crowell moring

CLIENT ALERT

Tele-Hacking: Video Conference Hijacking and Steps You Can Take To Mitigate The Risk and Respond

Apr.03.2020

The world's shift to video-teleconferencing (VTC) in the wake of COVID-19 has presented an opportunity for sophisticated hackers to infiltrate digital meetings and access confidential and proprietary information. This expanding threat has important implications for everyone in the public and private sectors using any VTC platform.

Privacy and security issues in VTCs may pose immediate business, economic, and national security risks. For example, reports suggest a world leader shared screenshots of national security issues during a VTC, raising concerns that national secrets may be compromised. For the private sector, the risks could also be significant. A tele-hacker could obtain access to and trade on inside information, steal trade secrets, or publicly disseminate sensitive and confidential information (or hold that information hostage for a sizeable ransom). To protect against these threats, public and private sector actors should revisit their cybersecurity policies, coordinate with VTC vendors, and ensure a mitigation plan is in place.

For businesses making such services available, redoubling cybersecurity and compliance efforts, and communicating best practices to customers, and users alike, is critical.

Law enforcement is also monitoring these trends. The Federal Bureau of Investigation (FBI) recently released guidance specific to mitigating the risk of tele-hacking with VTC, which businesses may use to benchmark their efforts:

- Make meetings private by requiring a password or controlling the admittance of guests.
- Limit distribution of teleconference links.
- Limit screen sharing to "Host Only" to prevent people and unintended participants from taking over and sharing images or content that is inappropriate or alarming.
- Constantly monitor for software updates.
- When selecting a VTC vendor, consider what security measures those vendors offer, such as end-to-end encryption.

If you believe you are a victim of a tele-hack, it is important to execute your incident response plan and consult technical and legal professionals to help with remediation and analyzing any disclosure obligations to the government, customers, or others.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Paul M. Rosen

Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Gabriel M. Ramsey
Partner – San Francisco
Phone: +1 415.365.7207
Email: gramsey@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com

Kayvan M. Ghaffari
Counsel – San Francisco
Phone: +1 415.365.7223
Email: kghaffari@crowell.com