CPA
Practice Advisor

threats, it's important to consider where your payroll information is being stored. Is it on a laptop, the Cloud, hosted on a server? Each comes with its own set of risks ...

Taija Sparkman • Nov. 09, 2015

November is National Security Month and there will be a lot of focus on making sure data of all kinds is secure. Your clients rely on you to keep their payroll data safe and secure all year-long, not just during the month of November. Therefore, it's

important to ensure that your firm's software and technology employs the proper

numbers, becomes compromised.

Regularly assess your firm's systems and processes for any potential risks. Develop a plan to safeguard against potential cyber threats and communicate that plan to your firm and clients. If your data is hosted on a server or in the Cloud, familiarize yourself with the providers' security systems and software. You should choose a provider that is dedicated to protecting your clients' payroll data and regularly updates and maintain their servers or software. Just because your data is stored in the Cloud doesn't mean it's automatically safe. Software such as RUN by ADP provides a secure Cloud environment and maintains a very stringent data security policy.

As a payroll practitioner, you are accountable for the security of your clients' data. They are entrusting you to manage their payroll and keep their employees' confidential data safe, so be aware of who has access to the servers your data is housed on and how often they are maintained. Additionally, have a process in place to determine who handles which data in case a glitch or issue arise. Actively log and monitor all network access and activity. Maintaining up-to-date logs will make it easier to pinpoint any unusual behavior earlier, if necessary. A process should also be in place to revoke access from all systems whenever necessary to prevent former employees from accessing and abusing sensitive client data.

Routinely update your virus and malware software and anytime a new threat occurs. Everyone in your firm should be required to routinely change their passwords and create strong passwords that are hard to hack. Many firms allow their professionals to access company data on personal devices. If this is the case for your firm, there needs to be a process in place to manage the access. Consider how data can be wiped from a device in the event of an employee's departure or lost device.

There should be a strong firewall in place to prevent any outside access to client data. If someone is able to breach your firewall, then your clients' data is at risk. As part of

that firewall, you want to regularly consult with anyone that may have access to

restore it at anytime if you need to. If you use a Cloud service provider, make sure backup and recovery services are not only included in your service agreement, but you are aware of the backup schedule. This should be done on a regularly basis to avoid the impact of data loss.

Your staff needs to be well-trained on the measures your firm is taking to protect client payroll data. Conduct regular employee training on data security to ensure everyone is aware of the threats facing that data and how to protect against them. As you consult with your clients, make sure they are doing their part, too, to aide in the protection of their payroll data.

Keeping your clients' payroll data safe can be a daunting task, especially if maintaining the proper technology and protocols interferes with providing quality payroll services. If necessary, appoint a Chief Information Officer or consider outsourcing the role to provide quality protection. Just as your clients hire you to expertly manage their payroll because they are not payroll professionals, it's okay to hire an IT expert to make sure you're keeping clients' data secure. Whether it's an internal or external role, someone should be solely responsible for ensuring employees are properly trained, data is securely backed up and anti-virus and anti-malware software is kept up-to-date.

Payroll • Security • Technology

Sponsors.