Right Networks®

CPA Cybersecurity Checklist

Introduction

The seemingly daily occurrence of major cybersecurity breaches has made many accountants somewhat numb to the security threat posed by hacker criminals. Many people assume it is a "big corporation" problem, but the reality today is that businesses of every size are more vulnerable than ever, and recent headlines point out CPA firms are of particular interest because of the treasure trove of client financial data housed within firm networks.

It is imperative that firm owners realize that they have a fiduciary responsibility to protect this data which clients have entrusted them with and that this information is being directly targeted by hackers for financial gain.

Roman H. Kepczyk, CPA.CITP, CGMA
Director of Firm Technology Strategy

Steps You Can Take

While there is no way to be 100% protected from cybersecurity threats, there are a number of steps that firms can take to significantly minimize the risk of becoming a statistic. Below we list twenty-two cybersecurity best practices that CPAs should take to heart to help protect their firms and client data. We encourage owners to meet with their IT personnel (internal/external) and discuss each point to understand the firm's current status and to determine which steps should be prioritized for remediation of the cybersecurity risk.

- ☐ **Automatic Screen Locking**: Workstations should be set to automatically lock their screens after 5-20 minutes of non-use. This will minimize unauthorized access to the applications and data that are accessible on the computer in the event the user walks away without turning off the computer. Computers should be turned off when not in use and system maintenance performed with the awareness of the workstation's owner.

- ☐ **Enforced Password Policy:** At a minimum, firms should mandate hardened password rules requiring all users to change their passwords four times per year with complex passwords requiring distinct passwords (at least eight characters) or more recently, security consultants are promoting pass phrases (NoHackersOnMyWatch!).   These should be a combination of numbers, letters, and special characters that are unique to each application and not numerically derivative of a previous password (AiCPA!01, AiCPA!02, AiCPA!03, etc.). It is also important to ensure that when any person is terminated that IT is involved to guarantee that the employee's network access and passwords are also terminated.

- ☐ **Enhanced Password Controls:** Firms should implement multi-factor authentication tools such as a physical security fob, biometric scan, or more prevalently, an application that would send a passcode to an employee's mobile device to be entered to validate the person signing in which is known as two factor authentication. To promote even more secure passwords and minimize duplicative password use, tools such as password managers generate a unique, extremely complex password for each application that requires one.

- ☐ **Secure Physical Access:** Physical theft of a file server, workstation, or tablet containing firm and client data can trigger a cybersecurity breach so it is imperative that firms protect these assets, including when they are sent out for repairs. On-premise file servers should be in an unmarked, locked room. Workstations containing data should have encrypted storage disks or better yet run everything on the secured server or in the cloud so there is no local data to be stolen. The office should have an updated alarm system with a unique code for each employee that is disabled when an employee is terminated.

- ❑ **Proper Information Disposition:** Firms should utilize inventory tags to track firm-owned equipment and document acquisitions, assignments, and dispositions including procedures to properly erase and reformat (or destroy) any devices that might contain client data. Also, as the firm transitions any manual documents to digital files, procedures should be verified to properly shred and dispose of all physical documents which may be housed onsite or in offsite storage.

- ❑ **Data Tracking/Access:** The firm must know where all client data resides to be able to secure it. This data map would include not only what is stored on internal servers, workstations and mobile devices but also backup systems, USB/storage drives, and cloud applications. Access to each of these systems should be limited to only those users that absolutely need it.

- ❑ **Limit Mobile Access:** The firm should only allow trusted, validated users and equipment to connect to the firm's IT resources. Mobile Device Management application require each workstation, tablet and smartphone to be individually registered to connect to the firm's network which minimizes the risk of unauthorized equipment connecting. Firm personnel should also be reminded of the importance of keeping their mobile device's operating system and security applications updated.

- ❑ **Updated Operating Systems:** One of the most successful ways that hackers compromise network systems is through known vulnerabilities to operating systems that the firm has not yet loaded system updates to block that vulnerability. The best way to minimize this avenue of attack is to set workstations to automatically update the operating system and key workstation applications. Turning off computers at night and rebooting promulgates these updates and also clears out system clutter making the workstation more efficient.

- ❑ **Minimize Administrative Privileges:** Hackers that obtain administrative access privileges to networks and workstations have significantly more power to take control of network resources. IT personnel should minimize allowing users to have administrator privileges and set access levels to the minimum level required by each user to complete their work.

- ❑ **Current Network Operating Systems:** Operating systems for all equipment comprising the network (file servers, firewalls, routers, Internet of Things [IoT] peripherals) should be reviewed regularly to make sure they are running the most current system updates. It is also critically important to change the default passwords on all devices connected to the firm/home network; which not only encompasses wireless printers but the IoT devices including security cameras, connected home appliances, and voice activated devices.

- ❑ **Antivirus/Malware Applications:** Each fileserver, workstation, and mobile device should have antivirus/security software installed that is being automatically updated and actively scanning for malware on a pre-set schedule. These applications have expanded capabilities to include intrusion detection and prevention in addition to Spam Management that will blacklist known threats and allow the firm to whitelist valid sites. If a client provides physical media such as a USB flash drive, each workstation should be set to automatically scan external media before loading files. Better yet don't allow the use of any flash drives and educate clients on the use of digital portals and secure email.

