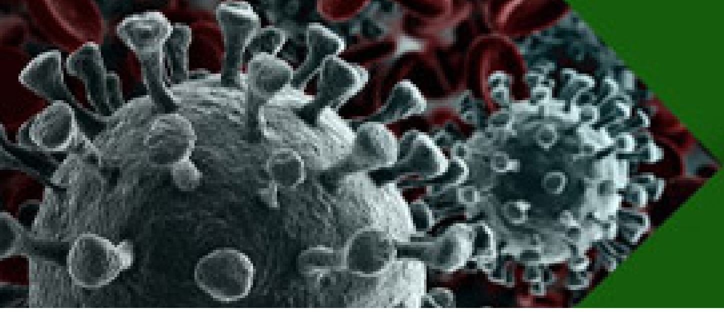

COVID-19 Webinar

Data Protection for the Remote Workforce

Employers shifting to a remote workforce to aid public health efforts must combat new data privacy and cybersecurity threats as they work to maintain employee efficiency. Managing employees located off-site, often using their own technology to connect to company networks via private Wi-Fi networks, takes careful planning and supervision. Whether remote working is new to your company or a regular part of your routine, it is very important to be mindful of confidentiality and security obligations to your clients and personnel while outside the office.

Fox Rothschild has created this helpful, at-a-glance guide to Data Protection for the Remote Workforce as a supplement to its COVID-19 Privacy Concerns and Response Strategies webinar.

Cybersecurity and Privacy Considerations for Remote Working

Remote Access Issues

- The three most likely connection scenarios are:
  - Connecting through company-issued computers, which is very safe if a properly configured, encrypted connection is used (e.g., VPN)
  - Transporting desktop computers to homes, which is generally safe if properly configured, encrypted connection is used (e.g., VPN)
  - Citrix, Remote Desktop, which is very safe if proper restrictions are in place (e.g., cannot download or upload files from the remote computer)
- Multi-factor security for remote working is a must.
  - Licensing issues may need to be addressed in advance.
  - Training may be the biggest challenge for users not previously used to multi-factor security.
  - Mobile and/or home numbers need to be collected in advance for sending multi-factor challenges.
- Unsafe Wi-Fi may be utilized, so users should be reminded to avoid public Wi-Fi options.

Remote System Resiliency

- System adequacy must be tested. It is not acceptable to rely on "in theory" business continuity.
- Unpredictable workload: Constant changes and sudden time zone loads will tax any system.
- Inadequate bandwidth/resources can halt work; the company may need to increase the load the pipe can handle.

Personal Computer Use

- Priority One: Avoid extra copies of data in disparate locations.
  - This requires constant reminders to users, and specific practices that should be avoided as examples.
- Prevent use of personal email and file sharing services, which create extra copies that never get deleted.
  - It is an excellent practice to block access to personal email and file share services while remote working is being utilized, provided those resources are not needed to do a job.

Printing

- Discourage or prohibit printing documents at home.
- Insist that any sensitive documents printed be brought to office for secure disposal.
- Remind users to prevent family members or other "trusted" individuals from reading documents while at home.
- Discourage transportation of files, if necessary, and avoid public transit.
  - Remind users that eyes wander in public and on public transportation.

Heightened Risk of Phishing/Scams

- Employees' guard is down, because of distractions in the home environment.
- COVID-19 scams are rampant, we already are seeing a lot of them.
- Easier to be tricked using mobile devices. You cannot see the true email address like you can on a desktop, you may only see a name unless you purposefully look.

IT Department Concerns

- Skeleton/remote crew likely, which will slow down response time.
- Augmented help desk is a good option but gives new employees on unfamiliar systems access to sensitive data.
- More false positives for Security Information and Event Management (SIEM)
  - o IT Department will be spending time confirming these false positives.
- Patches must be implemented while workers are remote.
- Split tunneling may be inappropriate/prohibited by client data security obligations (e.g., on a secure connection to the work environment, but can also print to a personal computer on the home network).

Data Incidents

- Can happen at the worst times, such as when the company is focused on supporting a remote workforce.
- Executing incident response plans is extremely difficult when working remotely.
- Important to practice (tabletop exercise) a remote workforce event.
- Limited resources will slow things down and not all essential personnel will be available.
- Data coaches and forensic experts may be hampered by own issues.

Governance Considerations

- ESG: Environmental, Social, Governance
- Where do boardroom and leadership fit into response? Will they adapt?
- Many companies will experience working remotely on large scale for first time, which will require calm and effective leadership throughout.
- Will employees return to the office? Many industries are assuming once remote working is proven, employees will demand remote working.
- What is the effect on employee relations? Social interactions matter, and leadership is generally developed and identified from in-person interactions.
- Will leadership adapt?

Mark G. McCreary is Co-Chair of Fox Rothschild's Privacy & Data Security Practice. He can be reached at 215.299.2010 or **mmccreary@foxrothschild.com**.

Fox Rothschild LLP
ATTORNEYS AT LAW