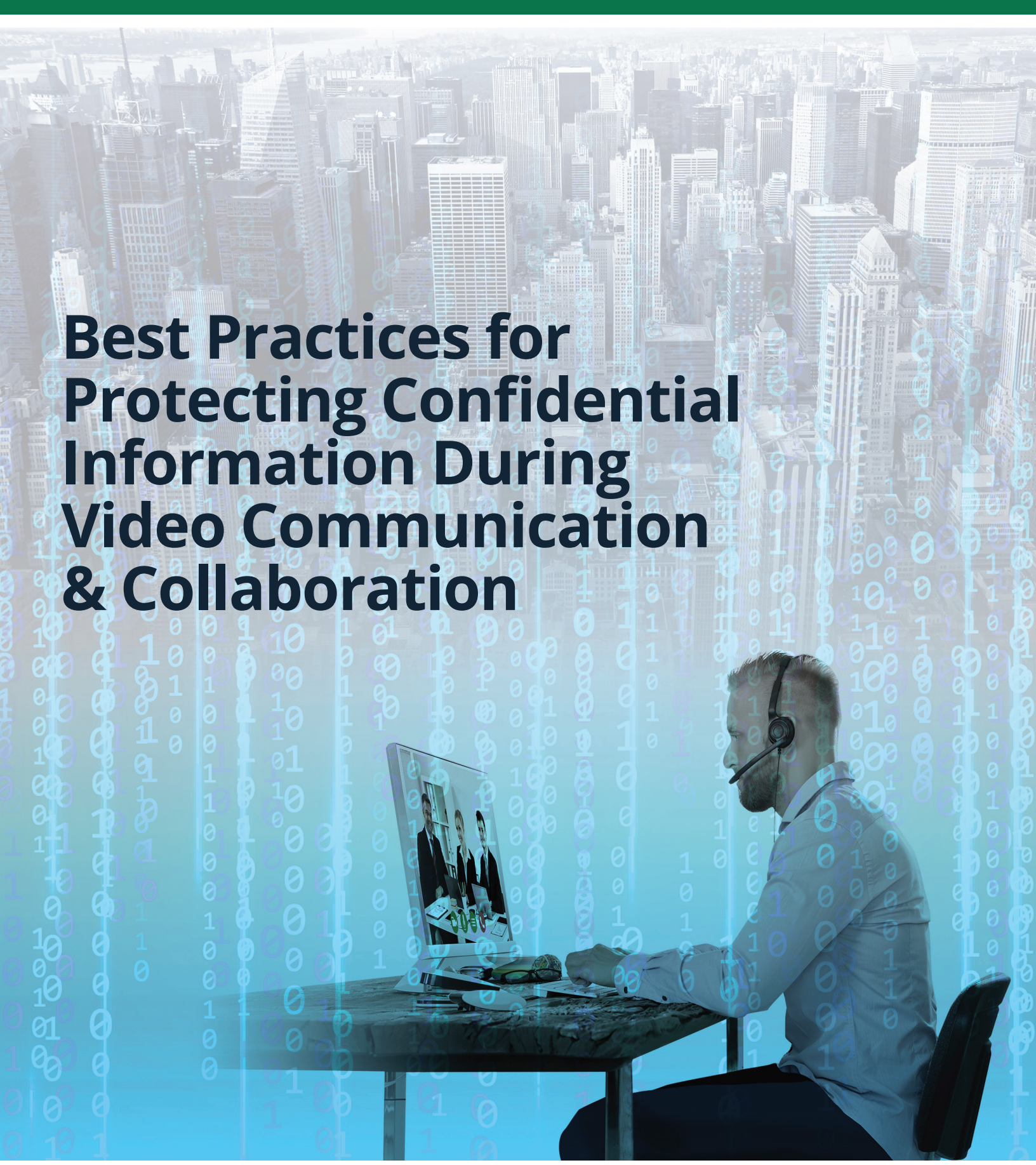
Best Practices for Protecting Confidential Information During Video Communication & Collaboration



THETALAKE

Introduction

Video conferencing has transformed the way businesses operate. It humanizes digital communications and enables people to make connections with each other. With the simplicity of exchanging electronic communications in new ways, it maximizes employee collaboration and customer engagement.

