboration Tools in the Enterprise

Content inspection/surveillance practices: Aside from regulated users, other risks introduced on collaborative tools by employees should be subject to periodic inspection. This is to surface code-of-conduct or other policy infractions. Most firms do not currently have an established, regular cadence to do this. However, proactive, periodic ad hoc inspection of content is an emerging best practice for spotting policy issues before they can damage the firm.

2. **User training:** The importance of employee training that is specific to new collaborative tools cannot be understated. As Brian Hill from Wellington Consulting noted, "A lot of organizations miss this point. Many organizations are focused on addressing this challenge clearly from a technology perspective, and that simply doesn't work. There is no silver bullet from a technology perspective. The human capital element is really, really critical. So the training on the use of a collaborative tool needs to be very explicit; the policies need to be set up well in advance, with coordination across the various stakeholder groups. The training around those policies needs to be repeated on a regular basis and should cover other tools that are currently being evaluated. Many may have great training that can be implicitly biased toward email but might not necessarily reflect the way users interact with Slack or Teams. It's important to address different features and functionalities that these tools have and what's allowed and what's not."[11]

3. **Selecting the appropriate capture technologies:** There are different options available for capturing content from collaboration technologies. It is important to consider these alternatives in more detail.

Capturing IM & collaboration content: the alternatives

There are a variety of mechanisms available to capture the activity that occurs on these platforms. Here is a summary of the most commonly used options:

1. **Native features:** One of the most important differences among collaboration tools is the mechanism provided to capture the unique conversational content, context and metadata that each produce. Every tool is different, and some providers are not fully versed in the requirements of regulated firms. If attempting to capture content directly via collaboration tool providers, firms should consider (at minimum):

   - Vendor strategy governing what level of access they give to customers and partners for back-end functionalities via APIs or other methods of access
   - What specific content and events are accessible for capture. Collaboration platforms provide multiple functionalities including chat, video, voice, edit/delete events, app sharing, bots, etc. Knowing what is accessible will inform decisions later about which capabilities are enabled for use and which should be prohibited by either technology or policy
   - How much historical content is accessible to customers and partners, and the mechanisms by which to access that content (i.e., how quickly content can be retrieved)
   - Storage technology used by the provider to ensure that content is not re-purposed or potentially altered
   - Data security and privacy investments, third-party attestations and accreditations (e.g. ISO 27002 and SSAE-16), as well as breach notification procedures
   - Availability of premium service tiers to support API access suitable for regulated firms
   - Notification procedures for API updates and enhancements

2. Build your own: Some firms with large IT development resources have opted to develop their own "connectors" to collaborative content sources in order to reduce cost. While this may be suitable for some, firms should consider (at minimum):

- Whether software development fits within the firm's business strategy and has direct bearing on enhancing revenue and improving client relationships
- How many networks are currently supported, and how many new sources are added per quarter or per year. Many large firms support 80+ communications sources, and compliance teams are under constant pressure from business users to enable new tools. Like compliance teams, most internal IT development groups will be hard-pressed to stay in front of demands of the business
- How frequently collaboration tools are updated, potentially requiring changes to the firm's capture mechanism
- Who in the firm will provide support, bug fix and other fail-safe options in the event of disruption to content capture data flows
- Where the captured content is delivered for archiving and the ease of consuming complex, interactive and meta-data rich collaborative content into that system

3. Construct basic content capture as needed: Another cost-driven approach is to rely upon outside service providers to build "connectors" to content sources as they are demanded. Many archiving providers follow this approach to initially gauge demand before investing in the "productization" of each content source connector. Considerations for those choosing this approach include:

- Skills of the service provider to build content collection assets with a relatively long shelf life, versus T&M development work
- "Ownership" of the connector, once constructed
- Whether only basic messaging content will be collected, or if metadata, event-based information and interactivity and non-text-based data (e.g., custom emojis) content will also be collected
- Responsibility for ongoing support, maintenance and upkeep
- Assurances that the provider will not alter original content properties and will attest to their development processes if the firm is questioned by a regulator or within litigation
- Knowledge transfer and the ability for internal teams to understand the development approach if they later choose to in-source the capture of that content type

