ISEA Guidelines for Video Conferencing

The need for security guidelines for video conferencing is growing as more and more companies look for new and innovative ways to make employees more productive through video collaboration which overtook the traditional face to face meeting.

In view of COVID-19, an increasing number of employees are working from home, collaborating with internal teams or customers via video conference on mobile devices. To meet the technology needs raised by this trend, a lot of organizations are implementing Bring-Your-Own-Device (BYOD) policies, allowing workers to work and communicate from their own personal devices, improving their flexibility and work-life balance as a result.

The changes in the way we work and communicate clearly promote a wealth of benefits for both businesses and the individual, but despite all the advantages of video conferencing across the organization require policies and security practices to be put in place in order to guarantee maximum data security.

It is important that users of videoconferencing, particularly those that are connecting their own devices to the system, clearly understand their responsibilities when it comes to security. Organization’s security policy should provide a set of guidelines for employees working from their personal devices and clear consequences for improper use.

Best security practices for businesses/organizations that should be followed when implementing video conferencing solutions.

1. Create a Bring-Your-Own-Device (BYOD) Policy

Allowing employees to use their own devices for work can have a significant competitive advantage for the organizations, but there are security considerations that must be taken into account. There is a need for strict policies in place with respect to employees using their own personal devices or else the company’s security could be at risk from unsecure networks, lost devices, forgotten or even complete lack of secure passwords.

An effective BYOD policy should include the following:

- Finely tuned security measures for using personal devices
- Training programs for employees to address the issues of compliance and consequences of improper use of personal devices towards official work

2. Implement Staff Training

- Implement adequate training for staff on necessary security measures, particularly when sensitive data and private information is being shared.

- Create and enforce appropriate standard operating procedures (SOPs) with device support and usage policy, encouraging users to follow security protocols and update their devices when necessary.
- Procedures should include things to be aware of in a video conference – simple things like what settings to use in order to prevent unwanted guests joining the call, and what equipment to switch off at the end of a call.

3. Review & Update Video Systems

- Review and enable appropriate security and privacy settings to prevent threat actors from exploiting known vulnerabilities.
- Use video conferencing systems/apps which support encryption. If it is not supported there is a greater risk of sensitive data falling into the wrong hands.
- **Patching**: Make sure video conferencing software is patched with the latest vendor-provided updates and have automated upgrades turned on.

4. Secure Networks and Devices

- Transmitting sensitive information and data across internal and external networks, businesses/organizations need to be assured that their conferencing solution is safe and not susceptible to security breaches.
- There should be a process in place to ensure that the devices used to access organization network are safe. The devices should have not been subjected to modifications such as jailbreaking, rooting, threatening malware, spam, or applications that can compromise the organization network or data.
- Make sure users and devices that are accessing the organization network on-premise or off-premise can be identified and allowed connectivity only if they are authorized and meet company policy.

5. Check the Signs

Most security-minded video conferencing systems use single sign-on (SSO) for user authentication because it greatly reduces the risk of user credentials being lost, stolen or compromised. SSO allows users to keep track of one set of credentials and system admin to track, control access to all video conferencing units quickly determine which video systems were breached, what occurred during the breach, and lock the system to control damage.

6. Use Meeting Lock/password for enhanced privacy

Using meeting scheduler, choose password protection where attendees will need to enter the secret password in order to join the meeting

7. Protect video conference units with permissions

Video conferencing can quickly lead to security issues if the wrong people are inadvertently given access to communications. For example by using open virtual meeting spaces for private meetings, or not getting the settings right when inviting participants. Creating different access levels for different types of conferences, controls can be built in accessing the communication where many video conferencing platforms support the creation of dedicated groups and team collaboration platforms

8. Check Meeting Links

When you receive a meeting invitation, verify that it's from a known, trusted sender. Also, check the meeting link before clicking, watching out for malicious links with ".exe," for example. There's a steep rise in phishing attempts where malicious links have the names of video conferencing vendors embedded but they take you to malicious login sites. Using password embedded links will increase security and reduce war dialing, a technique used to discover or guess the meeting ID.

9. Report Suspicious Activity

Remember to report any suspicious activity to organization Information Security and Information Technology teams. In case of an external video conferencing technology for non-work related calls, reach out to the vendor for the best way to report suspicious activities.

10. Have a Video Conferencing Policy in Place

A video conferencing policy enables to set clear boundaries and expectations for users. In addition to outlining user permissions for conducting video conferences in-house, rules should take into account those who will be connecting remotely. Companies entrusted with especially sensitive information, such as hospitals and financial institutions will want to be specific about who can connect with via video conference, such as pre-approved vendors and clients. A few guidelines most video conferencing policies include are:

- Users must get permission to record a video conference from everyone on the call.
- Personal mobile devices should not be used to record video conferences.
- Sensitive information should be discussed in designated video conference rooms and not in public places or open office spaces.
- Video conferences conducted at a user's desk should train the camera to focus on the users face, and any visible confidential data should be removed from camera view.
- Cameras and microphones should be turned off when not in use.
- Remote control of cameras is for authenticated users only.

Video Conferencing Protocol

1. Be prepared and on-time for the meeting

Make a meeting agenda in advance, send it out to attendees and stick to it throughout the call. Not only does it help with productivity and efficiency, it will also set the tone for the meeting and give others time to prepare their questions and contributions.

2. Keep it brief

Keep your video calls short and to the point. Everyone has schedules that are jam-packed these days, and perky conversation not only is unproductive and time-consuming but can also be extremely frustrating.

3. Utilize visuals to enhance participant interest

Visuals are a great way to keep a meeting interesting and fresh. Sharing applications, PowerPoint presentations, videos, charts, graphs and anything else for real-time collaboration will enhance participation interest.

4.Record the video conference for absent colleagues

Record video call so that late or absent colleagues can later view the information if it fits to the organizations video conferencing policies.

5. Mute when not speaking

If there are several people on a call or a group meeting, with unmuted microphones, the background noise can be extremely distracting. As a common courtesy to others, always mute microphone when a participant is not speaking.

6. Minimize distractions

It is important to make sure that everyone is focused on the meeting at hand and not on other distracting tasks like putting smartphone on silence or out of sight during meeting, disabling pop-up notifications, chats, calender notification and emails when sharing screen with other participants.

7. Don’t forget to be yourself

Just like texting, talking on the phone or walking over to your colleague’s desk and chatting in person, the video conferencing experience is about what’s being discussed. So don’t bother when it comes to getting on camera — just be yourself!

8. Keep meetings right-sized

The more people there are on a call, the more confusing and distracting things can be. Fewer people mean higher collaboration and increased participation.

9. Double-check VC settings

While video calling just takes one click of a button now, it never hurts to double-check settings and make sure audio and camera are correctly configured.

10. Use common courtesy

Because video collaboration is just like an in-person interaction, it is important to use the same courtesy used as someone is in the same room. This includes paying attention to the speaker, minimizing multitasking and refraining from interrupting. Though this may seem obvious, good manners can take it far when building business relationships.

References

- https://www.lifesize.com/
- https://blog.gotomeeting.com/
- https://highfive.com/
- https://blog.paloaltonetworks.com/
- https://www.uctoday.com/