uprite SERVICES

The CPA cybersecurity checklist:

What firms must do to protect their data

The CPA cybersecurity checklist: What firms must do to protect their data

Introduction

The constant onslaught of ransomware and cybersecurity breach headlines has made many CPAs numb to these threats. Most have relegated the responsibility of protecting the firm to their internal IT personnel or to an external IT provider with the assumption that it's "being handled."

The reality today is that many firms' internal IT personnel haven't had adequate cybersecurity training or access to resources. What's more, external solutions providers may not be aware of the unique data requirements and client situations accounting firms face. Many are not aware that they're required to have a written information security plan. While no individual or firm can be 100% protected from cybercriminals, implementing and documenting the following items in a written format will go a long way towards protecting the firm.

01 Automatic screen locking

Workstations should be set to automatically lock their screens after being idle for 5-10 minutes. This will minimize unauthorized access to applications and data that are accessible on the computer in the event the user walks away without shutting down. While putting a computer to sleep or virtually locking the screen is adequate during the day, computers should be shut down at night and restarted the next day to ensure updates occur.

02 Enforced password policy

Traditional eight-character "complex" passwords are no longer adequate. Passwords should have at least twelve characters with each password being unique (not reused on other sites). The use of passphrases (three or four random words connected) and password wallets can help personnel adhere to this policy. Any time an employee is terminated from the firm, it's important to have IT personnel also terminate access to the firm's network and data resources.

03 Multi-factor authentication (MFA)

Firms should implement multi-factor authentication tools such as a physical security fob, biometric scan, or more to the point, an application sends a passcode or confirmation to a mobile device to verify the person that is attempting to sign in. MFA is critical to firm security.

04 Secure physical access

The physical theft of a file server, workstation or tablet containing firm and client data can trigger a cybersecurity breach. Therefore, it's imperative that firms protect these assets—including when those devices are sent out for repairs. Onsite file servers should be in an unmarked, locked room. Any workstations containing data should have encrypted storage disks, or better yet, run everything on the secured server or in the cloud so there's no local data to be compromised. Office alarm systems should be capable of creating a unique code for each employee or contractor accessing the office, which can be disabled when access is terminated.

05 Proper data asset disposition

Firms should utilize inventory tags to track equipment and document acquisitions, assignments and dispositions—including procedures to properly dispose of 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 that may be housed onsite or in offsite storage.

06 Data Mapping Access

The firm must know where all client data resides in order to secure and prioritize it for restoration in the event of a system outage. Creating a data map would include not only what is stored on internal servers, workstations and mobile devices but also backup/storage systems and cloud providers. Access to each of these systems should only be allowed to those users who need it, which will minimize the risk of unauthorized access.

07 Protected remote access

Only trusted, validated users and equipment should be allowed to connect to the firm's IT infrastructure and cloud services. Firms should mandate the use of a Virtual Private Network (VPN) and Mobile Device Management applications, which require each workstation, tablet and smartphone to be registered to connect to the firm's network. Firm personnel should also be reminded of the importance of keeping their mobile devices' operating systems and security applications current with automatic updates.

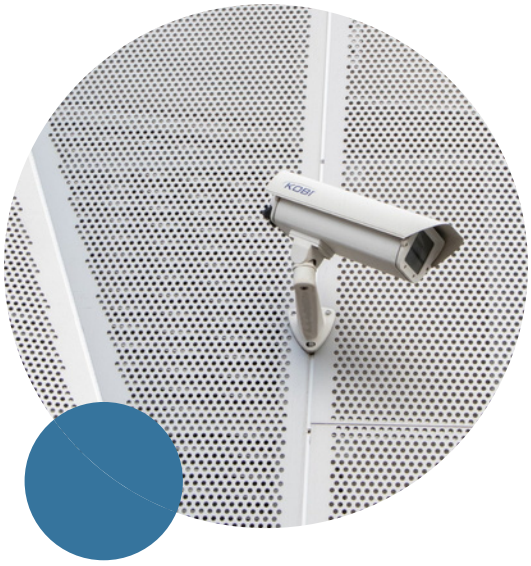
08 Updated operating systems

One of the most successful ways that hackers compromise network systems is through identified vulnerabilities to the operating system, which the firm has not yet updated. The best way to minimize this avenue of attack is to set all digital devices to automatically update the operating system and key workstation applications. Turning off computers at night and rebooting puts these updates into effect and also clears out system clutter, making the workstation more efficient.

