10-Point Plan To Protect Your Business From Zoom-Bombs And Other Videoconferencing Privacy Concerns

Insights
4.24.20

The COVID-19 pandemic has caused many employers now operating remotely to conduct meetings via video conference – which has created a whole new set of various privacy and cybersecurity concerns. While these remote work tools have facilitated a more personal connection and interactive experience, their use is fraught with privacy concerns you may never have before considered. If your organization is weighing its options or unaware of the risks these services may create, this article provides a 10-point plan to protect your personal and confidential information and ensure you remain compliant with various federal and state privacy laws.

The Risks of Video Conferencing
Before diving into the blueprint for compliance, it is first helpful to understand the three main risks of vide conferencing.

"Zoom-Bombing"
Since the start of the COVID-19 public health emergency, the FBI has noted a substantial increase in the number of businesses and schools reporting instances of video conference "hijackings" (also known as "Zoom-bombings"). During these hijackings — which generally occur where a video conference link is shared over social media or is not password-protected — uninvited participants have disrupted meetings by interjecting inappropriate language or displaying hateful or pornographic images into business meetings.

Aside from unwanted disruptions, uninvited interlopers pose a more serious threat. Those that choose to remain undetected could lead to the unauthorized disclosure of personal or confidential information.

Insufficient Or Non-Existent Encryption
Many video conferencing companies tout their services' encryption capabilities. However, these claims should be closely scrutinized. By way of example, the video conferencing platform Zoom has indicated that hosts may "enable an end-to-end (E2E) encrypted meeting." This was reportedly proven to be untrue. The company was supposedly able to access user data and video conferences in transit and it was reported that it could be compelled to provide access or information to the government if such a request was made.

Additionally, the storage of recorded video conferences creates other issues. Thousands of Zoom conference recordings were recently found on an unsecured online storage platform. Prior to Zoom restricting access to their storage location, anyone with an internet connection could access the private and confidential meetings of countless users. Likewise, if your business does not store its recorded conferences in a secure manner, there is a substantial possibility that an unauthorized individual may gain access to their contents.

Inadequate Privacy

Video conferencing raises privacy issues on two fronts. First, according to a recent California class action lawsuit, video conferencing providers may be improperly using their subscriber's data. Specifically, as alleged in the suit, California's privacy law and other state statutes may have been violated if users' personal information was shared with Facebook without the users' consent.

End-users may also create privacy issues. Among other things, confidential information may be mistakenly divulged if an employee shares their screen while such information is visible. If an end-user participates in a video conference in a public space, everything that is said and displayed during the conference is disclosed to those around them. Moreover, if an end-user records or takes screenshots of images displayed during the meeting, those items may be improperly disseminated.

Legal Consequences Of A Video Conferencing Breach

If you or your video conference provider has inadequate privacy and cybersecurity policies or procedures, your business may inadvertently run afoul of various federal and state laws. Among other laws, the unauthorized disclosure of your employees' personal and confidential information may violate:

- The Health Insurance Portability and Accountability Act (HIPPA) (prohibiting the disclosure of sensitive patient health information without a patient's knowledge or consent);
- California's Consumer Privacy Act (CCPA) (regulating the access to, deletion of, and sharing of personal information collected by businesses); and
- The European Union's General Data Protection Regulation (GDPR) (a wide-ranging law that governs how companies collect and manage data).

10-Point Plan To Prevent Video Conferencing Disasters

To avoid potential video conferencing related privacy or cybersecurity breaches when using Zoom or similar platforms, your business should consider employing the following practices:

1. Review your conference provider's privacy policy and user agreement. Also ensure you have the most recent version of your video conference provider's software before you launch a new meeting.
2. Ensure that your conferences are set as private, not public.
3. Require passwords for all meetings. And while this seems simplistic, do not post passwords (or

meeting links) to social media.

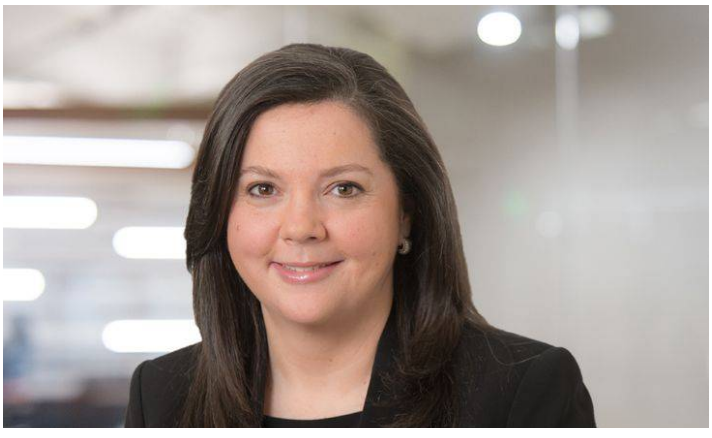
4. If available, create a waiting room that allows the conference host to individually admit participants. Review all meeting attendees before starting the conference and remove uninvited participants who gain access to the meeting. Once all expected attendees have joined, lock the meeting.
5. Limit who may share their screen.
6. Disable cameras and/or mute non-presenting conference participants, and consider disabling private chat.
7. Prevent attendees from changing user names to conceal identities.
8. Ensure no confidential or personal information is visible before sharing your screen.
9. Instruct all participants to refrain from recording or screenshotting any information shared during the meeting.
10. Review (and if necessary, create or revise) your company telework and IT policies to ensure that employees are aware of the steps they must take to keep the personal and confidential information they possess secure.

Conclusion

In the wake of the COVID-19 pandemic, many employers are relying on video conferencing platforms to conduct meetings and providing remote educational instruction. While Zoom and other video conferencing platforms can provide a valuable interactive experience while social distancing, it is important to educate employees on potential privacy and cybersecurity risks. You must require them to adhere to best practices to ensure the security of remote meetings, protect the privacy of participants, and reduce the risk of intervention by unwanted participants.

This Legal Alert provides an overview of a specific developing situation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People



Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber