

How Safe Is Your Client Data?

by Gregory H. Friedman, CFP®

Past Issues & Articles

[Past Issues](#)

[Find Articles](#)

[Large-Quantity Reprints](#)

[Permission to Reprint](#)

If you are like most of the advisors I have spoken with, you and your firm have taken reasonable measures to protect the information that you collect about your clients. You feel confident that you have taken steps to protect your paper as well as your electronic files. Your offices are locked after hours, your office building has some sort of security or alarm system, and your computers are probably locked up in a separate room within your office. This is all enough to provide good security, right? Wrong! Hopefully you can benefit from my experience, and I'll follow it with some important security tips.

A Secure Office?

Our office is located just outside of San Francisco in a highly populated suburb. It is in a three-story "A" quality office building, near other similar buildings and a hospital. Our suite has floor-to-ceiling, 2-inch-thick doors (11-foot ceilings) with industrial grade door locks, and is located at the corner of the building with lots of exterior windows made of very thick "shatterproof" glass. The building itself has (or so we were told) an alarm system after hours, as well as a security guard who makes periodic sweeps during the night and weekend hours (but is not on site full time).

We did not have a separate room for our server computers or paper files, or a separate alarm for our suite. We did, however, have a locked computer cabinet for our servers (more on this later).

The Break-ins

Our adventure began on a routine weekday morning. As I approached the glass door that I always use to enter the building, it was obvious something was wrong—the glass security door had been completely destroyed, with broken glass strewn up to 40 feet away. I immediately had a sinking feeling that our suite might have been broken into.

I went to our suite, and just as feared, the door locks were hanging down—they had been hit with a sledgehammer. I opened the door and began the process of determining what had been taken. We were lucky. The only items stolen were a laptop computer from our conference room and one flat-screen (LCD) monitor. Considering the amount of computer hardware we have, this was not much.

We immediately called an alarm company and arranged to have a security alarm system installed in our suite. That very day, the company put stickers on all points of entry, warning of the existence of an alarm system, but the system itself was not to be installed for about ten days. On the ninth day, at 3:00 in the morning, I got "the call" from our local police department—we had been broken into *again!*

Once again the glass security door had been destroyed, and the same technique as before had been used to enter our suite. This time they only took one laptop computer (the replacement!), although many other suites in the building were broken into and other laptop computers were stolen.

Lessons Learned

There are several things to be learned from this experience that might help you in terms of the security of your client data and your business:

- Investigate and know exactly how good your building security system is. What we *thought* was in place and what actually *was* in place were two different things. For example, we were told there was an alarm system when we moved in, but upon further questioning, it turned out there wasn't.
- If your suite doesn't already have deadbolts, add them. Although these can also be destroyed, it does make an attempted break-in more difficult and may act as a deterrent.
- Have your own alarm system for your suite. We have installed a sophisticated system that monitors all points of entry and includes motion detectors. If there is a break-in, there will be a piercing alarm to (hopefully) scare away the intruders. In addition, the alarm company and local police are notified.
- Centralize your client data storage and secure it. All of our data is located on our servers, and our servers are locked in a computer cabinet. To remove the cabinet would basically require a crane (due to the weight of a four-battery uninterruptible power supply unit), and in order to break into the cabinet, the computers would be destroyed. A separate locked computer room is *not enough*. The rooms are too easy to break into.
- Your computer systems, especially laptop computers, are valuable. It is essential *not* to have private information on these systems. We were fortunate in that we don't have any data on our workstations or laptop computers—the data is located entirely on our servers. Note that if your data is only in one location, it is essential to have good backups in case of data loss. We have two forms of backup: (1) all of our data is backed up nightly to tape and stored offsite and (2) we use Evault (www.evault.com) to do nightly Internet backups.

Mobile Technology and Security

These events should also be considered in the context of mobile computing, including laptops with data on them and hand-held computers (such as Palm Pilots). Many advisors wish to have access to some of their client data when they are out of the office. This data usually includes names, addresses, phone numbers, e-mails, notes and possibly some financial information.

Although this technology certainly can be useful, you should consider the potential disaster that could result from losing (or having stolen) computers containing confidential data. I have spoken with several computer experts who, although they feel that the security on hand-held devices is pretty good, have all agreed that they would not want their financial advisor using them! If an advisor were to lose his or her handheld computer (or have it stolen) and clients began having problems because certain private information was in the hands of a criminal, the advisor would have a tough time explaining to clients how carrying around client information fit within the advisor's privacy policy or duty for confidentiality.

There are many great ways to access your office from a remote computer—one of the easiest is GoToMyPC (www.gotomypc.com). If you have access to the Internet, you can access your office—securely. There are Internet cafés, computer kiosks in airports, hotel TVs and more. These methods for accessing your office do not require any confidential data to be on your mobile computer.

Conclusion

This column has addressed the physical aspects of providing security for your confidential client data. Not discussed, but equally important, is

protecting your data from “virtual” attack, such as destruction or theft of data from a hacker, virus or computer crash. It simply is not enough to think that if your office has door locks, your computer servers are in a locked room, and the building has some kind of alarm system, your client data is safe. Providing as much protection as possible to your client and office data is essential to the health and well-being of your clients and your business.

Gregory H. Friedman, CFP®, is the principal of Friedman & Associates, a financial planning firm in Novato, California. He is the original creator of Junxure™, an office management system for financial planning firms.



Contact Us



Copyright ● FPA Privacy Statement ● CFP Board Disclosure Statement ● FPA Disclosure Statement