Videoconferencing: Keeping Workers and Data Safe

With state COVID-19 measures forcing many businesses to direct employees to work from home, companies have rushed to find ways to hold meetings virtually. Some are utilizing existing videoconferencing solutions, others are quickly rolling out new platforms they never before tested, and even more are directing or allowing users to utilize platforms with personal accounts over which the business has no control. These platforms include solutions such as Cisco Teams, Google Hangouts, Microsoft Teams, Skype, Webex and Zoom.

Each of these platforms has its own benefits and drawbacks. This article is not designed to help you choose the best provider for your business, but rather to highlight common privacy and security issues inherent in videoconferencing platforms, as well as suggested best practices for all platforms.

Enterprise Solutions vs. Personal Accounts

When an employee uses an enterprise-provided solution, many security issues are minimized or eliminated if the platform has been properly configured and the user properly educated. Not

only has the business had the opportunity to vet the product for security adequacy, but proper controls can also be put in place. Proper controls may include prohibiting file sharing and enabling certain security features by default, with no user input.

On the other hand, when a personal account is used with a solution that is not provided by the enterprise, the business has no control over how the platform

is used or what security features are enabled. This scenario is most common with the Zoom video platform, which has seen explosive growth in popularity in the past three months.

Selecting an Enterprise Solution

Businesses are suddenly utilizing videoconference platforms with which they have little to no experience. Some businesses are learning now that their prior selection of a platform may not have been the best for their business.

While the current circumstances limit the normal testing and vetting that might otherwise be undertaken when selecting a videoconferencing solution, that does not mean the easiest, most popular or cheapest solution is the right answer. Take time to select a vendor, speak with others who have lived with these products for years, and personally get to know the safety features and usability before making a selection.

Companies that already were forced to make a selection can still revisit that choice, properly configure the security settings that are available, educate end users on best practices and offer and require safety training. Being rushed initially does not mean that a business cannot now slow down and take a more measured approach.

Public Meetings

Some platforms permit any user to join any meeting. While this does take some guesswork, once a user successfully accesses a meeting, all information and conversations are exposed.

Zoom famously previously set its default meeting setting to not require a password, allowing

unrelated third parties to "Zoombomb" a meeting with pornography or radical political content.

Although Zoom did correct the default no password problem, there remain cases in which meeting notices and passwords/codes have been shared on websites or social media. Any sort of public disclosure should be completely avoided. Additionally, even if the organization sets the application to require a password, it can still be disabled by individual users.

Recorded Meetings

One of the lesser-known features of some platforms is the option to record meetings. While a host may have a valid reason to record a meeting, the same can rarely be said of a participant and that feature should be disabled for participants. Confidential and/ or proprietary information may be shared as part

of a meeting, and recording a meeting is almost universally a bad practice. Additionally, hosts should be aware of the laws prohibiting the recording of participants without their consent.

Settings for Individual Meetings

Some videoconferencing best practices for users include:

- Allow only the host to share their screen.
- A webinar meeting will always be inherently safer.
- Disable all video for participants unless the purpose is a video call.
- Mute all participants unless the purpose is for all speakers to be heard — most platforms allow muting on a per-user basis.
- Use the "waiting room" feature, if available — the host may then screen all participants before joining.
- Use the invitation-only feature — once all invitees have arrived, "lock" the meeting to prevent additional participants.
- Consider disabling the private chat feature if there is any concern that side conversations may be a distraction or there could be a data leak.
- Some platforms will automatically blur your background, or allow you to select a background from their gallery or from your personal photos — this will protect your privacy at home.
- Do not reuse the same link and password for multiple meetings.

Mark G. McCrear
Co-Chair, Privacy & Data Security Practice
215.299.2010
mmccreary@foxrothschild

Fox Rothschild