IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

Remote Access Considerations: When your employees are working from home

The current Covid-19 pandemic has resulted in new and widespread work from home protocols for all, but a few essential services that cannot operate remotely. Conducting business from remote and dispersed locations represents a significant change in operations for firms and their employees, and introduces challenges to maintaining cybersecurity and ensuring that appropriate data privacy protocols are respected.

This document provides a number of tips and considerations for firms and their employees to assist in keeping firms compliant, and their information safe, during this operationally challenging period.

Advice for your organization

- Ensure your organization has set up secure end-point communication channels so that information, wherever it is created, stored and transmitted, is properly protected. Consider multifactor authentication and encryption of data. Some suggested protocols are presented in an NPC webinar; webinar PowerPoint presentation.
- Engage professionals with specific expertise in end-point security to ensure your remote set-up is done correctly.
- Ensure all your connections are http**s**.
- Check your cyber insurance policy to ensure it covers remote access situations.
- Ensure that all parties to contracts with vendors, that have information security provisions, are not in breach as a result of the current workforce situation. If there are issues, be proactive and reach out to other parties to develop proposals for temporary revised security controls.
- Make sure that you can communicate with all employees, and all employees are familiar with the chosen communication channels.
- Make sure employees have cell phone numbers of other employees they communicate with on a regular basis, as office numbers may not be available.
- Set up call routing of office numbers to employee cell phones, if you can, for employees working remotely.
- Setup a schedule of regular conference calls with employees to keep communication channels open, and offer the ability for employees to voice their issues and concerns. Employees may be reluctant to email issues and concerns, as they may not want to bother others.

- Be aware of the increased threat picture where criminals try to exploit the coronavirus situation. There has been a significant spike in ransomware attempts and phishing links through email and SMS under the guise of coronavirus issues.
- Make sure employees know the remote access processes, and test to ensure that they work (e.g. VPN, multi-factor authentication, etc.).
- Make sure the infrastructure that supports remote access has enough capacity and licenses to cover the increased number of users who need simultaneous access. Many vendors are now negotiating to provide additional temporary licenses for remote access, given the current circumstances.
- Make sure that automatic updating of employees' work computers also works when working from home. If this is not an option, employees should be reminded to update their computers regularly.
- Be aware of the risks associated with vendors granting temporary licenses or permits to access their systems remotely. Ensure they have the same degree of protection, and reassess them when you go back to your usual arrangements.
- When the situation is normal again, remember to gather lessons to improve remote access, processes and contingency plans.

Advice for the employees

- Make sure you have contact information for your IT support staff. This information should be available, even if your computer or other devices cannot be used.
- Ensure you obtain sufficient internet bandwidth to support the programs and processes that you will have to run through your home systems.
- Ensure that home Wi-Fi:
    - Has a strong, long password that has been changed from the default
    - WPA2 level security is enabled
    - The home router is patched and up-to-date
    - The router’s firewall, if present, is enabled
    - Has an obscure SSID, or disable SSID broadcast
- Use the tools and communication channels your workplace provides, and keep in mind that security policies also apply when working from home. For example, be aware of rules for using private mail accounts and file exchange services.
- If your work computer is not kept up-to-date automatically, remember to keep it updated yourself.
- Test that your remote access works so that any problems can be remedied immediately.
- Do not use a non-work related USB stick in your work computer.

- Be aware of any unsolicited emails or SMS you receive under the cover of news about coronavirus and fake offers from service providers, as there has been a significant increase in cyberattacks conducted through these tactics.
- Remember to protect the physical access to your work computer when working from home.
- Be sure to follow company established and announced guidelines for working from home.
- Use the designated secure access to professional systems (VPN, direct connection or other secure services).
- Whenever possible, use the normal central case management system - there is access control, document versioning, backup and general security in place.
- If you have papers containing information about individuals (if your company permits you to take such papers home), be sure to both store and dispose of them safely, as per company policy.
- If there is an urgent need to store documents locally (on your device), make sure that:
    - The device or file containing the document is encrypted.
    - No one else (including the kids ...) has access to the device.
    - You have control over the current version of the file so that data is not lost or incorrect.
    - The file will be uploaded to the case management system as soon as possible - and the local copy immediately deleted.
- Be careful when using cloud, storage or email services, especially when they are free (if your company's firewalls or internet security allows access to such services), because it is possible that such services are free because the provider uses your data for other purposes, such as marketing or selling data to third parties. It is also possible that these services are not properly protected against internet criminals.
- As always, be extra careful with personal data, such as medical data or data on ethnic origin, sexual preference or religion that can be derived.
- Are sensitive documents not on the server, but only on a USB stick or on paper? Then make sure they are placed on your organization's server.
- You can scan paper documents at the office and then put them on the server. If this is not possible, take the data on a USB stick with you, if your company allows the storage of data on a USB stick. Make sure you encrypt the data on the USB stick.
- This applies, for example, to customers' address lists, but especially to sensitive information, like religion, ethnicity or health. You can lose paper files or a USB stick and, in some cases, they may even be stolen.
- Be careful when using (video) chat services.
    - For conversations in which you discuss sensitive data, preferably use available secure means of communication. First of all, the phone.

  - Sometimes organizations have secure options for video calling or chatting. For example, many healthcare organizations use systems that meet the high standards set for healthcare for conversations with patients. Use these, if available.
  - Does your organization not have secure options for video calling or chatting? And, is it really necessary to use these resources? Then consciously deal with any alternatives that are approved by your organization. For example, apps like Facebook Messenger, Skype or Whatsapp. Get approval before downloading to your work computer or other devices.
  - Make sure to discuss as little sensitive data as possible. For example, do not mention names, but use things like agenda numbering or client numbers instead.
  - Whenever possible, inform the person concerned about privacy risks when discussing personal data via a consumer app. Where possible, ask the client with whom you are speaking for permission.
  - Do you use a chat app like Signal or Whatsapp? In any case, delete the chat history after every conversation. And remember to check if the app you are using sends your messages encrypted. Secure your internet connection with a strong password.

- Sanitize your equipment and workspace daily https://store.hp.com/us/en/tech-takes/how-to-clean-laptop-screen