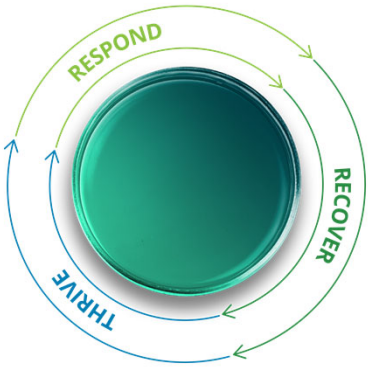
Deloitte.



Sustaining cyber hygiene amid COVID-19 disruption

Focus on collaboration technology

Business disruption associated with COVID-19 has led to greater emphasis on remote work in the past weeks and has subsequently led to an **extreme surge in the use of collaborative content and video/web conferencing platforms**. Users have turned to collaborative services to facilitate business meetings, real-time collaboration, file sharing, and storage. Although many of these technologies were already in use before the pandemic, sensitive topics and materials have shifted to these platforms, creating higher value targets, and the surge in use has drawn greater attention from malicious actors, increasing the likelihood of success for potential threats. As work patterns continue to evolve in conjunction with stay-at-home mandates, there will likely be an even greater reliance on collaboration technologies.

Given the unprecedented speed with which the services have been rolled out, **organizations should be cognizant of technology providers' ability to maintain user privacy and protect data shared on these platforms and implement available controls to protect sensitive information communicated.**

Key cyber and privacy concerns

Prevent camera and screen-share hijacking

- Collaboration technologies should support private, password-protected collaboration environments/ zones
- In instances where this is not enforced, unauthorized users have "dropped" into meetings and taken control of the screensharing function to display illicit content and even gained visibility through a user's video camera.[1]

Protect data and privacy

- Data collected from collaboration tools and platforms should not be shared/disclosed to third parties without prior consent
- Certain information/access should be prohibited, such as encryption key sharing, in foreign operating environments

Provide robust content security

- Comprehensive support for end-to -end (E2E) encryption is critical to safeguard confidential content
- Some platforms and tools may support rigorous encryption standards, but may have exceptions for encryption support that leaves organizations vulnerable without the proper controls in place

[1]FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, March 30th2020

Mitigation activities to consider

Do today

- **Enforce auto-generated password use** for meeting access
- **Enable meeting waiting rooms** and **lock meetings** once they have begun
- **Disable custom meeting IDs and passwords**
- **Disable the ability to integrate with third-parties and social networks**
- **Request (from platform provider) that meeting codes be expanded** to at least nine digits

Do this week

- **Integrate collaboration technologies with Cloud Access Security Broker (CASB) solution** to monitor for data exfiltration
- **Maintain and enforce guidelines on platforms** regarding meeting password access, meeting recording policies, and content transmission on the platform
- **Push security awareness training for meeting hosts** to reinforce secure collaboration practices, such as setting expiration dates for recorded meetings

Do next week

- **Reissue meeting invitations as needed** to include additional security layers
- **Implement a web application firewall** to detect and prevent application layer web-based attacks
- **Enable Single-Sign-On** to consistently enforce authentication rulesets
- **Contact platform provider** for additional information on specific organizational security requests and controls

Takeaways

Collaboration technologies, while vital during the surge of virtual work, can pose serious threats to organizational security and privacy if not properly managed. As these technologies expand their reach and prevalence in business operations, organizations should keep a pulse on potential threats, enact controls where feasible, and promote service availability.

1. **Identify potential loopholes and security vulnerabilities associated with the use of collaboration technologies**
2. **Accelerate implementation of risk-based platform controls to prevent inappropriate information access**
3. **Develop role-based education and awareness guidelines around collaboration applications and remote work**

Contact: Coronavirus Response | USCyberCoronavirusResponse@deloitte.com

Deborah Golden
Principal
debgolden@deloitte.com

Linda Walsh
Managing Director
lwalsh@deloitte.com

Mark Nicholson
Principal
manicholson@deloitte.com