PROFESSIONAL COUNSEL®

Advice and Insight into the Practice of Law®

The Importance of Incident Response Planning: A Cyber Risk Control Perspective for Law Firms

Cyberattacks continue to be a top concern for many security professionals in diverse industries, and indications are this is a trend that is likely to continue to increase with emerging technology. A single breach to an organization cannot only be a reputational risk, it can be very costly. It is projected that cybercrimes will cost $10.5 trillion by 2025.[1] Having a well-documented and tested Incident Response Plan ("IRP") can greatly mitigate exposure as well as reduced time for recovery in the event of a successful attack. Incident response planning is essential to a law firm's cybersecurity platform. In fact, the first question a regulator often asks after an incident is reported is whether or not the company had an IRP.

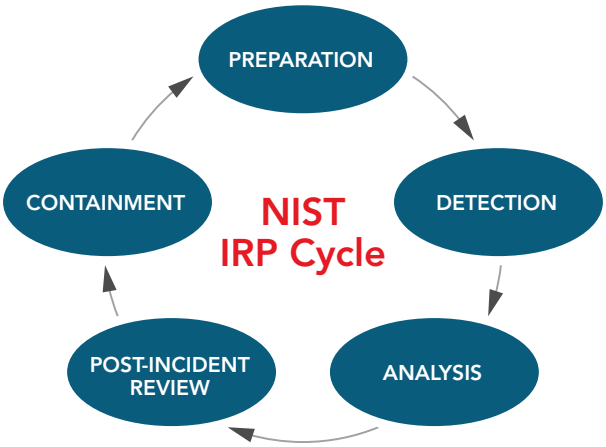
The Who

Lawyers are required to understand the technologies that they use in their daily practice of law. As specified in American Bar Association ("ABA") Model Rule of Professional Conduct 1.1 Competence, comment 8 specifies, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

As part of the attorney-client relationship, attorneys and their respective law firms are required to maintain client confidentiality. As specified in ABA Model Rule of Professional Conduct 1.6 (c) Confidentiality of Information, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Comment 18 to ABA Model Rule of Professional Conduct 1.6 discusses the importance of "reasonable efforts" to protect information related to the client representation. "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." Establishing an IRP is part of the reasonable efforts law firms may take to protect client information and knowing how to respond when it is compromised.

1 2023 Official Cybercrime Report



The What

There are many Incident Response Plan guides available to businesses but law firms have been a popular target for cybercriminals. As recognized by the FBI[2] and ABA, law firms hold a great deal of client data that may be monetized by bad actors. Cybersecurity professionals often follow National Institute of Standards and Technology ("NIST") guidance for Incident Response Plans. For this article, we will reference NIST guidance for best practices; however, your business may follow other guides to accomplish goals best suited for them.

It is important to note the differences of an Incident Response Plan, Business Continuity Plan and a Disaster Recovery Plan:

An **Incident Response Plan ("IRP")** is a set of documented procedures detailing the steps that should be taken in each phase of an incident. It should include guidelines for roles and responsibilities, communication plans, and standardized response actions.

A **Business Continuity Plan ("BCP")** should include steps to maintain or resume business operations **during** a disaster or other unplanned incident.

A **Disaster Recovery Plan ("DRP")** is the process of recovering business functions and systems **after** an event.

The NIST process emphasizes that incident response is not a linear activity that starts when an incident is detected and ends with recovery (as shown above). Incident response is a circular process, where there is continuous learning and improvement to discover how better to detect and respond to future incidents. Planning and preparation is vital for the IRP process.

The Why

These are the main reasons to have a strong incident response plan in place:[3]

1. **Prepares for Emergencies** – mostly, security incidents happen without warning, so it's essential to prepare a process ahead of time;
2. **Repeatable Process** – without a tested incident response plan, teams cannot respond in a timely manner;
3. **Coordination** – it is vitally important to have a coordinated response where everyone is aware of their roles and responsibilities and can act in a coordinated manner;
4. **Identifies Gaps** – frequently testing an incident response plan exposes obvious gaps in the security process which can be addressed before a crisis occurs;
5. **Practice Makes Perfect** – an incident response plan creates a clear, repeatable process that is followed in every incident, improving coordination and effectiveness of response over time;
6. **Documentation and Accountability** – an incident response plan with clear documentation reduces an organization's liability – it allows you to demonstrate to compliance auditors or insurance companies what was done to prevent the breach.

The How

Creating an Incident Response Plan

Creating a clearly defined Incident Response Plan will enable law firms to outline procedures for detecting, controlling, and remediating security incidents so that employees know how to respond to security events when they occur. Preparation is critical for an effective Incident Response Plan.

