Cybersecurity must-dos in the new virtual-workforce era

Rootworks

How modern firms are working hard to ward off hackers and keep client data safe

Seemingly overnight, COVID-19 required firms to operate entirely in a virtual environment. While many firms were cloud-enabled to some degree (set up for limited remote staff, for example), far more firm owners were unprepared for the transition to a fully virtual workforce.

Firm owners rushed to adapt—cobbling together disparate technologies without having a deeper understanding of the security risks. Hackers took notice and very quickly made the accounting profession their core target—zeroing in on security weaknesses.

As such, firm leaders need to ask the question: "Is my data secure in the new virtual-workforce era?" The time is now to start putting IT security measures in place and to educate your staff on core cybersecurity must-dos.

The time is now to put IT security measures in place.

Master machine security

Use authorized machines only

Access to firm applications and client data should only occur using firm-designated machines—including computers, smartphones and tablets. Machines should not be shared with family members in order to minimize the risk of malware infections and hacker access.

Implement automatic system updates

Mandate automatic updating of applications on work devices, and educate staff on how to verify these settings. No one should download non-firm approved applications or disable installed programs unless specifically directed to do so by an authorized IT support person.

Make screen locking mandatory

Access to devices should automatically be blocked via screen-locking capabilities. Firms should designate a standard period of device idle time for screen locking—for example, more than five minutes. This protects against unauthorized user access and enforces confidentiality of client data. Machines should be put to sleep if leaving for an extended period of time, such as for lunch breaks or to run errands.

Access to firm applications and client data should only occur using firm-designated machines—including computers, smartphones and tablets.

Secure all connections

Replace outmoded password guidelines

Mandate the use of multi-factor authentication to access all firm applications. Also consider implementing passphrases and/or a password manager to replace antiquated password rules. Passphrases consist of at least three nonsensical words (e.g., lunchgatelight), are unique for each login, and cannot be reused for other applications. Multi-factor or two-factor authentication requires users to verify their identity by entering a security code that is sent to their phone or email account.

Secure your home internet

Connecting your computer directly to the internet router with an ethernet cable and using a VPN represents the most secure home connection scenario. If you must use a Wi-Fi connection, first update the router's firmware, change the default password, and set up both 'work' and 'guest' access. This limits access to the 'work' account. If this cannot be confidentially secured, use the mobile hot spot on your phone.

Up your game for exchanging files with clients

Adopt client portals or a secure file sharing application to replace highly insecure solutions such as email. This will help further protect client data. All firm staff should be trained on proper use of these tools and be able to assist clients in using them. Some firms offer clients instruction via video or written tutorials on their website.

Consider implementing passphrases and/or a password manager to replace antiquated password rules.

Close the human-error gap

Consistently review your IT policies

Review and update firm IT policies to incorporate the latest remote user and virtual IT security requirements. Review your policies annually to ensure they are current, and take your firm's new technologies and/or move to the cloud into consideration when updating policies.

Offer scheduled security training

Hackers are notorious for using social engineering skills to trick employees into giving them full access to data. As such, be sure to mandate, at a minimum, annual security training for all firm staff—making sure to cover the latest cybersecurity threats. Record these sessions to show new hires and to use as refresher courses for staff who are struggling to meet security guidelines.

Training should incorporate the IRS' Security Six requirements—including an emphasis on evolving phishing and social engineering schemes, and how to respond if you suspect a data breach.

Hackers are notorious for using social engineering skills to trick employees into giving them full access to data.

Shore up IT support

Conduct an independent security review

What is your IT provider doing to keep up with emerging threats and protect your firm in the new remote-workforce era? Best practice is to hire a third-party firm that specializes in security to evaluate your current IT setup and help identify areas in need of improvement.

Maintain verified backups

The best protection against falling victim to ransomware is having offsite backup of all firm applications and data. Many cloud providers and technology vendors provide backup capabilities, but it's critical that your IT provider regularly verify this activity. They should be checking that data is properly backed up and in a format that can be quickly restored.

Minimize privileges

Access privileges should be set to the minimum level an employee needs to perform their work. Firms should limit the number of people who have full administrator rights, as this only opens more doors for hackers to gain full access to your data.

Create a breach response plan

The worst time to figure out how to respond to a security breach is after it happens. Create a response plan now, including naming a champion to execute the plan and the steps the firm will take. This plan should be communicated to all firm staff—detailing actions to be taken should they suspect a breach.

Update your cybersecurity insurance

Even well-protected firms are not immune to being hacked, so it is imperative to take extra precautions. Firms should review and update their cybersecurity insurance, taking into account the elevated number of remote workers.

Implement data and equipment tracking

A data and equipment tracking plan enables firms to pinpoint what data have been compromised in the event of a breach and when devices are lost or stolen. Firms should document all locations where data resides within the firm, in the cloud and on remote workstations. All firm devices should also have tracking tags and be inventoried annually.

The worst time to figure out how to respond to a security breach is after it happens.

Prioritize firm security

Now more than ever, it's imperative that firms take added precautions to ensure the security of client data. Living in the new remote-workforce era, hackers are focused on identifying system vulnerabilities to gain access to your data.

And don't be fooled. Hackers are not employing highly sophisticated methods. Rather, they are using basic phishing emails to trick untrained staff into clicking links that grant them access to your data.

Use this guide as your starting point to help ward off hackers and keep your data safe!

Rootworks is here to help your firm with all areas of operation.

Learn more at rootworks.com

Rootworks
rootworks.com

Source: Right Networks

Right Networks®

Content derived from the AICPA PCPS Digitally Speaking column written by Roman H. Kepczyk, CPA.CITP (April 2019)