PLF *in*BRIEF

ISSUE 135 | OCTOBER 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.

Incident Response Plan

By Hong Dao, PLF Practice Management Advisor

Law firms should be prepared to respond to cyberattacks. A cyberattack could be a security incident in which the confidentiality, integrity, and availability of data is threatened. Examples of these incidents include ransomware, attempted hacks, or a stolen or lost laptop. 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.

Regardless of whether data has been accessed or exfiltrated, it's important for lawyers to have a plan to respond to the incident. An Incident Response Plan (IRP) is a set of protocols for managing the aftermath of a cyberattack. Properly handling the incident can limit damage, reduce recovery time and costs, and provide business continuity for the firm.

Lawyers could use an IRP template available on the Internet as a framework, but it should be customized to fit the firm's size, technology infrastructure, and business operations. An IRP for a solo attorney may consist of a checklist while it may be a manual or handbook for a big firm. Your plan may not be perfect, especially when used the first time, but you can improve it as time goes on. It's better than having no plan.

Preparation

Preparation is key. Know how your firm will handle different types of incidents — what steps will be taken and by whom. Your firm's response to a stolen laptop may differ from that for a ransomware attack.

Preparation has two components. The first is creating an incident response team. This means identifying the people in the firm with a function to perform and specifying the hierarchy of team involvement. Those individuals must be trained and prepared to handle the incident. Their name, title, and contact information should be listed in the IRP. The contact list should also include a data breach lawyer or legal ethics lawyer, an IT specialist or a digital forensic consultant, the local FBI office, and the cyber liability insurer.

The incident response team, with assistance from IT, should develop a process to identify the nature and scope of the incident, contain it, eradicate the source, and recover the affected systems. This process will be different depending on the types of incidents involved.

The second component of preparation is creating mock scenarios to test the IRP. The mock security incidents will help team members understand their roles and give them opportunities to implement the IRP before a real incident occurs.

After an incident — either real or staged — it is important for the incident response team to meet to discuss any lessons learned. This gives them the opportunity to evaluate the success or failure of each step taken and discuss strategies to make the systems more secure and to prevent similar attacks from occurring again. ■