Incident response planning is essential to a law firm's cybersecurity platform.

2 FBI Alert Warns of Criminals Seeking Access to Law Firm Networks

3 7 Reasons You Need a NIST Incident Response Plan

Preparation

Establish Incident Response Teams

- Roles and responsibilities clearly defined. Who has the authority to make the call of a breach?
- Is Ransomware part of the scenario? Is there a predetermined policy/guidance on paying Ransomware? Who will make this call?
- Employee responsibilities during and after an incident.

Develop a Communication Strategy

- Understand how your law firm will share cyberincident information with each type of stakeholder: law firm employees, external partners, clients and, if necessary, the general public.
- Develop communication plan templates that are pre-prepared and ready to distribute that includes employee content, vendor content, client content.
- Include internal off-hours contact numbers, noting that many system breaches and network compromises are attempted after normal working hours, on weekends or on holidays.
- Establish relationships with other key contacts prior to any incident:
  - Law Enforcement (FBI, SEC, etc.)
  - Human Resources
  - Legal – Legal can assist with any potential actions and can give guidance and approval for answers to specific questions: Is the malefactor on list of Office of Foreign Assets Control ("OFAC") countries?[4] Are notifications different in different states? Countries' General Data Protection Regulation ("GDPR")? Regulators vs. customer notifications.
  - Critical Vendors impacted
  - Insurance Carrier – Reach out to your cyber insurance provider and determine what they may provide for negotiations. Have its reporting information readily available prior to an incident.
  - Technical Contacts (e.g. Amazon Web Services ("AWS"), Microsoft, etc.)

Understand Current Cyberthreats

It is important to know the most common attack vectors and capabilities that are being used so you can ensure appropriate controls are in place and tested to minimize potential threats.

- **Phishing and Business Email Compromise** – Phishing attacks have grown much more sophisticated in recent years, with attackers becoming more convincing in pretending to be legitimate business contacts. There has also been a rise in Business Email Compromise, which involves bad actors using phishing campaigns to steal business email account passwords from high level executives, and then using these accounts to fraudulently request payments from employees.
- **Malware** – Malware is a term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.
- **Third Party Exposure** – Cybercriminals can get around security systems by hacking less-protected networks belonging to third parties that have privileged access to the hacker's primary target.
- **Ransomware** – Ransomware is one of the most common cyberattacks, hitting thousands of businesses every year. These attacks have only become more common, as they are one of the most lucrative forms of attacks.

Detection, Analysis, Containment

Create/Consult an incident response playbook. Recovery should align to business continuity plans and recovery time objectives previously established. You should consider the following:

- What is the prioritization of recovery?
- What comes up first, second, etc.?
- Threat playbooks can explain how common cyberthreats like malware, Ransomware phishing attempts, and Distributed Denial of Service Attack ("DDoS")[5] attacks work and outline what actions an employee can take to protect key systems during each scenario.

4 Sanctions Programs and Country Information

5 Cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Testing, Testing, Testing

- Must test all components regularly (muscle memory)
- Review incident response plans quarterly, revisiting strategies to find areas for improvement.

An effective incident response plan is all about simplicity. If the response process is too complex, teams will struggle to implement it during a live attack. Taking a few basic steps like building an incident response plan, communication strategy, and threat-specific playbooks, like Ransomware, will dramatically enhance ability to respond to threats.

Ransomware Payment or Recover?

Ransomware is one of the top threats facing organizations and individuals today. Organizations are more worried about a Ransomware attack than any other cyberthreat.* Effective controls being put into place prior to any Ransomware attack can greatly reduce the risk of data or financial loss, reputational risk or regulatory fines.

* 12 Most Common Types of Cyberattacks

The Most Effective Controls to Reduce Risk of Ransomware

Backup Data – Regular backups of data are a critical control to ensure an organization can recover from Ransomware, and other issues like a hardware failure, or data center fire. Backups need to be tested to ensure they can actually be used for restoration, if needed.

Updated Systems – Always keep operating system, web browser, antivirus, and any other software updated to the latest version available. Malware, viruses, and Ransomware are constantly exploiting vulnerabilities with new variants that can bypass old security features. Timely vulnerability patching is key to stay ahead of these exploits. Additionally, minimizing the use of End-of-Life ("EOL") or unsupported platforms that cannot be patched or updated reduces Ransomware risk as well. EOL platforms may no longer receive security patches, creating an increased risk to the organization.

Network Segmentation – This control can help reduce the severity of an attack by preventing an automatic compromise of all data within the organization. Implementing network segmentation divides the network into multiple smaller networks so the organization can isolate the Ransomware and prevent it from spreading to other systems.

