IN BRIEF

THIS ISSUE
May 2014
Issue 123

OSB Professional Liability Fund

www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

Protect Confidential Files – It Helps!

A few years ago, at the end of a three-day holiday weekend, I received a call from my landlord. He reported that someone had broken into my law office. The police were on the way. He asked if I could come down right away. As you might imagine, this was not a great wake-up call.

My partner and I arrived at our small office. Someone had shattered the floor-to-ceiling glass window, scattering glass everywhere. Our server (containing confidential information about clients, opposing parties, and me), backup hard drive, scanner, phones, and two laptops were gone. Our client hard files were still there, but all of our business hard files and personal tax information was gone, as well as the operating and trust account checkbooks. I felt sick. I was overwhelmed. We would have to notify and protect our clients; close down bank and credit card accounts and set up new ones; and get new computers and updated software. I would have to deal with the loss of my private information as well.

Within about a week or so, we had replaced our stolen equipment and were up and running. In about a month, we were back at full capacity. Two protections we had put in place before the break-in made a big difference in helping us get back on our feet: (1) we had an off-site "cloud" backup of our files, and (2) we had a great business premises insurance policy that included our equipment replacement, damage to the premises, identity theft protection for our clients, and business interruption protection for us. The total cost for both of these expenses was just $600. It was worth every penny.

Electronic File Backup

Having an off-site backup for your electronic files is a must. We used Carbonite, but a variety of services are available. We were able to recover almost all of our electronic files in their original form because our server backed up remotely every week. It took about four hours to download everything. Since the break-in, we have our computers backed up daily.

Premises Insurance

Our landlord required us to obtain premises insurance. As a small firm, we didn't like the extra cost but decided it wasn't a bad idea. Our insurance agent looked out for us, suggesting coverage that included personal property loss, business interruption, and identity theft protection. Our coverage paid for:

- New computers and software
- Scanner and phones
- IT services to purchase and set up the new equipment
- IT services to recover our electronic files
- IT services to set up our office
- Assistance in notifying clients and opposing parties (Our insurer hired a well-known identity protection company. They helped us write notices. The PLF helped, too.)
- Costs of notifying clients of the break-in
- Identity protection monitoring and services to clients and employees for one year
- Cost of repairing damage to premises
- Compensation for loss of business income for the month we were not able to work at full capacity

Notifying Clients and Vendors

We notified clients, opposing parties, employ-

ees, vendors, and others of the break-in. Our insurance company helped us write the notice of the break-in and the steps that we were taking to secure confidential information in our possession. Our insurer provided identity theft protection services through a company that works with businesses facing this type of crisis. Because we had an off-site backup of our electronic files, we could access an accurate list of our client and vendor information quickly. We were able to get the letter out soon after the break-in so our clients and employees could monitor their accounts and financial profiles.

Quite a few of our clients contacted us, thanking us for the notice and protections. Honestly, they were more concerned about us. We were grateful for such good clients.

What to Do Before Something Happens

In light of our experience, we recommend taking the following steps:

1. Back up your server daily and maintain a copy of electronic files off-site. We also do on-site backup. You can't have too many copies.

2. Have insurance. It is not very much money when your ability to practice is at risk.

3. Maintain a good alarm system. Again, the cost is minimal and may be enough to scare someone off.

4. Lock up your server and hard files. Factor this into the space you rent.

5. Consult your IT professional about other precautions. Our electronic files are encrypted. There are many other options.

6. Maintain a paper calendar. We had (and continue to have) electronic and paper docketing calendars. We recovered our electronic calendar. The paper calendar saved us immediately after the break-in by enabling us to immediately identify and manage deadlines. We slept better.

What to Do After a Break-in

We hope you never experience a break-in. If you do, we recommend the following:

1. Call and work with the police. Ask for and keep police reports. You will need them for insurance.

2. Put holds on client trust and firm operating accounts. We recommend confirming requests in writing. One of our accounts was not changed despite our request to the bank. As a result, the thief was able to access some funds. Thankfully, our bank covered that check. I believe they did so because I often went into our local branch and had a good relationship with our business banker.

3. Call your insurance company.

4. Call your professional liability carrier(s).

5. Notify everyone who is possibly affected (e.g., clients, opposing parties, vendors, and others).

6. Change your login and passwords. You will be surprised by how many accounts you need to change. We have an encrypted list of this information.

7. Breathe. A burglary is painful, but you will survive if you have taken some precautions before it happens.

Better Safe Than Sorry