ISBA MUTUAL INSURANCE

The Fundamentals of Loss Prevention for Lawyers

EXCERPT

▶ CHAPTER 12:
Data Breach and Privacy

Serving Illinois Lawyers

Chapter 12: Data Breach and Privacy

If you think law firms are not attractive targets for data breaches, think again. Law firms have been increasingly targeted because they are holding massive amounts of information that can include business data, client's personal information, and litigation theories. Experienced hackers have come to learn that they don't have to target the business or the entity; they can target their lawyers and obtain the sensitive information they are seeking.

There are two major cyber security threats to law firms:

- Data theft – these attacks are usually in the form of malware that is downloaded from legitimate high traffic websites. It can collect data without being detected.
- Data leakage – disgruntled employee misuses or mishandles confidential information; or cloud-based sharing devices such as Google Docs become compromised.

While most of the newsworthy stories of law firm hacks are associated with large firms, all law firms regardless of size are attractive targets for hackers. These hacks put the law firm at risk for breaching the duty of confidentiality to keep client data safe; potentially subject the firm to malpractice claims; and may require costly data-breach notification actions.

Example A

> Jerry, a lawyer, who is at their desk working, receives an email from their friend Steve, who owns an all-you-can-eat burger joint, that invites him to join the thousands of others who have tried this great new weight loss smoothie for only $19.99. There is a button that reads "Click Here to Learn More About This Product". Jerry is intrigued that Steve would send him this email and he clicks on it. Within seconds, all the computers in the office shut down.

Example B

> Jodi is a new associate at the firm. She is doing a great job and she receives great performance reviews. For a variety of reasons, none of which make sense to Jodi, the firm will not promote her or increase her salary. She continues to work every day but she is starting to get angry by the lack of recognition. She decides she is going to leave the firm and she downloads all the client files and firm templates to her personal computer. Later she uploads all the documents on the internet to embarrass the firm.

Review your ISBA Mutual Policy to understand the coverage that you can expect to receive if either of these scenarios happens to your firm. Most policies provide coverage for Breach Response Coverage. Ideally, your firm should have a crisis management plan in place that will guide you through the adverse impact on your firm's reputation and the impact to your firm's clients when confidential information becomes public.

Safeguarding Client Data

You may be wondering if there is anything you can do to avoid the scenarios described. Candidly, you will not likely be able to avoid these situations but here are some things you can do to reduce your risk of being a victim of a cyber-attack.

Copyright ISBA Mutual Insurance Company 2021

- Use encryption so that all data on all firm devices is inaccessible without the pass key.
- Install threat detection and prevention software.
- Require strong passwords and/or authentication mechanisms.
- Protect firm networks with firewalls or other technology that limits access.
- Ban access to certain websites like file sharing services from firm devices.
- Develop and maintain procedures for when breaches occur.
- Prohibit employee use of personal emails and/or limit
- internet access to certain sites.
- Implement firm policies and procedures relative to the use of mobile devices with access to firm systems, including email.

Computer Backups.

A law firm should generate a backup copy of all computer data on a weekly basis. This back up copy should then be stored outside the office in a secure location such as a safe deposit box or your home. Not only will it protect your client data in the event of a computer breach, it will also protect your client data in the event of a system crash, power failure or fire.

Data Breach and Privacy Do's and Don'ts

Do…

- ✓ Use encryption so that all data on all firm devices is inaccessible without the pass key.
- ✓ Install threat detection and prevention software.
- ✓ Protect firm networks with firewalls or other technology that limits access.
- ✓ Develop and maintain procedures for when breaches occur.
- ✓ Implement firm policies and procedures relative to the use of mobile devices with access to firm systems, including email.

Don't…

- ☹ Don't assume your employees will be able to identify infected emails.
- ☹ Don't assume you will never have a disgruntled employee
- ☹ Don't allow firm devices to access file sharing services.
- ☹ Don't allow employee use of personal emails. (Or limit internet access to certain sites.)
- ☹ Don't forget to backup all computer data on a regular basis.

ISBA MUTUAL INSURANCE

ISBAMUTUAL.COM
(312) 379-2000