Five Data Security Tips for Accounting Firms

Wade Yeaman

***

From working hand-in-hand with our tax practitioner clients, accounting services, and bookkeeping clients over the years, I know a thing or two about data security and how best to protect your firm from data losses or data breaches. In today's world, accounting firms and tax practitioners must do everything they can to protect their client's sensitive financial information. I've pulled together a few best practices for you to keep in mind.

1: Assess your current data protection and security levels

If you never measure your security performance, you never know if your network and data are secure or not. That is, until you learn from a breach or malicious virus that you had poor security after all. We recommend an outside firm provide an annual security assessment and review. You may not have the time or budget to implement all suggestions, but at least you will know your weaknesses and you can develop a plan to improve over time.

2: Physical security, Information Systems Policies

Your network can be bullet proof to hackers and your data encrypted, but if your team isn't trained or your office isn't physically secure, your data is still at risk.

- Ensure the physical security of your office with card keys, visitor logs and badges, and proper locks on doors leading to all critical infrastructure.
- Use cable locks to ensure laptops, desktops, tablets, and any other critical devices are locked to desks.
- Policies for each employee
    - Clean desk (no sensitive information left on desks, whiteboards or print stations)
    - Password policies that define the proper construction and maintenance of passwords
    - Acceptable use for utilizing company data and technical assets
    - Mobile device policies to help employees understand the risks associated with mobile devices
- Keep users informed and accountable
    - Training classes are great vehicle for delivering written policies and procedures
    - Weekly (or even monthly) information security newsletters can help remind users of the importance of information security, as well as provide updates on the latest trends and threats.

3: Secure technology solutions

This is the sweet spot. We feel you need to start from the outside and work toward each user device to implement proper security.

Continued on the following page

- Are your cloud vendors Payment Card Industry (PCI) compliant? It's a great standard that can generally be trusted.
- Follow best practices when setting up office infrastructure
    - Place a business grade firewall at the front of the network that is supported and continually updated
    - Ensure WiFi networks use strong passwords and encryption protocols. Keep guest networks separate from internal networks.
    - A business-grade Anti-virus solution for all PCs
    - Standard email defense software

Do you know what compliance regulations your business or your customer's business requires you to have?

4: Automated backup and disaster recovery

What if you are hacked or a malicious virus infects your system? If major financial institutions or fortune 500 companies have some vulnerability, you probably will to (even if you follow some of these tips).

Can you recreate lost data or data held hostage by a malicious virus? Do you conduct a periodic test of your data backups to confirm their validity? Do you have multiple layers of backup – local, onsite, or offsite?

A good, up-to-date backup or disaster recovery solution can be your "get out of jail (almost) free" card if you run into a problem.

5: Address your Bring Your Own Device (BYOD) policy and its security implications

The use of personal devices on a company network to handle client data is always one of your largest security concerns. If you allow company data on personal devices, there are some steps you can take to limit the security vulnerabilities this may cause. Here are a couple of ideas:

- Have a policy in place that states when it is acceptable to use personal devices for work purposes. If it is acceptable, provide guidelines to help employees understand the risks of using personal devices for business purposes.
- Have a mobile device management (MDM) solution deployed to help manage all company data on personal devices.

The cost of proper security, if done proactively, will generally be much cheaper than the cost of a data breach or work stoppage from an IT problem. Your firm can work on some of the solutions on your own, but be sure to reach out to security specialists if you get stuck.

About the Author:

Wade Yeaman, with more than 20 years of experience in business and information technology, Wade founded Fluid IT Services because he passionately believes that small and medium businesses deserve the same technology support services that big companies enjoy. He attended Texas Tech University. When Wade isn't working with his favorite people (that would be Fluid staff and clients), he can be found fly-fishing or playing his guitar.