09 Minimize administrative privileges

Hackers who obtain administrative access privileges to networks and workstations have significantly more power to take control of network resources. IT personnel should minimize the number of users who have administrator privileges and set access levels to the minimum level required by each user to complete their work.

10 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're running the most current system updates. It's also critically important to update the firmware and change the default passwords on all devices connected to the firm and home networks. This not only encompasses wireless printers but also IoT devices including security cameras, connected home appliances and voice-activated devices.

uprite SERVICES

11 Antivirus/malware applications

Each fileserver, workstation and mobile device should have antivirus/security software installed that's 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 blocking known threats. Firms should disallow the use of any flash drives and instead educate clients on the use of digital portals and secure email.

12 Protected backups

Data backups not only protect the firm from lost/corrupted data but are critical in the recovery of a ransomware attempt. Shadow copies of all changed files should be made throughout the day and then stored separately offsite. The firm's IT team should regularly review backup logs to verify that data backups are complete and randomly restore files to verify that data is accessible. All backup data should be encrypted—including that which is going offsite via the internet or physical storage media.

13 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 applications.

14 Secure staff connection

All staff should be trained to verify secure connections to websites, which are often signified with a green padlock image and https: in the web address bar. When working remotely, personnel should utilize a Virtual Private Network (VPN) connection and verify the SSID/password for any client-provided Wi-Fi access point (or preferably utilize a secure digital cellular mobile hotspot).

uprite SERVICES

15 Screen employees and contractors

A surprising percentage of breaches occur with the help of insider personnel, so it's important to conduct background checks on anyone being given access to the firm's office, workstations and computer network. IT needs to be involved in providing users with the minimum level of access needed to do their work and also to monitor access and terminate it when access is no longer required.

16 Greet office visitors

Personnel should be trained to ask unrecognized visitors if they can provide assistance and then escort them to the right person. 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.

17 Hire cybersecurity expertise

If the firm's internal IT personnel do not provide ongoing security support for clients, it's not likely that they'lll be able to provide an optimum level of cybersecurity expertise 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, including intrusion detection, prevention and ongoing system monitoring.

18 Breach response plan

The worst time to develop a cybersecurity incident response plan is after the firm has been compromised. Firm leadership and IT personnel should document the process in writing as part of the firm's information security plan, including educating employees on what 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, which includes listing external resources and meeting insurance requirements.

uprite SERVICES

19 Update IT policies

Firms should review IT policies annually and formally remind users of those changes along with updated internet and computer usage policies.

20 Security education

Proactive and ongoing security training to protect client data should be part of the firm's annual learning curriculum. In addition to providing an annual update on IT policies, all personnel should be educated on current threats like ransomware, phishing, SMiShing (SMS phishing), vishing (voice mail phishing) and other social engineering examples designed to trick employees into downloading malware or inadvertently offering sensitive information. Employees should also be reminded to be careful handling unsolicited support calls and never provide login, password or financial information as well as to never download a file without first confirming the identity of the caller.

21 Phishing training

Phishing schemes have become increasingly sophisticated. "Spear" phishing emails are addressed to a specific recipient and are often from a known colleague whose email has been spoofed or compromised. Employees should be updated regularly on current phishing schemes, reminded of red flags that should invite additional scrutiny, and educated on what to do if they receive a suspicious email or phone call. There are services that provide ongoing phishing/security training and testing of employees' response to phishing emails.

22 Cybersecurity insurance

The reality today is that even the best protected firms are not immune to constantly evolving cybersecurity threats, so it's important that firms also review insurance policies to understand what's covered for a ransomware event and the lost productivity resulting from a cybersecurity breach. Firms should also include coverage for damages caused to any clients whose data may have been compromised and who have subsequently become victims of identity theft because of the breach.

uprite SERVICES

Conclusion

While most compromised organizations envision supersophisticated hackers using complex technical expertise to breach their systems, actual findings have shown that the majority are rooted in human error such as inadvertently clicking an email attachment, accidentally providing compromising information or neglecting to update software in a timely manner. Having a written, structured process to proactively manage cybersecurity will go a long way to protecting the firm. And discussing and remediating the items on this checklist with your IT team will help make it more comprehensive.