And, video conferencing is a primary avenue for potential inappropriate sharing and data loss.

Sharing all types of data over video has only become easier and more multifaceted. There are unlimited scenarios where companies can experience loss of sensitive and regulated data given video is more robust than any other communication form. Yet, video is an area where companies have allowed a rapidly growing blind spot to go unchecked.

With the increased sharing capabilities, improved connectivity from any device and location, and greater ability to record at lower costs, the rationale to forgo video monitoring makes less and less sense. This is especially true with the shift in regulatory focus from capture and storage to proactive measures for privacy and data protection. It's simply not safe for companies to ignore the most robust and fastest growing data communication channel they own.

It's important for companies to harness the power provided by video communication while also ensuring they have solid oversight on sensitive and confidential data. This can be achieved with a video data monitoring model that provides:

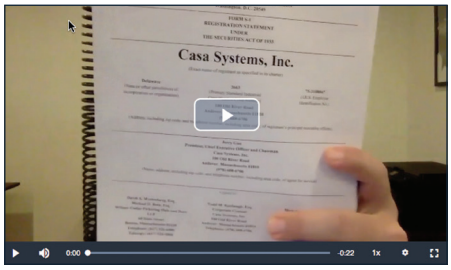
1. Basic risk assessment capabilities with the ability to conduct audits on a representative sample of recordings
2. Persistent recording review and supervision after identifying key demographics for ongoing monitoring
3. Practical real-time help during video calls to avoid mistakes, put users on notice, and boost auditing

Where Can Data Loss Occur in Video Conference?

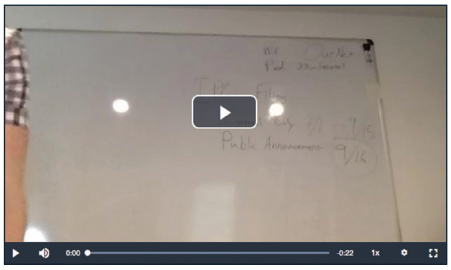
Video conferencing is a rich platform that supports several forms of electronic communication. When it comes to potential data loss, there are many ways to share and show confidential data and display risky insider behavior.

Video

Visible details shown on camera, including the whiteboard, notepad, and background



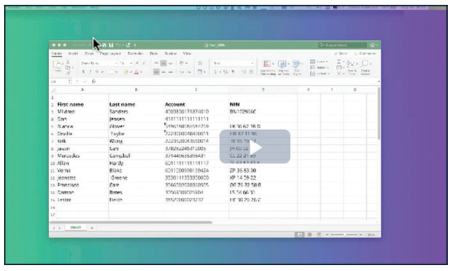
Financial report details



Whiteboard with password details

Collaboration

Files and information shared on screen like documents, presentations, and virtual whiteboard

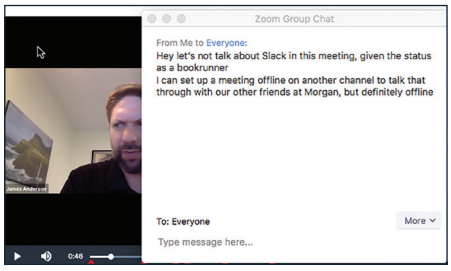


Excel sheet with account numbers

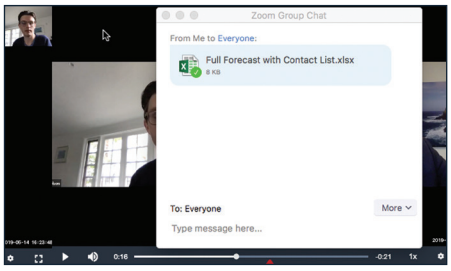
Virtual whiteboard with confidential information

Chat

Information communicated in text format and files shared over chat



Misleading chat exchange



Financial forecast file shared in chat

It's important to note that you can't simply disable these potentially risky features, like whiteboarding, chat, and content sharing without impeding the benefits of using video conferencing. Video conferencing is popular and effective because of these capabilities. Instead, you should have a plan, process, and technology approach for reducing the risks of embracing video collaboration.

