CPA
Practice Advisor

not likely to be terminated by our clients or our firm, even this type of loss ...

Randy Johnston • Oct. 12, 2014

Risk mitigation when your practice is attacked is an economic consideration. What will breach reporting cost? What will recovery cost and time lost be? Although we are not likely to be terminated by our clients or our firm, even this type of loss is possible. What can we do to minimize the possibility of identity theft, malware, viruses, and attack from attackers? By the way, whether you run a private cloud or use public cloud facilities, you have a risk of attack and theft. As you might surmise, the public cloud data centers have more sophisticated tools to watch for attacks, but their tools are marginally better at preventing attacks in the first place than properly maintained in-house IT equipment.

Attacks come from a number of sources: PDF files, email links, direct attacks from

becoming desensitized to the risk and impact of a theft. With massive identity thefts like those reported in August 2014 of the Russian hackers accumulating 1.2 billion stolen user names and passwords and a half a billion email addresses garnered from 420,000 sites, it is hard for us to imagine the size and scale of the theft. Many of you probably have trouble recalling the October 2013 report of 153 million credentials being stolen from Adobe. These large scale thefts remind us of the importance of routinely changing our passwords and maintaining these credentials with some sort of password management tool.

Consider the Solutions

There are a number of strategies that must be followed by public cloud providers or on your own in-house network and private cloud. Even though it is our belief that all firewalls and anti-virus products are becoming less effective as the hacker's tools become more sophisticated, you should be following current best practices for security to establish that your firm is making reasonable efforts to protect client data. The responsibility of protecting client data can't be transferred to another entity who is doing your hosting or your IT work.

Minimum protection today includes:

1. **Firewall with intrusion protection services** – options include Cisco, SonicWall, WatchGuard and others.
2. **Anti-virus that is updated regularly** – options include GFI Vipre, eSet, McAfee and others.
3. **Password managers** – options include Citrix Password manager, LastPass, RoboForms, Password Depot and others.
4. **Encryption of all drives and removable media** – options include Microsoft Bitlocker, PGP and the built-in encryption in the Mac OS, which unfortunately is off by default.

5. **Software patching policies** – patching software can be done manually or

http://www.nmgi.com/tag/security/

2. **Cyber insurance** – consider if protection is needed beyond your firm's base professional liability coverage. Options include: AON, Lloyd's of London, Rhodes Risk Advisors and others.
3. **Policies** – the firm should have a variety of acceptable use, security and breach response policies. We can provide samples of these on request.
4. **Business Continuity Disaster Recovery Plan** – all firms should have a plan, but few do. A BC/DR plan seems to be a something that is particularly easy to put off.
5. **Currency of applications** – older software, for example Windows XP and before and Office 2003 and before are no longer maintained by Microsoft. These products allow bad guys easier access to our systems.
6. **Remote workers** – in the world of Bring Your Own Device (BYOD) and working from client sites or homes, how do we protect the systems from attacks started from authorized user's infected computers?
7. **Security breach preparation** – what do you do to prepare? Is encryption sufficient?

The main concern for accounting firms is that if data is compromised, you would have a security breach reporting incident. Today, all but three states have security breach reporting laws. The chances are pretty good that you are doing business with clients in more than one state. While I'm not an attorney and unable to render legal advice, if all workstations are protected with disk encryption, and the server drives are by default encrypted with your virtualization software, under most security breach statutes, your firm should be exempt from reporting. In other words, since you have encryption active at the desktop and a level of protection at the server, you don't have a reportable incident.

What To Do

You may want to give management teams some background on the aggressiveness and risks of attacks. For additional information, you may want to review my blog

post on security here. Some attacks or infections are particularly aggressive. For

Consider what you believe to be the risks for your firm. Build a response plan. Remediate any short falls in your security, policies and procedures. Train your users to minimize the risks. And be safe out there!

Digital Currency • Firm Management • Security

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.