- ❑ **Protected Backups:** Data backups not only protect the firm from lost/corrupted data but are critical if the firm is the target of a ransomware attempt. Shadow copies of all changed files should be made throughout the day so the most recent versions can be restored. The IT team should regularly review backup logs to verify that data backups are complete, and randomly restore files to verify the data is accessible. All backup data should be encrypted, including that which is going offsite via the Internet.

- ❑ **Secure Client Transmission:** All firm personnel should be trained on utilizing encrypted email and/or portal solutions for the secure transmission of files to and from clients. This training should include proactive training of clients to use the firm's system to foster adoption and minimize data being exposed.

- ❑ **Secure Staff Connection:** All staff should be trained to verify secure connections to websites (green padlock image and https: in the web address bar) or to utilize a Virtual Private Network (VPN) connection when working outside the office and accessing the Internet and/or firm resources. When working remotely, personnel should also verify the SSID/password for any client-provided WiFi access or utilize a secure digital cellular mobile hotspot rather than public WiFi such as hotels, coffee shops or airports which can be stealthily compromised.

- ❑ **Review IT Policies:** Technology is evolving rapidly and few firms have updated their IT/HR policies to reflect current changes including the security ramifications of BYOD (Bring Your Own Device), social media, and the remote workplace. Firms should review policies annually and remind users of changes along with updated Internet and computer usage policies.

- ❑ **Security Education:** Proactive and ongoing security training to protect client data should be part of the firm's annual CPE curriculum. In addition to providing an annual update on IT policies, all personnel should be educated on current threats including ransomware, phishing, SMiShing (SMS phishing), vishing (voice mail phishing) and other social engineering examples designed to make employees download malware that compromises the firm's security or inadvertently give out sensitive information. Employees should be reminded to be suspicious of unsolicited support calls and never provide login, password or to download a file without first confirming the identity of the caller.

- ❑ **Phishing Awareness:** Employees need to be regularly reminded of current phishing schemes and to be trained on what to do if they receive a suspicious email. This would include hovering over the sender's email address in the header or any hyperlinks to verify properties and to ensure they match, or typing in website address directly into a browser. Staff should also be reminded to not click on a link or open an attachment within an email if the email is unexpected and suspicious. If the user has any concerns, there should be a process to have a member of the IT team be notified to review the email or to contact the sender to verify intent. There are a number of services that provide ongoing phishing/security training and testing of employee's response to phishing emails which seem to peak in accounting firms around tax deadlines and holidays.

- ❑ **Screen Potential Employees and Contractors:** A surprising percentage of breaches occur with the help of internal personnel so it is important to conduct background checks on anyone being given access to the firm network. IT needs to be involved to not only provide the minimum level of access to do the work, but to monitor access and terminate it when the project is completed.

- ❑ **Greet Office Visitors:** Personnel should be trained to ask unrecognized visitors roaming alone in the office if they can provide assistance and then escort them to the person they say they are meeting with. If there are any concerns about the validity of the visitor's response, a member of the management or administrative team should be notified immediately.

- ❑ **Hire Cybersecurity Expertise:** If the firm's internal IT personnel do not provide ongoing Security support for clients, it is not likely that they will be able to provide an optimum level of cybersecurity expertise internally to protect the firm. Internal IT personnel should partner with external security-focused integrators to review the firm's network security and provide direction and implementation assistance on securing the firm including intrusion detection, prevention and ongoing system monitoring.

- ❑ **Breach Response Plan:** The worst time to develop a cybersecurity incident response plan is after the firm finds out it has been hacked. The IT team should document the process and educate employees on what they are to do if they suspect a breach. This training should also include the steps the IT team will take to verify and mitigate the breach including identifying external resources and meeting insurance requirements.

- ❑ **Cybersecurity Insurance:** The reality today is that even the best protected firms are not immune to innovative new hacker threats, so it is important that the firm also review their insurance policies to understand to what extent they are covered for lost productivity resulting from a cybersecurity breach. Firms should also include coverage for damages caused to any clients who's data may have been compromised and become victims of identity theft because of the breach.

Summary

While most compromised organizations envision super-sophisticated hackers using complex technical expertise to breach their system, the actual breach findings have shown that hackers most often utilize common phishing techniques, known system vulnerabilities, and social engineering approaches to get access to confidential data. In the majority of cases, firms that address and deploy the solutions above make it difficult enough that the hackers move on to easier targets. Protecting client data, and by extension the firm, is everyone's responsibility but it's up to owners to make it a priority and ensure it is taken seriously.

Roman H. Kepczyk, CPA.CITP, CGMA, LSS BB is the Director of Firm Technology Strategy for Right Networks and works exclusively with CPA firms to implement today's leading best practices and technologies incorporating Lean Six Sigma methodologies to optimize firm production workflows. Roman is also the author of the 2019 Edition of "Quantum of Paperless: A Partner's Guide to Accounting Firm Optimization" which is available for download to members of the AICPA PCPS section.

To learn more about how Right Networks can help you protect client data and your firm, contact Sales at **1-888-210-0237**