survey by Gallup reports that the average worker telecommutes two days per month, with 46% of telecommuters doing so during the workday.

Dec. 07, 2016

Many Americans now have the flexibility to work remotely, and more want to do it. A survey by Gallup reports that the average worker telecommutes two days per month, with 46% of telecommuters doing so during the workday.

However, accountants deal with highly sensitive client data. Security can be compromised if a mobile device or a wifi network isn't secure. "As an employee, I'd also be concerned about my home computer being available for legal discovery and

everything on it open for review," said Bill Thompson, president of CPA Mutual, a

past practice may no longer satisfy federal law.

Due to U.S. Department of Labor scrutiny of employee classes and overtime, firms need to carefully monitor timekeeping for non-exempt seasonal workers. This is particularly true when they are handling any work out of the office. Non-exempt employees must be paid overtime, and compensatory time off can't be given in lieu of overtime pay.

Also, make sure to correctly categorize seasonal workers as either employees or independent contractors. According to the DOL, employees are considered to be employees and not independent contractors if they look like employees – they regularly work in the firm's office, have firm email addresses, use firm resources, have firm business cards and/or titles, and take direction from firm personnel.

Reduce Human Error

Employee error is much more likely to cause a mishap than technology failures, according to the Association of Corporate Counsel. Keep the following in mind when it comes to your data:

- **Use a secure data portal to gather client information.** Limit access to necessary personnel only and provide client-specific passwords and links.
- **BYODP – bring your own device protection.** If your firm allows employees to use their own devices for work – a laptop, tablet, smartphone – ensure that the device is secure with updated firewalls and anti-virus software.
- **Review and enforce data security policies.** Hackers often target "back-door" access points to gain entry to company servers. They include the wifi at your favorite café and the apps you use. Once they get into the mobile device, hackers can access sensitive emails and any open portals from that device. Employees should log off of portals and servers and change passwords frequently. Keep

devices locked when not in use. At a minimum, employees should only log-on

prepared with questions about security and their contractual liability if your system is breached due to solution error or their personnel. Ideally, the vendor will carry some liability coverage for incidences involving a breach of client data security.

- **Limit access.** Who has the most need for the data? Often, access to sensitive financial, HR or client information is broader than it needs to be.
- **Exiting employees.** Have a process for shutting down access by former employees that extends to all programs, apps and devices as soon as possible. If former employees used a company-owned mobile device or smart phone, make sure the device is turned in or, if it isn't, can be wiped remotely as a fail-safe option.

"Allowing your firm the flexibility and added benefit of remote work can be good for retention and recruitment as well as productivity," Thompson added. "Consider all your firm's options to protect client data in this new environment, whether it's employee training, secure cloud technology or supplemental liability coverage. Because rules may vary from state to state, it may be a good idea to consult with a local experienced attorney in your area."

———————

Bill Thompson, CPA, RPLU, helps CPAs navigate the minefield of professional liability issues with practical risk management. Bill is also responsible for underwriting, reinsurance negotiations and placement, coverage and policy issues as President of CPA Mutual. Visit www.cpamutual.com to learn more.

Firm Management • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy