Six Ways to Protect Your Firm From a Data Breach

By Tom Parker

As you go about your day conducting business online, hackers are in the wings, waiting to pounce and exploit one innocent miss-click, mistake or mismanagement of company data and files. Since you are your clients' trusted advisor, you are responsible for protecting valuable information, from credit card and bank account numbers, to client names, Social Security numbers, tax IDs and anything else that can personally identify an individual. Standing pat, turning a blind eye or being in denial of the realities of cybercrime and data breaches will destroy lives.

If you don't believe me, here are some statistics that should wake you up. The Identity Theft Resource Center estimates there was an average of 15 data breaches a week in 2014, and according to *USA Today*, 43 percent of U.S. companies had a data breach in the past year. Moreover, cybercrime cost the global economy $575 billion and the U.S. economy $100 billion annually, making it the largest hit to any country, according to a report from Intel and the Security and the Center for Strategic and International Studies.

It wasn't always this way. Before the Internet became mainstream in the mid '90s, hackers were isolated. They were probably more successful picking your pocket or even rummaging through your trash than finding anything of value online. Today, it's a different story—even the most unsophisticated hacker can create real problems for an organization. All the hacker has to do is copy a more-seasoned hacker's code from the Internet and run it. It's very scary, but it is the reality in which we live. Think of it as a chess game where you must protect your queen from being captured. In your firm, you must work toward protecting your organization from cybercrime, without fail.

To keep your valuable information from being captured, following are six ways to protect your firm from a data breach.

1. Create Security Awareness

You must first have the mindset that your system isn't something that just processes information, but rather something that "lives" and needs to be protected. Build a culture of accountability with your staff and in your firm. It is *everyone's* responsibility to think about security, and it's time to make this *personal* by reminding the staff about their own privacy. After all, would you want your own Social Security number, bank accounts or any other data to be breached? If it can happen to you, it can easily happen to your clients.

Email is a huge problem. Just one innocent-looking email to a co-worker can trigger the breach, if sensitive information is transmitted. Phishing, too, is getting more sophisticated – an email that looks like it's valid from your bank could cause great harm. A rule of thumb is that no one should ever ask for your password in an email, so clicking a link inside your email is one of the most popular ways a system gets infected. An easy way to tell if the email is a phishing expedition is to hover over or right click the "from" address. Look at the domain – if it's anything that seems suspicious, it probably is.

However, just like your accounting advice, you must take a comprehensive approach with your clients when it comes to data breaches, educating them about email in terms of receiving messages and automatically opening them. For example, tell them about phishing and what you're doing within the firm to protect their information. Not only may this conversation save them from having their data hacked, the fact that you are having the discussion also goes a long way to maintaining the trust and loyalty they have in you as their financial advisor.

2. Maintain Simple System Hygiene

Protecting your firm from a data breach isn't difficult, but it does require constant attention, something I like to refer to as "simple system hygiene."

At the very least, you want to update your security on a regular basis. This comes down to patching your systems and usually involves more than Microsoft Windows or Mac system updates, such as Java, for example. Anti-virus software helps, too, but you can't always rely on standardized programs, such as McAfee or Norton, to protect you. All software providers provide security updates, so if you aren't getting these or are unaware of where to get the updates, you should contact your provider right away.

3. Establish Policies and Procedures

In my experience, firms and organizations that have clear, written systems' policies and procedures are far less vulnerable to data breaches than those that don't. Creating these policies is good for several reasons. First, it gives your staff a roadmap to follow and takes away any guesswork on their part as to what they can, for example, download from the Internet. Second, it helps protect your clients' personal information, because you've implemented best practices in your organization. Third, you can tell your clients about your proactive stance in mitigating any potential risk. That establishes a great deal of trust between you and your clients.

Your policies and procedures should be a working document, constantly updated as needed, and if your firm is large enough, you may have an IT professional on staff who can take it on. Regardless, you can think of these policies and procedures as the repository for a security awareness program. The main function of the program is to make all of the staff aware of what they need to do to protect the firm's sensitive information. As basic as it sounds, include, for example, procedures on password length and how often a password ought to be changed. It is good, basic hygiene to change your passwords every 90 days.

