## Incident Response Plans

The foundation of the respond function is advance planning. This means that attorneys and law firms should have a plan, usually called an incident response plan (IRP). An IRP should broadly cover all kinds of security events, incidents and breaches, including spearphishing, ransomware, business email compromise, insiders accessing data without authorization, a lost or stolen laptop or mobile device, and others.

Preparing processes and technology in advance is necessary for effective incident response. For example, having an inventory of information assets and data, and a data map showing data flow and storage locations, will expedite an incident response. It can be a nightmare to put together when an incident is in progress. Notice requirements should be identified in advance, including the type of covered information, who should be notified, and contact information. In addition, enabling and retaining logs in networks, cloud services, and intrusion detection/prevention software can provide invaluable information, otherwise unavailable, to understand the nature and scope of an incident. Effective backup and business continuity measures are also important.

The IRP should be appropriately scaled to the size of the law practice and the sensitivity of the information. For a solo or very small firm, it may just be some checklists and who to call for what.

The elements of an IRP should include:

- Assign responsibility
- Internal reporting procedures
- Criteria for activating the plan
- Internal personnel and resources
- Alternate communications channels for response
- External resources:
    - Data breach lawyer
    - Insurance carrier
    - Law enforcement
    - Digital forensics consultant
    - Notice and credit monitoring service provider
    - Crisis communications consultant
    - Bank
- Communications plan (internal and external)
- Notice:
    - Identify required and optional notice
    - Employees
    - Clients
    - Service providers
    - Other third parties
- Keep a record of response activities and systems changes
- Preserve digital evidence
- Mitigation: confirm that compromise has been contained and eradicated
- Restore systems
- Practice the incident response plan
- Training

- Periodic review and update

IRPs should be flexible. They may not survive first contact with the enemy, but that's okay. It's usually better to have to adapt than to have to start from scratch in a panic. Alternates should be included for internal and external personnel and resources in case the primary ones in the plan are unavailable. It's much easier to move down a list than to scramble for an alternate during an incident.

The plan should identify a full complement of internal and external resources that may be necessary for the most serious incidents or data breaches. It should be scalable so that resources are activated as they are needed. For example, malware on a single laptop may be handled by IT, with notice to management, while a major ransomware infection may require all of the resources in the plan.

The IRP should identify internal personnel who may be necessary for each function in the plan, including management, IT, compliance, security, human resources, finance, marketing, etc. In a small firm, the same person(s) will perform multiple roles. Include complete contact information (e.g., home and cell phone numbers and personal email) in case of an incident at night or during a weekend, or if firm communications are down or compromised. Some laws firms use communications services that can send notices to personal phones and emails – either the entire firm or selected groups.

An experienced data breach lawyer will often serve as a coach or quarterback for an IRP team. In addition to providing legal advice and coordinating response activities, he or she may be able to assist in protecting privilege for some of the information related to the investigation and response.

It's generally a good idea to contact external resources, like a breach attorney, digital forensics consultant, and law enforcement, in advance, before any incident. Having a working relationship or even just an introduction can make an actual response more effective.

If the firm has an insurance policy that provides or may provide coverage, check the notice requirements in the policy. Policies often require the use of approved service providers, like breach attorneys and digital forensics firms, and may require prior authorization to use an approved provider.

It is sometimes difficult to get prompt and active involvement of the appropriate federal agency (FBI, Secret Service, Department of Homeland Security, etc.) in response to a complaint. They have a priority for national security and heavy caseloads. A good approach is to start with an online complaint to the FBI's Internet Crime Complaint Center (IC3). This provides an immediate record of the complaint and may start an IC3 analyst on financial account recovery if the details of the transaction are provided on the appropriate online form. A complaint to IC3 can be promptly followed by contacting the appropriate federal agency and state or local law enforcement.