smarsh®

THE DEFINITIVE GUIDE TO ELECTRONIC COMMUNICATIONS CAPTURE
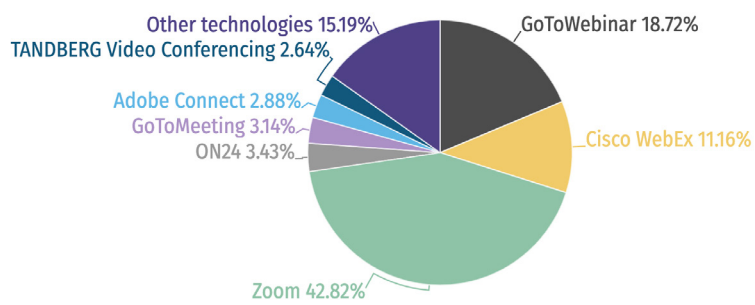
Conferencing Technologies

smarsh®

THE DEFINITIVE GUIDE TO ELECTRONIC COMMUNICATIONS CAPTURE

Conferencing Technologies

Online meetings were already a regular occurrence in our professional lives. But since the onset of the COVID-19 pandemic, they have become the estuary from which all information flows. Organizations must be able to quickly adapt to these social and environmental pressures, as well as the resulting industry changes.

In December of 2019, Zoom reported the number of daily meeting participants was 10 million. By March of 2020, that number had increased by 1900% to 200 million.[1]

Market share of top web conferencing technologies in the United States, as of April 2020

- Other technologies 15.19%
- TANDBERG Video Conferencing 2.64%
- Adobe Connect 2.88%
- GoToMeeting 3.14%
- ON24 3.43%
- GoToWebinar 18.72%
- Cisco WebEx 11.16%
- Zoom 42.82%

Source: Statista, Datanyze

Top 3 US Web Conferencing Apps Hit Over 70% Market Share[2]

Zoom was not the only beneficiary of the suddenly remote workforce. Other established conferencing technologies used by regulated organizations, such as Cisco Webex Teams, BlueJeans Network (recently acquired by Verizon), 8x8 and others, have experienced spikes in usage.[3,4] This has also spilled over into the collaboration space. Video use has increased exponentially, as illustrated by Microsoft Teams' 1000% video growth.[5]

Unfortunately for regulated firms, for every established conferencing technology seeing expanded use, there has also been a surge experienced by more risky newcomers. Technologies like Discord and Marco Polo, for example, have massively increased in adoption but were not designed to meet the requirements of financial services firms.

The benefits of enabling conferencing technologies

Embracing web conferencing as part of your communications strategy offers several benefits, including:

- Ability to easily and rapidly transition employees to remote work

- No scheduling conflicts like those with a physical meeting room

- Elimination of commute and travel times, adding to productive work hours

- Ability to share documents electronically with some or all attendees

- Ability to virtually meet with people anywhere in the world

Aside from saving time and resources, web conferencing can also significantly increase collaboration and customer satisfaction. Perhaps the most valuable benefit, though, is the advantage a business gains by assuring its flow of information does not have to be interrupted.

The unique challenges of capturing content from conferencing technologies

The transition to a remote work environment was daunting for many companies. Physical meetings were suddenly replaced by electronic communications, where users are sharing files, chatting about the firm's business and directly engaging with customers.

Organizations have shifted their view of conferencing technologies themselves. Rather than simply tools for "video broadcasting," business itself is being discussed, shared and delivered using conferencing technologies. This raises unique challenges, including:

- Choosing conferencing technology that is not designed to meet the requirements of regulated firms

- Inability to capture key features and modalities due to the lack of available APIs or other reliable methods of capture

- Capturing large video conferences files, which are typically significantly bigger than other content types

- Enforcing communications policies across those networks

- The current lack of regulatory guidance on the capture of video conferencing content. Firms must continue to push regulators to define the parameters around necessary capture and storage of this data

Any of these challenges could have a serious impact on operations and force a business to balance compliance and productivity. These are trade-offs that could significantly raise a business's risk exposure.

The risks associated with conferencing technologies

As with any communications source, there are certain risks associated with using conferencing technologies.

Home networking risks

A sudden transition to remote work meant that many firms did not have the opportunity to set up employees with proper infrastructure. Some are now working from home at their dining room tables on the family computer that is not current on its security updates. Others may be on unprotected Wi-Fi networks or sharing bandwidth with family members that can cause connections to drop in the middle of an important client meeting.

User identity risks

Conferencing technologies all have unique controls to guard against unauthorized access to meetings. However, despite enabling waiting room features or protections for user-specific access codes, firms are only one user error away from a potential unwelcomed visitor (or "Zoom bomber") into an important meeting.

InfoSec risks

Issues with security protections from conferencing providers are well documented. These include their use of end-to-end encryption and protections against malicious attacks, credential stealing and ransomware. For those conferencing providers who seek to serve the financial services industry and other regulated markets, enhancing their security posture is essential. The need to withstand rigorous security audits will be a prerequisite to ongoing adoption in those markets.

Data privacy risks

The potential presence of personally identifiable information (PII) within video conferencing is a new reality firms are facing. This has given rise to the recent adoption of the California Consumer Protection Act (CCPA), as well as other state regulations that require that prior consent be given prior to recording a meeting (or video conference).

