Be ready

with an Incident Response Plan

Because a cybercrime attack can cause irreparable harm, law firms should be prepared to take action immediately. Being able to do this requires an Incident Response Plan, or IRP.

An effective IRP can put a firm in a position to effectively and efficiently manage a breach by protecting sensitive data, systems, and networks, and to quickly investigate the extent and source of the breach so that operations can be maintained or promptly restored. Many firms design IRPs so that they address inadvertent breaches as well – for example, a lost USB key, or a misdirected email. An IRP can help avoid many of the pitfalls of an ad hoc response, such as slow containment (leading to more widespread impacts and damage), lost productivity, bad press, client frustration, and even malpractice claims or discipline complaints.

A complete IRP addresses the detection, containment, and eradication of a cyber breach, recovery of normal operations, and follow-up analysis. When creating your plan, we encourage you to address the following issues:

Build an IRP team.

The size and composition of the team will vary depending on the size of your firm, but teams of all sizes should have a leader. If the firm employs IT staff, they will be key members of the team. There should also be representation from senior management, from the firm's main practice groups, and from the communications and human resources departments, if these exist. Roles and responsibilities for all team members should be documented in the firm's plan. Where necessary, team members should be trained in the procedures required under the plan.

Establish priorities.

In the event of a cyber attack, what should the firm's first priorities be? Presuming no staff are in physical danger, a firm's first priority is often protecting the confidentiality of client information. Identify and rank your priorities (be sure to include the need to notify LAWPRO and/or your cyber risk insurer), and design your response accordingly. For example, the IRP may specify the order in which servers and services will be restored. Ensure that business objectives and priorities are met while negative effects on users are minimized.

< PREVIOUS NEXT >

Be ready to investigate.

To be able to respond appropriately, you will need to understand the nature and extent of the cyber attack or breach. If you have an IT department, there may be individuals on your staff with sufficient knowledge of forensic investigation to isolate the problem. Firms without an IT department should identify, in advance, the provider that would be contacted to investigate a breach, and record this contact information in the IRP.

Remember – non-IT staff may be the first to discover a cyber incident. Encourage your staff to report indications of trouble. See "How to recognize your computer is infected with malware" on page 16. In the event that a third party (for example, a client) detects a problem – for example, by receiving a phishing email – you should ensure that it's easy for third parties to identify the appropriate contact person to whom to report the issue.

Have a communication plan.

Prompt and effective internal communication is essential to an effective incident response. The IRP should have a "call tree" with current contact information that will govern communication between staff should an incident occur when many are out of the office. Contact information for outside IT and other service providers should be documented in the plan and kept up to date. It is useful, where the firm is trying not to immediately tip off the intruder, to avoid email communications – in these cases, phone, text, BlackBerry Messenger, or fax communication should be preferred.

It is useful to have a list ready in advance of outside parties who should be notified, along with current contact information. These parties may include the police, clients, insurers, credit card companies, a public relations firm, and your Internet service provider (be sure you have a current contact list saved outside your usual system).

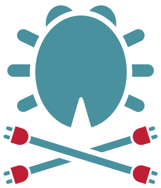
Be technically prepared. While the details of breach prevention protocol are beyond the scope of this article, some of the basic protective steps firms can take are:

- create an inventory of computing resources;
- back up systems and data daily;
- create an offsite record, updated regularly, of client and service provider contact details;
- create a software archive and a resource kit of tools and hardware devices;
- create redundancy capacity for key systems;
- prepare a checklist of response steps;
- log and audit processes;
- use automated intrusion detection systems and a secure firewall; and
- use secure mechanisms for communication.

Have a containment plan.

As soon as a problem is identified, be prepared to make decisions about how to contain damage. IRP team members should have authority to lock down accounts and change passwords, to determine whether and which systems need to be shut down or isolated, and how to decide when it's safe to restore operation. It is useful for IRP members to document events and responses as they unfold – this record will be invaluable for the analysis of the attack once it's over.

Effectively eradicate threats.



Once the damage is contained, the firm will need to be prepared to resolve the incident by identifying and correcting all breach points, and eradicating all intruder leavings (malware, etc.). This is a complex and sometimes tedious process that may require external help.

Analyze the incident and the effectiveness of your response to help prepare for the next event.

Once the threat has been contained and then eradicated, the incident should be thoroughly analyzed. How did the intruder get in? What was he/she looking for? What did he/she accomplish?

You should also review the effectiveness of the firm's response. If there were any areas of confusion or parts of the plan that didn't work well, consider how those aspects of the IRP might be improved, so you'll be better prepared for the next attack when it happens.

While it takes some time and effort to create an IRP, being ready to respond to an incident in a coordinated and effective way can reduce damage to records and systems and minimize the impact of a cyber attack on your firm's productivity. Because the panic associated with a crisis can lead to errors and missed steps, it is much better to have thought these issues through calmly beforehand. ■

Nora Rock is corporate writer and policy analyst at LAWPRO

< PREVIOUS NEXT >