Email Protection – Alerting employees about an email's external origins can help ensure the message receives scrutiny, and stop a social engineering attack at the very beginning. Sender Policy Framework ("SPF")/Domain-based Message Authentication Reporting and Conformance ("DMARC")/Domain Keys Identified Mail ("DKIM")[6] technologies help secure a company's email systems to prevent spoofed messages, as well as phishing and spam.

Endpoint Detection and Response ("EDR") – Traditional anti-virus agents rely on signatures to detect malicious software (Norton and McAfee), EDR looks at the behavior of software and processes to detect malicious activity. An EDR tool should be deployed to all workstations, cloud and non-cloud servers. **This is a critical control that can go a long way towards preventing Ransomware.**

Limit Privileged Access – Removing local admin privileges from employee workstations prevents unauthorized changes from being made. This control prevents unauthorized software installation, and configuration changes as well. It also makes it more difficult for malware to install itself and propagate throughout the network.

Security Awareness – Conduct regular Security Awareness Training and frequent anti-Phishing campaigns. Employees are on the front lines and need to be aware and vigilant against social engineering and phishing attacks. Regular security training helps keep employees aware and vigilant regarding their responsibilities to keep the company secure.

Multi Factor Authentication ("MFA") – The principle of least privilege combined with MFA creates a solid foundation for securing a network or system. This is the single most important control that should be implemented in these areas:

- Remote access to the network, including web-based email
- To protect Privileged[7] User accounts
- For all Cloud resources

A law firm's survival may depend on getting the encryption key from the cybercriminals to decrypt and get back their stolen data in a short period of time. Even with the most effective controls outlined above, there is still the risk of an attacker getting around these controls and disrupting the business. Determining whether recovery and restoration in a timely fashion is adequate to resume business operations or to consider payment of Ransomware can be determined by a few questions long before any attack has taken place.

6 SPF, DKIM, and DMARC help authenticate email senders by verifying that the emails came from the domain that they claim to be from. These three authentication methods are important for preventing spam, phishing attacks, and other email security risks.
7 Privileged users are those that have been granted access to sensitive information, such as law firm financial or payroll records.

Key Considerations to Address Before a Ransomware Attack

It is imperative that a law firm have immediate contact information for their cyber insurance provider before taking any action in response to a Ransomware incident.

Law firms facing Ransomware threats or an actual incident should work with their cyber insurance provider to coordinate an appropriate response to minimize the exposure and evaluate the impact on law firm clients. Beyond a potential payment, law firms will need to consider notifying clients of a cyber security breach and respond in accordance with the relevant jurisdiction/s breach protocols.

Cyber Concerns

Contact your broker to find out more about cyber insurance options for your law firm.

As known targets of cyber criminals, law firms should consider implementing an IRP to respond to the increasing likelihood that client information will be compromised by unintended disclosure or a cyber security breach. In addition to providing competent legal services, law firms should make reasonable efforts to protect information related to the client representation part of law firm protocol.

Additional References

- Incident Response Blog
- Best Practices to Prevent Ransomware Attacks

About CNA Professional Counsel

This publication offers advice and insights to help lawyers identify risk exposures associated with their practice. Written exclusively by the members of CNA's Lawyers Professional Liability Risk Control team, it offers details, tips and recommendations on important topics from client misconduct to wire transfer fraud.

This article was authored for the benefit of CNA by:
Mike Berryhill and Theresa Garthwaite

Mike Berryhill, CNA Cyber Risk Control, has 38 years of experience in the financial industry, and is recognized as a leading expert in Operational Risk oversight, with a specialized focus on Information Security and Technology. Throughout his extensive career, Mike has honed skills in conducting comprehensive risk assessments and providing consulting services that ensure organizations are well-equipped to safeguard their operational integrity and security in an increasingly complex digital landscape. Mike has also obtained several industry certifications, including Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), and Six Sigma Black Belt and Green Belt.

Theresa Garthwaite serves as Risk Control Consultant for CNA's Lawyers Professional Services program. She is responsible for the overall assessment, evaluation and delivery of risk control services for complex risk exposures within CNA's Lawyers Professional Liability business. She is responsible for developing risk control content for presentations and publications. She oversees the "In Practice … with CNA" and "CNA's Professional Counsel" publications. Prior to joining CNA, Theresa worked as an associate in a boutique law firm, specializing primarily in plaintiffs' medical malpractice, catastrophic personal injury and wrongful death matters. She is admitted to practice in Illinois and United States District Court, Northern District of Illinois. Theresa also holds the Commercial Lines Coverage Specialist (CLCS) designation, and is a recipient of the Risk Control Superior Service Award.

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com