CRI REMOTE WORK RESOURCES

CYBER READINESS INSTITUTE

Making Your Remote Workforce Cyber Ready

Although technology enables people to work remotely, it also opens the door to new cybersecurity and data protection risks.

Now more than ever, every organization needs to have a designated Cyber Readiness Leader – someone who will guide your workforce. To learn more about our free Cyber Readiness Program and the role of the Cyber Leader, please check out our website (www.cyberreadinessinstitute.org).

Here are three key areas for managers to consider in establishing a cyber ready workforce:

- What devices will people use to connect and access information?
- How will they connect to access the information?
- How will they access, manage and protect the information?

Devices

If employees are using a company-issued device from home:

- Remind employees to adhere to your password/ passphrase and software update policies

If employees are using personal devices:

- Have different passwords/passphrases for work and personal use
- Install and run virus-scanning software
- Update all software before connecting to your organization's network
- Turn-on auto-update for all software
- Turn-on multi-factor authentication whenever it is offered

If employees are using shared personal devices (with a spouse, children, etc.):

- Close and quit all applications at the end of each work session
- Log-out, close and quit from databases or web browsers
- Do not write down passwords/passphrases and leave them on or near the computer
- Do not store passwords/passphrases in the device or use auto-login

If employees are using public computers (like a park, libraries, cafes, etc. – if they are open):

- This use should be strongly discouraged and only done if essential
- Quit and re-open any applications that were already open
- Use private browsing on the web browser if possible
- Close and quit all applications, including web browsers, at the end of each work session
- Never save any documents to the public computer
- If you use a USB drive, which is strongly discouraged, never put it in a public computer

guide@cyberreadinessinstitute.org

Connections

If employees are using a personal Wi-Fi connection from their home:

- Change the existing Wi-Fi password/passphrase before starting to work remotely

If employees are using a company-provided or personal hotspot

- Always use the hotspot instead of public Wi-Fi

If employees are using a public Wi-Fi:

- In general, employees should avoid using public Wi-Fi unless your organization has a Virtual Private Network (VPN) that employees know how to use

Access and Data Management

List what systems and data each employee can access in normal operations.

Will there need to be any changes in what they can access when they are working remotely?

Concerning the use of USBs, it is best to ban them and provide cloud-based file-sharing to transfer, share and store data:

- If your organization has a "no USB" policy, remind people of it and stress how important it is to follow the policy while working remotely
- If your organization allows the use of USBs (not a good idea), provide each employee with one that has been scanned for malware. Tell employees they can only use it on the computer they will use to work remotely AND to make sure they have virus-scanning software on the computer BEFORE they insert the USB

Sharing and saving work for remote workers may bring up new challenges.

- If your organization has been using centralized file-sharing (OneDrive, Google Drive, i-Cloud, Box, Drop Box, etc.), employees will be used to managing how they collaborate to work on documents
- If not, you need to establish guidelines for how employees manage and share the documents:
  - Ideally, you should set-up a file-sharing site.
  - In the meantime, have employees send the documents as encrypted email attachments. Many email applications (Outlook, Gmail, Apple Mail, etc.) allow attachments to be encrypted. There are companion programs that provide encryption for emails and attachments (Virtu, Tutanota, VMware Boxer, Symantec Desktop, etc.)
  - Your guidance should cover document naming and some basics of version control. If employees are saving work documents onto a personal device, you need a way to prevent having multiple versions of the same document

We are committed to being a key resource in helping SMEs balance remote work and cybersecurity. Feel free to contact us with questions, comments or success stories (support@cyberreadinessinstitute.org).

About the Cyber Readiness Institute

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). The self-guided, online Cyber Readiness Program is available in Chinese, English, French, Spanish, Portuguese, Arabic, and Japanese.

To find out more, visit www.becyberready.com.