IP and data loss risks

As more companies conduct customer meetings, webinars and virtual conference presentations, they must be extra diligent about high value or sensitive information that may be discussed or presented in an online conference. Firms are a simple screen grab or iPhone photo away from a potential loss of an important business asset.

Regulatory risk

Every regulated firm needs to meet regulatory recordkeeping, storage and supervisory requirements for communications that are approved for business use. If conferencing technologies are used, firms must capture all generated content, such as instant messaging activity.

Mitigating the risks of conferencing technologies

As with other content sources, risk mitigation of conferencing technologies is a function with three variables: 1) policy adjustments, 2) updated user training and 3) selection of the appropriate capture technologies. Each of these deserves further exploration.

1. Policy Adjustments

Here are some of the most critical policy adjustments required to address conferencing technologies:

- **Retention policies** should be adjusted to any modality that can be captured and is used for business purposes, such as instant messaging. Firms should also monitor advances in functionality provided by conferencing providers, so that they can adjust capture practices as those solutions become available. They should keep up with additional guidance provided by regulators for recommended recordkeeping treatment of video conferencing technologies.

- **Communication policies** - Video conferencing is one of the most critical areas where communications policies should be updated. Policies should outline acceptable and prohibited uses of approved conferencing platforms as well as clearly identify platforms that are prohibited from use entirely. This should be prescriptive, recognizing that video meetings can easily take on a casual, informal feel outside of the familiar norms of in-person business meetings.

  While policy infractions are independent of the method of delivery, video does create some unique conditions. One example is the mandated use of backgrounds to avoid any unintentional display of offensive material. Alternatively, a policy to not use the camera function except when speaking can minimize the risk of something embarrassing being shared with your customers

- **Content inspection/surveillance practices** - In addition to the supervision of regulated users, firms should also periodically inspect conferencing for code-of-conduct or IP policy infractions. A good place to begin is with client-facing video meetings. Recordings should be reviewed prior to publishing or sharing that information with clients or prospects.

2. User training

Each conferencing technology provides a unique set of features and enables access to only a subset of these features for capture. Therefore, user training on acceptable and prohibited use policies is imperative. For example, if the firm prohibits the use of files subject to NDAs within conferences, that needs to be explicitly addressed in training programs and regularly monitored by the compliance team.

Training should also address the appropriate use of security and privacy features within each platform. These include the use of waiting room features, the importance of not sharing user-specific access codes and training for meeting organizers to carefully manage distribution and attendee lists. This is to ensure that ethical wall or other policy violations are not created.

3. Selecting the appropriate capture technologies

There are different options available for capturing content from conferencing technologies. It is important to consider these alternatives in more detail.

Capturing content from conferencing technologies: the alternatives

There are alternatives to using a specialized content capture solution. Some businesses choose to explore the native features within the communications tools or to build their own solutions.

1. Native features:

There are differences between out-of-the-box functionality and specialized capture solutions for conferencing technologies. Most important are the mechanisms provided by each to capture the unique conversational content, context and metadata that are produced by the multi-modal platforms.

Every tool is different, and none are specialized to meet the unique requirements of highly regulated firms. If attempting to capture content directly via web conferencing providers, firms should consider the following:

- Level of access available via back-end APIs
- Events that are accessible for capture
- Amount of accessible historical content
- Storage technology used by the provider to ensure immutability
- Data security and privacy
- Notification procedures for API updates and enhancements

2. In-house solutions:

Some businesses with large IT development resources have chosen to develop their own connections to web conferencing content sources as a strategy to reduce cost. While this may be suitable for some, businesses should consider the following:

- If IT is a core part of the business strategy
- How many communication channels are currently supported
- At what rate new channels are added
- Who will provide support for maintenance and disruption in the capture of data flows
- Where the content will be archived, and if that archive can scale

3. Specialized third-party capture solution:

This is often considered the safest and most comprehensive option. The solution must have the capability to capture communications in full context so firms can leverage their rich metadata and see how conversations start and develop. When content can be sent directly to a robust data archive, communications can be accessed and understood alongside other communications sources such as IM and collaboration content. Some table stakes capabilities are outlined here:

- Ability to capture direct and group chat content
- Capture of voice content for platforms such as Zoom
- Ability to send content directly to an archive for retention and further analysis

Conclusion

Web conferencing technology is not just a featured component of a communications strategy; it is essential to conducting business. All businesses that are required to — or would like to — manage and monitor communications must have a way to capture that content and enforce related policies.

For businesses that are not in the IT industry, taking on these challenges may be more onerous than they anticipated, and they may be unable to keep up with regulatory requirements. Likewise, relying on the native features some technologies offer may leave gaps that increase a business's risk exposure.

For most, the best course of action is to rely on a specialized provider. A fully managed content capture solution allows organizations to fully adopt web conferencing technologies without the increased concern about risk exposure.

References:

1) https://venturebeat.com/2020/04/02/zooms-daily-active-users-jumped-from-10-million-to-over-200-million-in-3-months/

2) https://learnbonds.com/news/top-3-us-web-conferencing-apps-hit-over-70-market-share/

3) https://www.bluejeans.com/blog/video-conferencing-usage-during-coronavirus-outbreak

4) https://finance.yahoo.com/video/zoom-competitor-8x8-sees-spike-195401644.html

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

smarsh®

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.