Speaking of passwords, I know you've seen this time and time again in your firm and probably at home – yellow sticky notes stuck to the monitors with passwords. You may think your co-workers aren't paying attention to the notes, let alone the cleaning crew who comes in at night. Losing control of your passwords can easily lead to lots of problems and you do not want to be the one responsible for the breach.

Thanks to advanced technologies, there are quite a few password programs on the market that can be had for a firm or company at a very reasonable cost. These cloud-based programs will create secure passwords and store them for you. Search for a program that makes sense for your firm and/or ask your colleagues in other firms or companies for their recommendations.

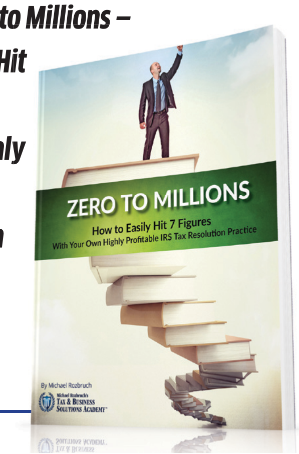
4. Establish Access Controls

As a firm grows, you must implement access controls, and while you might think that a sole proprietor doesn't need to worry about access, you're greatly mistaken. Even the presence of one more staff person – administrative or otherwise – could create an opportunity for a data breach.

Access controls focus on "who" gets access to "what" information. Think of this in terms of your finances. Your admin may prepare the checks for you to sign, but he/she shouldn't also have signing authority. Similarly, you want to ensure you aren't giving access to everything in your firm to everyone in your firm. Instead, give employees access only to what they need access to, and if you get pushback, you may have a larger problem.

Access controls are also referred to as role-based security, granting access designed for each employee's specific role. A good place to write down your role-based security procedures and processes is in the document you created when you looked at simple system hygiene.

continued on page 17


ZERO TO MILLIONS
How to Easily Hit 7 Figures
With Your Own Highly Profitable IRS Tax Resolution Practice
By Michael Rozbruch
Michael Rozbruch's Tax & Business Solutions Academy

continued from page 15

5. Conduct Regular Risk Assessments

Risk assessments should be conducted at least once a year. It's important to pick a vendor to do this that isn't just running tools against your network. The vendor needs to look at your firm holistically and understand that you need a mobile, secure workforce. This is vital since your CPAs and staff are out in the field talking to clients and working from their locations. The end game here is to take a risk-based approach to your systems and processes instead of just thinking of them as stand-alone components that do not integrate with the rest of your organization.

There are lots of control frameworks out there, including the ISO 27,000 Standards and the Committee on Sponsoring Organizations (COSO) framework. Do a search for resource materials on these frameworks.

6. Don't Forget About Physical Security

The last piece to discuss is physical security. Protecting your firm from a data breach isn't just about systems and processes, but also about leaving that data exposed outside of an electronic system. I touched on this earlier when talking about passwords, but physical security goes much further than sticky notes.

While many firms have tried to go paperless with cloud-based storage, the old four-drawer metal file cabinets hanging around in your storeroom are totally exposed. Take an inventory of exactly where you are vulnerable and begin to create practical policies around physical security. No one is saying to completely ditch the file cabinets, but you could do something as simple as locking the cabinets or storing your files in a secure location offsite.

Secure Everything

Security is no longer just about guards, cameras and blindly hoping your wires don't get crossed. You must pay attention, do your research and seek help from professionals. A data breach can make or break your life's work, so you must take action and do everything you can to protect yourself and your clients. This issue is bigger than just you and your day-to-day activities.

Tom Parker is chief information officer for Avalara. Prior to joining Avalara, Parker was director of application security at Microsoft, accountable for the overall risk management of its IT application portfolio. He also served as strategic security advisor and helped shape Microsoft's enterprise application platform business architecture. In addition, Parker was a managing consultant for Shavilk Technologies, a senior security engineer and division manager for the National Security Agency, and has held several leadership roles in the United States Navy. Contact him at tom.parker@avalara.com.