More Tips On Protecting Your Virtual Meetings to Avoid A Cybersecurity Breach: An Update

FG Law Blog

April 17, 2020

Donna Urban, Krishna Jani

To view the post on the FG Law Blog, click here.

At this point, many of us are well into our fourth or fifth week of quarantine due to the outbreak of COVID-19. Even for those of us who are fortunate enough to be able to work remotely from our homes, this comes with certain challenges, including potential security issues with virtual conferencing. In our first installment about virtual meetings, and their unintended vulnerabilities, we provided some guidance on how you and your staff might implement certain strategies to keep your virtual conferences as safe as possible from hackers and trolls. In this new installment, we will provide further guidance on staying safe amidst emerging privacy and security concerns associated with virtual meeting platforms.

Zoom Announces Updates to its Data Privacy and Security Measures

On April 1, 2020, the Chief Operating Officer of Zoom, Eric Yuan, announced certain changes that Zoom is making to enhance its virtual meeting spaces. On April 14th, the Chief Product Officer of Zoom, Oded Gal, provided clarification on those enhancements to those of us who are using Zoom during quarantine.

- **Have a plan and be prepared for interference in your virtual meetings.** Zoom has encouraged its users to have a plan in place for their virtual meetings and to be prepared should any unwanted interference arise. This includes ensuring that the application has been updated to include the latest security features, co-hosting meetings whenever possible, and utilizing preexisting and new security tools built into the application. To check for updates to the app, click on the main menu, then click on "Check for Updates," and then "Begin Upgrade" if any new updates are available. We recommend doing this every week or so to ensure that you and your staff are up to speed on all available cybersecurity protections.
- **Co-host and record your virtual meetings whenever possible.** A meeting creator can choose to co-host a meeting while creating the meeting invitation or in the actual Zoom meeting itself. A co-host can monitor the virtual waiting room or assist with any disruptions. Furthermore, record your Zoom meetings whenever possible because recording meetings creates a forensic trail of the meetings, as well as any bad actors that interfere with them, as soon as the meetings begin. The more data that virtual meeting platforms are able to collect about bad actors, the better able they are to stop the threat of further disruption.

- **Zoom has increased access to its security features.** Zoom has made its pre-existing security features easier to find. A "Security" button has been added to the bottom banner of virtual meetings and is now easily accessible to meeting hosts. By clicking on this new security feature, meeting hosts are able to enable a waiting room or lock the meeting. Moreover, a meeting host can also remove a participant from a virtual meeting. Once that participant has been removed, he or she cannot reenter the meeting, even if using a different username. This is because as a part of Zoom's new security rollouts, Zoom has started to collect IP addresses, among other data, to be able to better respond to security threats. While removing a participant from a meeting will only remove the participant from that particular meeting, you have other tools available to permanently block that user.

For example, right now Zoom recommends recording your meetings whenever practicable to ensure a forensic trail is created, as stated above. In addition, Zoom recommends taking a screenshot whenever a bad actor enters your virtual meeting. Then, you can report this intruder on Zoom's website. And starting this coming weekend, Zoom will be releasing a new security feature built into the app, which will allow users to send a report to Zoom right from the security button should any unwanted interference arise.

Other Noteworthy Developments

Zoom announced that as of April 1, 2020, it would freeze all future product development *except* for data privacy and security updates for the following 90 days. Moreover, beginning April 18, 2020, every paid Zoom customer will be able to customize which data center regions their account can use for its real-time meeting traffic. By default, however, there will be no connection to any data centers in China beginning April 18, 2020 for all users. Additionally, users with an ".edu" registered email address are automatically given the highest level of security in their meetings, and this will continue. Zoom has begun to address user demands for a "kid-friendly" interface, but it has not yet launched any such interface.

Other virtual meeting platforms, such as GoToMeeting, have also enacted enhanced security protections in their respective applications. For example, GoToMeeting gathers cyber threat intel through partnerships including external intelligence communities, personal and professional sharing groups, and its own internal research to collect Indicators of Compromise or IoC data. IoC can include forensic data such as IP addresses, domains, hashes, and pulls them into its threat intelligence platform to reduce the risk of cyber threats.

Still though, platforms like Zoom and GoToMeeting urge users to utilize additional security measures as outlined in our previous blog post, and above, to provide the greatest level of privacy and data security for your virtual meetings.

Updates on Regulatory Guidance

On April 8th, Senator Edward Markey, whose priorities include telecommunications, technology, and privacy policy, urged the Federal Trade Commission (FTC) to publish industry cybersecurity guidelines "for companies that provide online conferencing services, as well as best practices for users that will help protect online safety and privacy during this pandemic and beyond."

In Senator Markey's letter, he urges that the guidance cover, at a minimum, the following topics:

- Implementing secure authentication and other safeguards against unauthorized access;
- Enacting limits on data collection and recording;
- Employing encryption and other security protocols for securing data; and
- Providing clear and conspicuous privacy policies for users.

Senator Markey also requests that the FTC develop best practices for online conferencing users, so that they can make informed, safe decisions when choosing and using these platforms. He requests that these best practices cover at least the following topics:

- Identifying and preventing cyber threats such as phishing and malware;
- Sharing links to online meetings without compromising security;
- Restricting access to meetings via software settings; and
- Recognizing that different versions of a company's service may provide varying levels of privacy protection.

To date, the FTC has not published new guidelines.

Remember to have a plan and be prepared. Stay safe, everyone!

If you have any questions, please feel free to reach out to Donna Urban, Krishna Jani, or any member of Flaster Greenberg's Telecommunications or Privacy & Data Security Groups.