The Basics of the IRP Four Phase Plan for Lawyers

The NIST's Computer Security Incident Handling Guide organizes the IRP in four phases:

- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Post-Incident Activities

The specific tasks that law firms will need to include in each phase will vary depending on a variety of factors. Below are some suggestions for developing a basic IRP.

1. Preparation

In the preparation phase, the IRP should describe the procedures for maintaining and updating the plan itself and identify the personnel responsible for those tasks. This part of the IRP should discuss training personnel on how to implement the plan.

The phase of the IRP should also:

- identify the personnel and devices covered by the plan;
- establish the preventative measures required for covered devices (i.e.- password policies, lock screens, software updates);
- assign responsibility for those preventative measures;
- include a procedure for verifying that those preventative measures are in place;
- identify the personnel responsible for that verification and define the responsibilities of each.

2. Detection & Analysis

An IRP will only be effective if personnel know when to implement it. This phase of the plan should:

- describe how a cyber-attack is detected;
- identify when signs of attack should be reported;

- identify the personnel to whom the report should be directed;
- assign responsibilities to the personnel who receive a report of cyber-attack.
- describe a procedure for escalation of the report;
- establish a timeline for escalation;
- describe the tasks to be completed internally to confirm and analyze the attack;
- identify when outside professionals should be consulted and provide the appropriate contact information.

Determining how a cyber-attack is detected will include obvious signs of an attack such as receipt of a ransom demand, discovery that an unauthorized email was sent from the user's account, or notification from anti-virus software that a virus has been detected. The plan should also alert personnel to less obvious signs of infection. The Federal Trade Commission has warned that any of the following can be signs of a malware infection on a device:

- device slows down, crashes or repeatedly displays error messages;
- device will not shut down or restart;
- device will not allow user to remove software;
- inappropriate ads, ads that interfere with page content, excessive pop-up ads;
- appearance of new or unexpected toolbars or icons on a browser or desktop;
- change in default search engine or home page;
- new tabs or websites not opened by user;
- sudden loss of battery life.

Personnel should be advised to collect information about the event or events that triggered the report and preserve that information in case it is useful in the next phase.

3. Containment, Eradication & Recovery

The level of detail provided in the containment, eradication and recovery phase of the IRP will depend upon the complexity of the system and the capabilities of internal personnel. If there is no in-house IT department, outside professionals will likely perform

most of the tasks in this phase. It is wise to consult with those professionals to understand the containment, eradication and recovery tasks required and what those tasks will reveal about the attack. Some understanding of this phase is necessary to confirm that the proper steps are being taken to identify what client data has been compromised so that lawyers can advise affected clients. The containment, eradication and recovery tasks should also be described in the IRP. Understanding this phase will help personnel appreciate the need for full compliance with the IRP at the preparation and detection phases and may help guide updates and revisions to the plan.

4. Post-Incident Activities

For most IRPs, the post-incident activity phase focuses primarily on analyzing the cause of the breach and revising policies and procedures based on lessons learned. For lawyers, the post-incident phase of a cyber-attack is more involved. As discussed in ABA Formal Opinion 483, lawyers have an ethical obligation to inform affected clients of a data breach. This obligation derives from a lawyer's duty under Prof.Cond.R. 1.4 to keep a current client reasonably informed about the status of matters and the duty to explain the matter so that the client can make informed decisions about the representation. The lawyer must communicate with current clients about a data breach if there has been:

- a misappropriation, destruction or compromise of client confidential information; or

- a situation where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the event

The disclosure must provide enough information for the client to make an informed decision about what to do next. The lawyer must identify for the client the data that was accessed or disclosed and describe the lawyer's efforts to respond to the attack.

In this phase, a law firm's IRP should:

- describe a process for notifying clients by:
    - identifying the data that was accessed;
    - analyzing the risk to each client caused by the access, and
    - communicating that information to the client.
- describe a process for analyzing the incident to determine whether changes to firm policies and procedures are necessary;
- identify the personnel assigned each task in both processes;

- establish a timeline for performing those tasks.

The analysis of the risk to the client and communication with the client cannot be delegated to nonlawyer staff.

We recommend the following resources for additional guidance:

- OBLIC's CyberToolbox
- NIST's Computer Security Incident Handling Guide
- CISA Cybersecurity Incident & Vulnerability Response Playbooks

As always, if you have any questions, please contact us. We are here to help.

Gretchen K. Mote, Esq.
Director of Loss Prevention
Ohio Bar Liability Insurance Co.
Direct: 614 572 0620
Email: gmote@oblic.com

Monica Waller, Esq.
Senior Loss Prevention Counsel
Ohio Bar Liability Insurance Co.
Direct: 614 859 2978
Email: mwaller@oblic.com