4. License third-party providers with productized connectors to capture collaborative content: The final option is to partner with a provider with greater expertise and specific focus on capture technologies. These providers can capture content in a manner that will withstand the rigors of financial services regulatory compliance. Given the fast pace of innovation in the collaboration technology market, the following considerations should be prioritized when selecting a third-party provider:

- Established track record of delivering capture technologies that help firms satisfy SEC, FINRA, FCA or similar regulatory requirements
- Proven ability to deliver at a comparable scope and scale to your firm's compliance volume and workload
- Ability to capture all available content sources made accessible by the collaboration tool provider, including metadata and event information
- Capture features that allow firms to enforce pre-archiving policy controls on collaboration sources where they are available. These include ethical walls, disabling features, content moderation, disclaimer filtering and message blocking
- Presence of direct relationships with key collaborative technology providers, including listing on those websites and marketing materials
- Content capture development methodologies that minimize the gap between new collaborative feature releases and updates to the capture solution
- Complete portfolios of onboarding, professional services, support, training and customer success services
- Ability to deploy content capture solutions to align with the firm's IT architectural objectives, whether on-premises, in the cloud or while in transit
- Transparent processes to notify firms of service changes or disruptions and enable customer self-diagnosis, where possible

Conclusion:

The already-increasing popularity of Microsoft Teams and Slack, along with a suddenly remote workforce, have moved the adoption of IM and collaboration technology onto a new trajectory. More firms are experiencing the benefits of greater productivity and improved responsiveness to colleagues and customers as a result of collaboration technologies. They are also experiencing a reduction in the issues typically associated with being overrun by email. The trend is only set to continue.

These tools create new challenges for compliance teams, given their multi-modal, interactive and conversational platforms. Any activity that occurs within a virtual meeting could potentially be relevant to a regulatory event. Such activities may include employees joining and leaving chats, individuals modifying or editing content or replies that occur hours after the beginning of a persistent chat.

The sheer variety of collaboration tools on the market is a challenge on its own. Some of these are just a free download away, and not as well-suited to enable firms to meet their SEC, FINRA or FCA books-and-records and supervisory obligations.

In addition to regulatory risks, the choice of the wrong tool — or the unguided use of a market-leading technology — can expose a firm to several other vulnerabilities. These are led by very visible and real InfoSec threats, such as the recent increase in spam, ransomware and other advanced targeted attacks.

Firms must acknowledge that content with business value and risk can live on any collaboration tool. The surface area for loss of intellectual property, violations of codes of conduct or policy infractions has now increased dramatically. With the implementation of GDPR, CCPA and emerging laws, firms must also consider data privacy risks and their ability to respond to right of access requests that might center on the use of a collaboration tool.

Compliance teams seek to allow their businesses to use the collaboration tools with which they are familiar and that enable greater productivity. Doing so requires a thorough evaluation of the benefits and risks exposed by each collaboration tool. The selection of tools should be weighted toward those where risks can be mitigated using the appropriate capture technology.

Updated policies must reflect the accepted and prohibited use of each collaboration tool modality. Additionally, guidance must be issued to users to ensure that they understand how to safely get their job done on approved tools without introducing unnecessary risk.

References:

1) https://nemertes.com/research/the-relentless-shift-from-uc-to-workstream-collaboration/

2) https://venturebeat.com/2019/03/19/microsoft-teams-is-now-used-by-500000-organizations/

3) https://www.theverge.com/2019/7/11/20689143/microsoft-teams-active-daily-users-stats-slack-competition

4) https://www.smarsh.com/webinars/assessing-benefits-costs-of-todays-collaboration-tools

5) https://www.microsoft.com/en-us/microsoft-365/blog/wp-content/uploads/sites/2/2019/04/Total-Economic-Impact-Microsoft-Teams.pdf

6) https://a.slack-edge.com/eaf4e/marketing/downloads/resources/IDC_The_Business_Value_of_Slack.pdf

7) 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

8) https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/09/remote-work-trend-report-meetings/

9) https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

10) https://www.bleepingcomputer.com/news/security/slack-bug-allowed-automating-account-takeover-attacks/

11) https://www.smarsh.com/webinars/assessing-benefits-costs-of-todays-collaboration-tools

Smarsh is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

US: 1-866-762-7742 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh