PLF *in*BRIEF

ISSUE 134 | MAY 2018

Malpractice Prevention Education for Oregon Lawyers

Cyberattack Prevention Series

A cyberattack can be a security incident in which the confidentiality, integrity, and availability of electronic data are threatened. Examples of these incidents include ransomware, attempted hacks, or malware. A cyberattack could also escalate to a data breach in which sensitive, protected, or confidential data is potentially viewed, stolen, or used by an unauthorized source.

A cyberattack can have devastating consequences for a law firm. The impact of an attack can include the financial effects of lost revenue due to shutdown, as well as the costs associated with protecting clients following a data breach. A cyberattack can also affect the firm's reputation and ability to sustain or bring in future business.

The article that follows provides guidance on how to prevent and respond to cyber incidents. For an overview of cyberattacks, see "Anatomy of a Cyber Claim," August 2017 *in*Brief.

Cybersecurity Risk Assessment and Analysis

By Rachel Edwards, PLF Practice Management Advisor

Whether you have electronic data, all paper files, or a mix, the threat of data breach is present. Incidents that result in compromised electronic law firm data are often referred to as "threat events." Threat events include cyberattacks, physical damage due to water or fire, and loss due to stolen or misplaced files. In the context of paper files, incidents may include damage caused by water or fire, or they may be due to stolen or lost paper files. Although this article focuses on electronic threat events, the recommendations discussed apply equally to paper and electronic files.

Conducting a cybersecurity risk assessment and analysis can reduce the risk of data loss or exposure from a cyber incident. The level of risk varies depending on the probability of an incident occurring and the type of damage an incident may cause. For example, if an incident is very likely to occur and would cause a loss of all firm data, the risk may be characterized as "high." Whereas if the incident is not likely to occur and the impact would be nominal, the risk may be characterized as "low."

To accurately determine your firm's level of risk of data loss and effective strategies for reducing that risk, consider first conducting a "risk assessment," followed by a "risk analysis."

A risk assessment is the process of identifying "what can go wrong." It evaluates all of the threats to and vulnerabilities of the firm's data system, as well as potential impacts and probabilities of threat events occurring. A risk analysis identifies what can be done to reduce the risk.

Risk Assessment

Consider using a third-party vendor to conduct or assist with the risk assessment. Below are some questions to answer during a risk assessment and some examples of each:

- **What data does the firm hold?** Client names and contact information, Social Security numbers, financial information, medical records
- **Where is the data being stored?** Paper and/or electronic:
  - **Paper** - File cabinets, offsite storage unit
  - **Electronic** - Desktop computers, servers, portable devices, zip drives, CDs, cloud storage
- **Who has access to the office?** Attorneys, firm employees, landlord, mail carrier, cleaning service, delivery service
- **Who has access to which types of data?** Attorneys, firm employees, bookkeeper, IT support
- **What should be kept?** Is it necessary for the firm to store the data, and if not, how can it be properly destroyed?
- **What are the potential threats to the data?** Physical damage, theft, computer virus, lost device
- **What is the probability of threat events occurring?**
  - **Office location** (is the office in a flood plain or an area prone to burglaries?)
- **Virus protection software** (does the firm have virus protection software, and if so, is it regularly updated?)
- **Lost devices** (does the firm allow employees to take devices out of the office that contain confidential client information?)
- **What are the vulnerabilities of the firm's data system?** Weak passwords, lack of employee training, failure to implement backup systems, poor network management, unsupported software
- **What safeguards are in place?** Office security, virus protection software, office policies and procedures

Risk Analysis

After the risk assessment has been completed, conduct a risk analysis to determine appropriate steps for reducing the risk of data loss or exposure:

- **Identify the risks discovered during the assessment:** For example, outdated virus protection software, unnecessary storage of client data, firm policies allowing for removal of confidential information from the office, lack of employee training regarding cybersecurity risks
- **Identify the level of risk of data loss or exposure for each type of risk:** Low to high
- **Determine appropriate responses to each type of risk: Options for responses may include:**
  - Discontinue the activity related to the risk;
  - Improve building security;
  - Improve network security;
  - Implement a proper data backup system;
  - Improve passwords;
  - Maintain updated hardware and software;
  - Maintain updated virus protection software;
  - Secure portable devices with passwords and encryption;
  - Implement written security policies;
  - Implement employee training regarding cybersecurity;
  - Implement employee confidentiality agreements;
  - Limit access to certain types of sensitive data;

- Implement departing employee protocol to ensure no continued access;
- Create an incident response plan.

A firm's threat environment is constantly changing due to various factors, such as changes in data storage and increasingly sophisticated hacking capabilities. Conducting a risk assessment and analysis on a regular basis will help to reduce law firm risks.