Video Conference Data Loss Prevention (DLP) Best Practices

Incorporating DLP into your company's use of video conference can be simplified with the right processes and technology. Organizations can quickly get started with the following best practice recommendations:

PROCESSES

Starting with a well thought out plan for video data loss prevention will guide your steps and ensure your efforts are focused on the most important areas to mitigate the risk of losing confidential data during video communications.

1. Prioritize the Types of Videos to Review

Your video DLP plan should identify and prioritize the user groups and types of video communications you want to supervise, including all the components of a video call (i.e., video, collaboration, and chat).

The highest priority videos are those that may contain content and activity that are likely to include confidential data. For example, you may want to focus on teams that interact with clients and share client data, as well as teams that work with confidential and personally identifiable information such as M&A, IPOs, client policies, claims, and more. These types of video communications are a prudent starting point and you can expand your priority list over time.

2. Audit for Risks

Establish a plan for the types of risks you want to look out for in your review process. This ensures you're thinking about specific opportunities for confidential data loss in what gets shared, as well as considering potential misconduct risks in how people behave. An ideal approach aligned to best practices is to start with a risk assessment where you are reviewing a sampling of recordings across all groups.

3. Adopt Persistent Recording Review

Once you've run an auditing program for a period that has allowed you to identify your high priority video scenarios and user groups, you should expand your program to conduct ongoing review for all the videos that meet your identified high priority criteria. This advances your video monitoring program to the next maturity stage that ensures your organization is actively protecting against misconduct and data loss in video conference communications.

4. Define Your Format for Supervision Review Workflow & Reports

Your review process should follow a well-mapped workflow that is consistent across videos and review outcomes. For example, you should identify your first and, if desired, second-level reviewers and the steps that you want your reviewers to follow when a risk is identified during a review cycle—based on the type of risk.

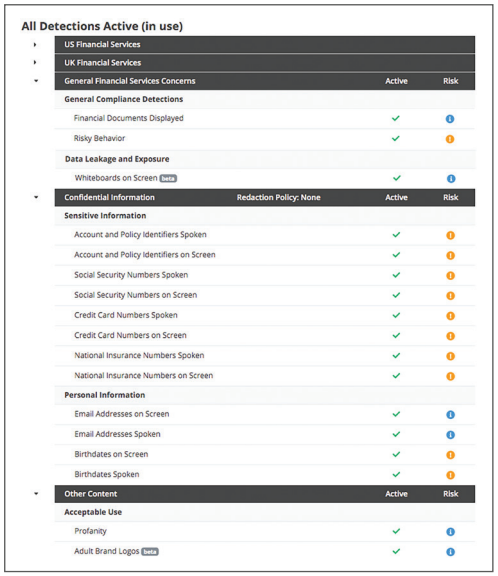
Your reports should include details on the authorized reviewers, review steps, and the outcome of the review. If your review discovered compliance risks, you should denote where the risks occurred in the video and the steps that were taken to resolve the risk. This rigor ensures that you're applying the best duty of care to mitigate organizational risk.

TECHNOLOGY

The right technology will streamline your video review process. Adopt a solution that provides full video recording and supervision, as well as visual, audio, and chat content review with automated supervision for archived videos. The ideal technology for your organization should include these essential requirements:

1. Strong Partner Integrations

First and foremost, your solution should support your existing video conference platform. Doing so allows you to automate your video recording ingestion, map specific users and groups who require review, and customize policies based on those groups. And, of course, you'll want to verity that it supports a wide range of video conference vendors. This will give you the flexibility to easily change your company's video conference platform in the future without losing integration capabilities between the two products.



