PRIVACY COMMISSIONER RELEASES TIPS FOR SECURE VIDEOCONFERENCING

Posted on May 5, 2020

Categories: Insights, Publications

It goes without saying that organizations' use of videoconferencing is at an all-time high as many businesses have converted to remote work. Like all technologies, videoconferencing poses unique cybersecurity and data privacy risks.

Recognizing the surge in videoconferencing, the Office of the Privacy Commissioner of Canada (the "**OPC**") has published tips to ensure compliance with privacy laws during videoconferencing. Below is a summary of the OPC's tips, together with some advice from McMillan's Privacy and Data Protection team concerning best practices while telecommuting.

Do Your Diligence

Prior to selecting a videoconferencing service, businesses should review the service's privacy policies and terms of use to understand the service's privacy and data handling practices. In particular, review and understand how the videoconferencing provider may collect, use and disclose personal information from those who set up an account or participate in a videoconference call. Consider whether these policies and terms of use align with your business' own privacy policy, contractual terms, and other commitments or obligations with respect to privacy and data handling. Your organization may need to revise its privacy compliance program, including its privacy policy, to permit the use of videoconferencing.

Users of the videoconferencing service should be encouraged to implement and periodically update a unique and complex password when setting up a new account with a videoconferencing service. The OPC recommends that users avoid using social media accounts to sign up for such accounts.

Stay Current

Businesses should stay current on news and publications related to privacy concerns and security vulnerabilities associated with their videoconferencing service of choice.

We recommend establishing a Google alert or other means of tracking updates from reputable sources concerning any reported vulnerabilities or breaches in your videoconferencing software. This will allow an

organization to act quickly to install any patches or updates needed, or take other steps to minimize any security risks. We also suggest that organizations update their patch management policy or program to include regular testing, updates and patching for all videoconferencing services.

Videoconferencing users should also be encouraged to periodically review their devices' permissions and ensure that they are up-to-date.

Limit Participants

Videoconferencing users must make sure that meetings are private and limited to invited participants.

Avoid announcing meetings on social media platforms or websites to prevent uninvited participants from joining the meeting and potentially overhearing private discussions. If possible, ensure that videoconferencing calls are secured with a password, particularly if the meetings involve the discussion of sensitive personal information. Meeting hosts should also disable features such as "join before host" and file transfers to limit security risks.

At the outset of a videoconference, we recommend conducting a quick "roll call", particularly if there are users dialing in who are not visible onscreen. This can help to crosscheck that everyone who is on the call is meant to be there.

Prevent Overhearing & Oversharing

Where the videoconference is held is also important. Participants should ensure that there is nothing in the background of the call that reveals private information, such as a whiteboard or calendar with confidential notations. If using a web browser, users should open a new window for the call and close all other applications, including email, to ensure that confidential information is not inadvertently disclosed if screen-sharing occurs during the call.

The videoconference should be hosted in a private area, ideally a separate room in one's home. However, for some employees, taking a call in a private room or completely out of earshot of others in their household may not be possible. At the outset of a videoconference, we therefore recommend that the host ask all users to disclose if they may be within earshot of others in their home during the call. Such users should listen in to the call by headset, and should be encouraged to send any input containing confidential information either by follow-up email, private chat feature or on a separate call when they are in a private space.

Meeting hosts should disable participants' ability to record a call. Ask attendees to switch off personal home assistants (such as Alexa or Siri) or smart speakers during a video call, as these technologies may be triggered or inadvertently record the call.

Takeaways For Your Business

Given the vulnerability of videoconferencing services to security threats, it is important that organizations adopt the suggestions and best practices developed by the OPC.

However, the above tips should form only a part of a broader effort to address any privacy and cybersecurity vulnerabilities caused by remote working.

Times of crisis give rise to an increased risk of cyberattacks and threats. Threat actors exploit security vulnerabilities, employee distraction and unfamiliarity with new technologies as an opportunity to attempt to unlawfully access sensitive business and personal information. Businesses must emphasize a culture of cybersecurity and compliance with privacy and data protection laws in order to minimize such risks. Providing adequate training and frequent reminders to employees about cyber risks, including the proper use of videoconferencing technologies, is an important step in avoiding data breaches.

While we all eagerly await the day we can connect with our colleagues, clients and customers face-to-face again, many suggest that a rise in working remotely may be here to stay. We advise organizations to act now to develop and implement policies and practices that keep confidential and personal information safe and sound during these unsettled times.

by Kristen Pennington and Chiedza Museredza

A Cautionary Note