Best Practices for Securely Working Remotely

Presented by John Laffey

PJR Information Security Program Manager

Before We Begin:

- All participants have been muted for call clarity
- The slides from this presentation will be available shortly from www.PJR.com – under "Training," click "Past Webinar Slides"
- A recording of this webinar (and all past webinars) will be available for review on YouTube
  - Search "Perry Johnson Registrars" to view them – free!

PERRY JOHNSON REGISTRARS, INC.

Topics to be covered -

- Advice for employees working remotely
- Advice for Organizations and System Administrators
- Responses to questions asked during presentation

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Separate your work and personal activities.
  - Do not use company furnished equipment for personal activities.
  - Avoid using personal email or cloud storage accounts for work purposes.
  - Force yourself to use personal devices to perform non-work-related tasks.
  - If you must use a personal device to conduct work, consider creating a separate user account that is only used for work activities.

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Be aware of your surroundings
  - Safeguard your work computer and screen from others at your house.
  - Ensure you continue to adhere to company policies regarding who is authorized to view the information you are working with.
  - Adopt a clear screen approach and lock your computer anytime you are not using it.

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Keep software and antivirus up to date
  - Patches are critical for securing discovered vulnerabilities.
  - Ensure you are downloading the latest definitions for your antivirus software.
  - If operating system patches are deployed from a server located at your office, reach out to your IT department to see if you can continue receiving critical patches.

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Be cautious about phishing emails
  - Would be thieves use times of crisis like the current pandemic as an opportunity to compromise systems via phishing attacks.
  - Attacks may come in the form of emails from people you work with who have already been compromised.
  - Emails may seem legitimate given the circumstances of everyone being out of the office and regular workflows being unavailable.
  - Emails may also appear to come from federal or stage agencies urging response in order to receive benefits or critical safety updates.
  - If you receive any email that seems suspicious, especially with instructions to click on links or open attachments, make sure you are reporting them to your IT or security team for their review prior to opening.

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Make you home internet connection as secure as possible
  - If you are using wireless internet at your home, configure it to use the most secure wireless settings available on your hardware.
  - Ensure you are utilizing a strong passphrase for wireless access.
  - If your company has made a VPN connection available to you ensure you are using it.

PERRY JOHNSON REGISTRARS, INC.

Employees Working From Home

- Continue to follow company policies
  - It is just as important to follow security policies when working remotely as it is in the office.
  - Ensure you are familiar with your organizations expectations, specifically regarding remote access, using personal devices for work, and backing up and saving work data.
  - If you are unsure if something your are doing is secure or not, reach out to your system administrators or helpdesk and ask.

PERRY JOHNSON REGISTRARS, INC.

Organizations and System Administrators

- Communicate your expectations and policies
  - It is critical that your employees understand what is expected of them when working outside of the office.
  - This current environment is a great opportunity to provide refresher training content to staff on relevant policies, where they can find them, and who they should ask if they have questions about them.
  - If formal policies are not in place this is a critical time to at least determine some guidelines concerning working remotely and communicating them as soon as possible.
  - Specifically provide guidance on how users should be connecting to company assets, personal device usage, how to safeguard devices used for work purposes, and clear direction on who to contact in case of concerns.

PERRY JOHNSON REGISTRARS, INC.

Organizations and System Administrators

- Highlight security as a priority during this time
  - With many companies being forced to relocate staff to work remotely, it is likely that getting them up and running has taken priority over security concerns.
  - Communicate to staff the importance of maintaining information security while working remotely, as well as identifying methods of contacting appropriate personnel with questions and concerns.
  - Ensure staff know expectations concerning working remotely and provide links to where they can review relevant policies and procedures.
  - Emphasize adherence to policies which are not enforced via technical controls and depend on users working within the documented requirements on their own.

PERRY JOHNSON REGISTRARS, INC.

Organizations and System Administrators

- Provide training content
  - This may be the first time many of your staff are working outside of the office, which can be overwhelming.
  - To ease anxiety provide online training to all users.
  - Include practical advice for assisting them to be able to work remotely, as well as security focused content relevant to the new reality of working from home.
  - Training should include threats your users are likely to encounter working remotely.
  - Most importantly, make sure to clearly direct users on how to ask for help and who to contact with concerns.

PERRY JOHNSON REGISTRARS, INC.

Organizations and System Administrators

- Utilize technical controls wherever possible
  - Utilizing technical controls removes the human element in many situations, reducing opportunity for unsafe usage of assets.
  - Many users do not know when they are potentially compromising information security and having technical safeguards in place can prevent mistakes or ignorance resulting in a costly breach.
  - Requiring multi-factor authentication, encrypted VPN connections, and ensuring endpoints have compliant antivirus in place go a long way to securing remote users and company assets.

PERRY JOHNSON REGISTRARS, INC.

Organizations and System Administrators

- Evaluate new or changed risks
  - A shift to users working remotely can expose your organization to new risks that were not relevant when employees were in the office.
  - Take the time to evaluate the changes that have been made to enable business to continue and the potential risks associated with these changes.
  - Think through the various roles in your organization and the systems they are now accessing remotely.
  - Is additional encryption required? More stringent user authentication?
  - Whatever changes have been made, ensure security is a factor when determining if the change has been completed successfully.

PERRY JOHNSON REGISTRARS, INC.

Thank You for Attending!

Download these slides & view a recording at www.PJR.com.
Feel free to contact John Laffey with questions at jlaffey@pjr.com.

PERRY JOHNSON REGISTRARS, INC.

Questions & Answers

- Contact us for further information at 800-800-7910