TOOLKIT

WFH Cybersecurity Compliance

Nicsa explores best practice tips for cybersecurity compliance in a work-from-home environment.

It is important to safeguard customer and company information, regardless of where we work. Data breaches can be costly to the customer and the company, and can damage a company's reputation. The following guidance is provided for global asset management industry participants and can be applied to ensure good cybersecurity practices in work-from-home environments.

These are just examples of some helpful tips. Individual member firms may have their own specific policies and procedures associated with these topics.

SECURE YOUR HOME NETWORK

- Check for and apply software updates and patches to routers on a timely basis.
- Change default username and password for the router. Ensure the password is a strong one using an online password strength test. Use a corporate password manager when possible.
- If your router has Wi-Fi capability, confirm the Wi-Fi access password is a strong one and the connection uses a strong encryption method (e.g. WPA2 or WPA3) to prevent your router from being hacked. Check with the router manufacturer's website for instructions on changing the Wi-Fi password or encryption method if it is weak (e.g. WEP or WPA).
- If your router has WPS functionality, turn it off as it may be used to hack your router.
- Update any home anti-virus/anti-malware software.

SECURE YOUR COMPUTER

- Lock the computer if you work in a shared space and plan to be away.
- Store the computer in a secure location when you are finished for the day.
- Do not use company equipment for personal use.
- Don't share your passwords with anyone under any circumstances. Also, don't keep written passwords under the keyboard or anywhere on your workspace. Use a corporate password manager when possible.

SECURE CUSTOMER AND COMPANY INFORMATION

- Do not print at home.
- Use a company VPN when accessing customer or company NPI to add extra security.
- Use email encryption if it is necessary to send confidential information.
- Store documents and files on company approved devices and storage solutions. Check your firm policy on storing documents/files to personal devices, personal email, or individual cloud services.

BE WARY OF FRAUD

- Educate everyone who uses your home network on phishing email red flags so they know what to look for and can avoid downloading malware to the network.
- Be cautious of emails with attachments or links from non-trusted/external sources.
- Verify the sender IP address before opening emails.
- Review the email for red flags before opening any attachments or clicking any links. Red flags include but are not limited to: phony COVID tests and cures, access to personal protective equipment, government assistance, requests for charitable donations, etc.
- Report any suspicious emails to your IT department.
- Consider requiring call backs for some requests in order to double check that you are dealing with the correct people and they have indeed instructed the request.

VIRTUAL MEETINGS

- Know your firm's preferred method of virtual meetings.
- Educate your staff about PII (personally identifiable information} while working from home.
- Password protect your video conferences.

SECURE YOUR INTERNET ROUTER

- Disable remote management features to prevent someone from taking control over the internet.
- Change the admin password for your router. This password allows you to configure settings for your wireless network. The current password may be what your service provider uses for all subscribers, or it could be the default. Neither are secure.
- Change the network Wi-Fi name, also known as the SSID. Use something generic rather than a Family name or similar that would indicate who it belongs to. Extra credit if you can hide the SSID!*
- Enable strong communication security between the router and your wireless device. Select WPA2 for better data protection and network access control.*
- Use a strong Wi-Fi password (different from the router admin password) for access to your home network. You only need to enter it once for each device.*

**NOTE that implementing these steps will require you to reconnect all wireless devices to the network. Contact your service provider for help with accessing your router configuration.*

SECURE YOUR INTERNET-CONNECTED DEVICES

- Update the firmware and software on all devices that connect to your home network. Many of these devices have an auto update option that should be turned on. It is very important that these devices are updated as a vulnerability in any one of them can result in breach of your home network.
- It is particularly important that all personal computers and laptops are on a supported operating system and are set to be automatically updated. A computer with an unsupported operating system (i.e. Windows 7) on your network increases the risk of malware, which can lead to your online credentials and data being compromised.

- Turn off Google Home/Alexa during confidential calls.
- Avoid broadcasting employee computers through smart TV's or other smart devices.
- Activate multi-factor authentications for any internet connected devices.

Observations contained in this work represent the best thoughts of individuals comprising Nicsa committees, and do not necessarily reflect the views of Nicsa or any member organization. Nothing herein is intended to be or should be construed as legal advice. Contact your own counsel in order to obtain legal advice regarding legal or regulatory matters.