SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW

HEALTH LAW
A SHIPMAN & GOODWIN® ALERT

March 20, 2020

Secure Teleworking at Scale during Coronavirus

Authors:

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

Alexander R. Cox
(860) 251-5236
acox@goodwin.com

With the increase in remote work during this COVID-19 outbreak, many organizations are vulnerable to new data privacy and cybersecurity risks. For teleworkers, we have put together a Best Practices Checklist to help minimize risks associated with remote work. For organizations, we have a Best Practices Checklist with recommended next steps to help your organization manage the risks of teleworking at scale.

Best Practices Checklist for Teleworkers:

- **Avoid public Wi-Fi.** If you are unable to access a trusted network for internet access, use your phone as a hotspot. Public Wi-Fi networks are one of the riskiest ways of accessing the internet.
- **Secure your home network.** Determine if your router has up-to-date firmware and permits secure encrypted communications. If not, determine if a router upgrade is available.
- **Use work-issued devices.** While you may prefer to use a personal device when teleworking, if possible, use a work-issued device to minimize security and data leakage risks associated with using an unsecured, personal device.
- **Avoid sharing your work-issued device with others in your household.** Telework can break down the barriers between work and home. Device sharing dramatically increases the risk of unauthorized information sharing.
- **Be security-aware.** Report suspicious emails to your security team and remember that teleworking opens up a new range of social-engineering style attacks. When calling coworkers on personal phones, always verify their identity through known work-issued communications channels.
- **Keep a clean workspace.** Take care to ensure that work-related papers, particularly those relating to confidential, personal, or customer information, be kept out of view of family members.
- **Lock your screen.** When in a shared workspace or family environment, lock your screen when away from your computer.
- **Dispose wisely.** If you have confidential or sensitive information in paper copy, shred it. Do not dispose of sensitive information in your household trash.

Best Practices Checklist for Organizations:

- **Review your software-as-a-service products.** Especially evaluate existing collaboration apps (Skype, Slack, etc.), and plan for increases in utilization.

- **Review onboarding processes.** Review any existing processes for credentialing new or existing users. The rush to enable remote work capabilities for existing personnel can create additional security risks during a crisis.

- **Do not trust personnel home-networks.** Plan your telework security policies and controls on the assumption that external environments contain hostile threats. You cannot rely on personnel to have enterprise level security on their home networks. Treating each teleworker's network as unsecured mitigates ongoing risk.

- **Check your policies.** Review or develop your telework security policies to define telework, remote access, and bring-your-own device requirements. Confirm that your servers are configured in line with these policies.

- **Be cautious about permitting bring-your-own devices.** If your organization permits the use of bring-your-own devices on the organization's network, consider establishing a separate, external, dedicated network for these users in order to mitigate security risk.

- **Remind personnel of incident reporting procedures.** Ensure clear reporting mechanisms for security incidents. Personnel should be informed of the value of reporting incidents as soon as possible. Early discovery mitigates many of the worst consequences of security incidents.

- **Promote a security-aware workforce.** Keep your telework staff informed of common social-engineering attacks and train staff on work-from-home security basics. Teleworkers should be further trained to recognize situations that require involvement from your organization's security teams.

Your personnel and security teams may request additional guidance on the specific controls and recommendations provided in these checklists. Please refer them to the following resources.

- NIST: Bulletin on Remote Work; Guide to Enterprise Telework
- NCSC: Preparing your organization for home working
- CISCO Systems: Understanding Remote Worker Security
- FTC: Online Security when Working from Home

If you have any questions regarding appropriate responses to COVID-19, please do not hesitate to contact any member of the Data Privacy and Protection Group at Shipman & Goodwin LLP.