Risk detection policies for all video content

2. Advanced Analytics for Visual, Voice, and Text Content

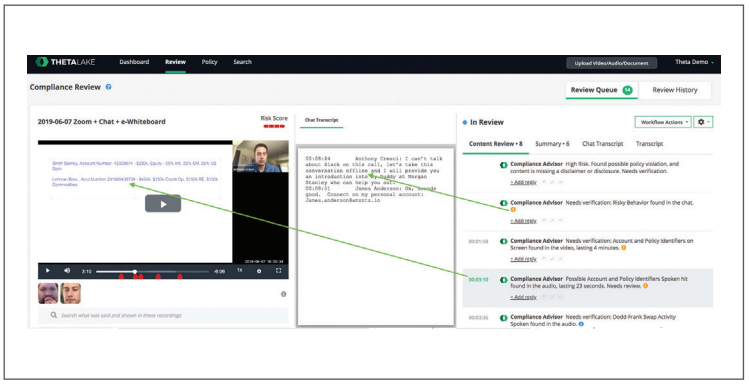
Confidential data can come in many formats during a video conference meeting, including visual, audio, and text content. Your solution should have comprehensive analysis capabilities to address each of these mediums. These should include natural language processing, machine learning, facial recognition, image recognition, whiteboard identification, document analysis, and text analysis, as well as optical character recognition (OCR) and audio transcription analysis.

3. DLP Policies

Your solution should have pre-built policies that are tuned for identifying real and relevant data loss risks, including detecting confidential data, risky behavior, compliance risks, and even letting your risk teams know when a whiteboard was visible in the background.

4. Ease of Use

The ideal solution should have extreme ease of use that requires minimal effort to get up and running. For example, the solution should make it easy for you to roll out video recording and review to a subset of your employees or groups and to selectively record their video conferences for a short timeframe. Taking this approach coupled with a selective review of those recordings is an easy way to start. From there, you can do recurring audits, which is an equally powerful approach with low resource impact and a high return due to knowing versus speculating on organizational risks.



Theta Lake points reviewers to risk on screen, in chat, and more

5. Automated Workflow

Manually keeping track of your review progress and status creates a time-consuming and complex process. Your solution should eliminate this hurdle with an automated workflow process that is directed, easy, and consistent.

6. Real-Time Resources for User Training & Behavior Modification

Your solution should have resources available in "live" video calls that provide your users with your corporate disclaimers, disclosures, and confidentiality statements that make it easy for them to do the right thing at the right time.

In addition, your solution should help your users to reduce potentially risky actions by providing real-time alerts when they are doing something that might introduce risk, such as sharing a screen or turning on their camera. This provides real-time tips to help your employees avoid mistakes while reinforcing that their riskier actions are being reviewed as part of your video monitoring program. These solution capabilities will help drive a dramatic reduction in careless behavior.

Theta Lake: Making Video DLP a Reality

Theta Lake provides a purpose-built solution for protecting your confidential information during your video communications. Because video is such a rich medium, our solution provides comprehensive detection of risks in audio, visual, and documents that are spoken, shown, typed, or shared in a video conference.

Theta Lake applies deep learning and AI to automate video data loss prevention and manage workflow for potential confidential data and compliance risks. Our solution scales your video supervision efforts saving you time and resources while reducing your organizational risk.

KEY FEATURES

Enterprise Integrations

Provides an enterprise-ready solution with extensive video conference platform integrations

Powerful Risk Detection

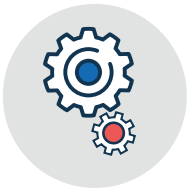
Powerful natural language processing and deep learning detect confidential data and risky insider behavior

Pre-built Policies

Our pre-built policies are driven by our AI and data scientists who have extensive DLP and compliance risk detection expertise

RealTime Compliance Advisor

Supports your employees during a video meeting with compliance resources, such as disclaimers, to help reduce risky actions by reinforcing the company's video monitoring program

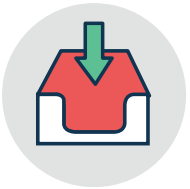


Advanced AI Workflow

Sophisticated, visual workflow system with an AI-assisted review workspace to enable fast and efficient review

Detailed Reports

Gain a full picture and context of your video recordings with detailed reports on the video recording, policy violations, reviewer comments, and review steps



Archive

Capture and store electronic communications within video conferencing, such as chat, file sharing, whiteboarding

Learn More

https://thetalake.com/solutions/video-monitoring/

ABOUT THETA LAKE. Theta Lake provides cloud-based compliance for video, audio, and other modern digital communications. Its patent-pending technology uses AI, deep learning, and seamlessly integrates with the leading audio recording, video marketing, and video conferencing platforms to detect compliance risks in what was said or shown in modern digital communications. Using AI to also power insights and automation, Theta Lake provides directed workflow to add consistency, efficiency and scale to the compliance review and supervision process, driving down the cost of compliance.