

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

May. 28, 2008

It was Friday, March 14, and it had been an extremely bad week for Mr. Hapless of Hapless CPA. Mr. Unforgiving, the largest client at the firm, was sitting in the lobby waiting to meet with him. Mr. Hapless knew why. The whole week had been about disclosures — the disclosure of personal data from Mr. Hapless' computers and the theft of personal client information. The FBI and State Police had been in the offices most of the week investigating.

“Fortunately, they are gone,” thought Mr. Hapless as he walked down the hall to the front lobby. The news media had moved on to another story in town. He was thankful for the focus shifting from him to someone else. The news media had been camped out in the parking lot waiting to pounce on any customers or employees coming into or leaving the office for comments about the disclosure of data, so Mr. Hapless had given most of the employees the week off. Not that the media could understand the issues facing the firm this time of year. All they wanted to know was how it happened and why the firm had been so careless with client data. No important work had been done this week; most corporate returns had to be extended even though some could have been completed if this issue hadn't happened. This, by far, had been the worst tax season, and there was still a month left.

Mr. Hapless escorted Mr. Unforgiving into the conference room and asked him how things were going, but he knew full well the answer would not be good. Mr. Unforgiving hardly ever came into the office as he preferred to have his underlings take care of his dealings with Mr. Hapless.

Mr. Unforgiving began: “Happy (Mr. Hapless's nickname), we have known each other for a long time, and it is a terrible thing happening to your

firm right now. I really feel badly for you. You probably don't know this,

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

revenue for his small firm. "Bob," Mr. Hapless said, "is there anything I can do to change your mind?"

I know this is bad, but I really thought I was protected; my outside IT person said the firewall I had was sufficient. I didn't know that it wasn't.

Would you reconsider? We have known each other for a long time and that has to be worth something."

"No," said Mr. Unforgiving, "you have cost me considerable time and money already; and from what I have learned about identity theft, it's going to take me several months to clean all this mess up. You should have been thinking more about your security instead of relying on your outside IT guy. See you around town." With that, Mr. Unforgiving got up and walked out of the office.

Is the experience of Mr. Hapless typical in our profession? Fortunately, not yet! As accountants, we need to work diligently to keep it that way. While this story is fictitious, it does give us something to think about. How good our protection is at the Internet perimeter and how much vulnerability we have to an outsider's intent on stealing computer information is a matter all public accountants have to address. The answer resides in how well we protect our networks from both inside and outside threats.

What is Enough Protection?

Risk is the primary issue related to assessing what is enough. How high is an accountant's risk to data compromise and theft? Well, the threat is ever changing. As accountants, we need to prepare and continue to monitor our networks to threats both existing and new. We must continue to understand what is happening

in the connected world of the Internet and make sure we are implementing state-of-

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

a well-protected network so they pass by fairly quickly.

To reduce our risk, we need to implement good solid commercial firewalls and intrusion protection devices on our networks. The definition of good is a device that provides blocking of unauthorized Internet traffic, scanning of approved Internet traffic to ensure it complies with the protocols for that type of traffic, and monitoring logs of activity from our protection device to ensure that no unwanted activity is being detected.

What is the Proper Firewall?

Commercial firewalls are not the devices you find in the local Best Buy or Circuit City; those devices are designed for the consumer market and aim to minimize user support calls. This means that such devices are configured at the factory with settings that allow for more openings than what is desirable for a business. As a practitioner, it is unwise to use such consumer devices in your business because consumers have less risk of attack to their home computers. The consumer items are great for consumers, but not great for businesses.

Leading commercial firewall makers include Cisco, SonicWall and Microsoft. Cisco (excluding Linksys) and SonicWall make physical devices that act as a gate between the Internet and the internal corporate network by placing their device between the two network connections (WAN for the Internet and LAN for the internal network).

Microsoft's firewall product, ISA Server 20xx (where xx is the year of issue), is a software firewall that will run on a standard Windows Server operating system. The last release was 2006, and a new release is expected this year. ISA server works in much the same way as a physical hardware firewall, but instead of a device you use a server purchased from a server manufacturer and install ISA on top of the Windows Server operating system. ISA Server is called a software

firewall because it is independent of a physical piece of hardware. ISA server,

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

to allow the internal network to communicate with the Internet. This difference is the exact reason that commercial firewalls are better; they require the user to specifically allow the types of communication needed. Consumer firewalls are inexpensive and designed to be very much plug-and-play. Many of the more common communications protocols from the Internet are pre-configured to allow the communication whether the user has a need for that particular communication protocol or not.

This pre-configuring, while easy for the consumer, does little to provide significant protection for the business user. And finding and using an open communication protocol is an easy task for hackers. It's even easier to do this on a computer infected with some type of malware such as a Trojan or spyware because most consumer firewalls allow an outgoing connection to create a reciprocal incoming connection. The commercial firewalls will not allow an incoming connection to be created unless it is specifically allowed in the firewall policies. This difference in allowing incoming connections is what separates the commercial firewalls from consumer firewalls.

What Should You Do?

If you are running a consumer-based firewall, you should seriously consider upgrading this device to a commercial firewall because you are barely protected. With the valuable data you hold, you are a sitting duck for someone to pluck out the information and sell it. If you are running a commercial firewall that happens to be several years old, you might consider an upgrade this year. If you are running a commercial firewall and it is less than 18 months old, you are right where you should be in terms of security.

Not sure where you are? Armed with this article, you need to talk with your

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

all of Hapless CPA's client data to ID-Me. As for Hapless CPA, after his largest client left, several others followed. Mr. Hapless ended up selling his firm to Abel, Able and Kuntz for one-third the price he would have received had his data not been stolen.

While the events described in the hacking incident have fortunately not yet happened to a public accounting firm, the scenario is something that could happen if firms do not take proper precautions to protect their data. Every day, criminals use the Internet to obtain stolen credit cards, social security numbers, ACH information, and other personal information that they, in turn, sell to other criminals via the Internet or use for their own benefit to obtain money from the unsuspecting.

Protect yourself with a commercial firewall, and don't let what happened to Mr. Hapless happen to your firm. If you are using a consumer-grade firewall, work with the technical people who help your firm to implement a commercial-grade firewall. It is important to lock and deadbolt the door to your house, so make sure you do the same for the data stored on your network. Not securing your data is an invitation to identify thieves and hackers to break into your network and steal information. Don't become a victim.

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.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us