Incident Response Preparation Primer

SHOOK HARDY & BACON

This primer provides Shook, Hardy & Bacon's new Privacy and Data Security clients preliminary guidance to prepare for a data security incident. It addresses who should be involved, what initial steps should be taken to prepare for the incident, how the organization can minimize the risks of an incident, and how the organization can respond quickly and effectively when an incident occurs.

1. FORM AN INCIDENT RESPONSE TEAM

Led by legal counsel (preferably outside counsel with strong privacy and data security expertise) to maximize potentially applicable privilege, the Incident Response Team (IRT) is responsible for evaluating enterprise risks, identifying and classifying regulated information, and ensuring compliance with legal obligations governing the collection, use, and storage of sensitive information. "Sensitive information" includes personal information to which legal obligations apply, proprietary information and other confidential business information. The IRT should be composed of stakeholders from various areas within the company. For example:

- **Legal**
- **Information Security and Physical Security**
- **Human Relations**
- **Operations**
- **Marketing/Communications**
- **Compliance**

2. ASSESS THE LEGAL AND SECURITY RISKS

During this phase of preparation, your organization should identify risks, rate them based on likelihood and severity, and understand applicable legal obligations.

(A) Define "Sensitive Information" for Your Organization

- **Personal information** – The definition of personal information differs depending on the residence of the data subjects. Identify those jurisdictions as soon as possible.
- **Proprietary information** – This is sensitive non-public business information you must protect. It often includes trade secrets, pricing information, and strategic planning documents.
- **Confidential information** – This is other sensitive information that does not fall into one of the previous categories. It includes legally protected information and privilege documents. Legal obligations often apply to this information (e.g., protective orders, privileged information, etc.).

(B) Perform an Inventory of Data in Your Organization's Possession and Control

- How is the data created/imported?
- Where is the data stored?
- Who has access to the data?
- With whom is the data shared?
- For how long is the data retained and how is it ultimately destroyed?

(C) Assess Your Organization's Legal Risks

- Identify the domestic and foreign statutes, regulations, industry standards (e.g., PCI DSS), contractual provisions, and other legal obligations that apply to your sensitive information.
- If a regulator were to audit your organization, would you be able to confidently say that your organization is in compliance with these requirements?
- Determine what administrative, technical, and physical safeguards are in place to protect the sensitive information.
- Create a matrix that measures risk against the likelihood of adverse event. This will help you prioritize action items.

(D) Assess the Security of Your Sensitive Information

- Retain outside counsel with expertise in directing information security assessments.
- Have your outside counsel engage an outside forensic firm to conduct an information security assessment.
- Identify scope of the information security assessment – which systems, what are your goals, and what is your budget?

TYPES OF INFORMATION SECURITY ASSESSMENTS

1. Compromise Assessment – identifies whether the organization is or has recently been infected with malware or other programming tools that would indicate a pending or recent data compromise. Highly recommended for organizations in the "beginning" phase of developing an incident response program.
2. Penetration Test – tests the ability of an unauthorized third-party to penetrate the technical safeguards (firewalls, network segmentation, etc.) an organization has implemented. Highly recommended for organizations in the beginning to moderate phases of implementing an incident response program.
3. Red/Blue Teaming – the forensic firm uses creative measures to obtain access to sensitive information. These measures may include spear-phishing and onsite visits by a disguised forensic firm employee, in addition to the techniques discussed in the penetration test. Recommended for organizations with highly developed incident response programs.
4. Tabletop Exercise – assesses your incident response program through a series of onsite workshops, provides guidance on improvements, provides a simulated data breach exercise with the IRT, and the deliverable identifies strengths, weaknesses, and benchmarks your organization against your peers.

3. ENGAGE INCIDENT RESPONSE VENDORS

(A) Legal Counsel

Arguably the most important vendor you will select as part of the incident response preparation process is your outside counsel, who will guide you through the response to a data security incident, direct your forensic vendor, advise you on legal obligations, and respond to regulators and counsel for third parties affected by the incident.

Some questions to consider when vetting outside counsel include:

1. Do they have a dedicated and robust privacy and data security practice group?
2. What experience does the firm have representing organizations like yours in preparing for and responding to data incidents?
3. What relationships does the firm have with your regulators?
4. What kind of a "fit" will the firm be with your organization? How familiar is the firm with best practices in information security in your industry and with your industry's business culture?
5. Will the firm provide references from other privacy and data security clients?
6. Your engagement letter with outside counsel should state that you are retaining the firm for the purpose of evaluating your compliance with privacy and data security laws, and that you understand that it may be necessary for the firm to hire a forensic expert to assist the firm in obtaining information necessary to render legal advice. By doing this, your organization maximizes protection of the documents through the attorney-client privilege and work product doctrine.

(B) Information Security Forensic Firm

When responding to a data incident, you do not want to waste time vetting various forensic firms and negotiating contractual provisions with the selected vendor. Your organization actually loses leverage if it waits until that point in time to engage the forensic vendor. The forensic firm should be engaged by a Master Services Agreement and, for each specific project, through outside counsel via a Statement of Work ("SOW"). The SOW should make clear that the forensic work is being done at outside counsel's direction for the purpose of allowing outside counsel to provide legal advice regarding your company's compliance with privacy and data security laws.

Some questions you should ask the forensic firm during the vetting process include:

1. What is the largest data incident the firm has handled?
2. How quickly can they have "boots on the ground" when an incident occurs (and will they guarantee a certain level of responsiveness)?
3. How highly recommended is the firm by your outside counsel? What is outside counsel's experience with the forensic firm's responsiveness, quality of work, and ability to make complex information easy to understand?
4. Do you have an existing relationship with the forensic firm? (It may be best to retain a firm that can provide a "fresh set of eyes" and greater objectivity).
5. Will the firm provide references?
6. If the firm requires an upfront retainer, and you do not need the firm's services during the retention period (usually one year), can you use the retainer toward other services like a compromise assessment or tabletop exercise?

(C) Credit Monitoring

In the event of a data breach, you may want (or be legally obligated) to provide credit monitoring to individuals affected by the incident. Here are some points to consider when vetting credit monitoring vendors:

1. What different types of credit monitoring services are available?
2. How much do these options cost? Is there an advantage to purchasing monitoring access codes before an incident occurs? If so, is there an expiration for those advance-purchased codes?
3. If your organization does not purchase the access codes before an incident, how long will it take the vendor to provide the requisite number of access codes to your organization when needed?
4. You should proactively identify when credit monitoring is and is not appropriate. For example, credit monitoring does little to help targets of payment card breaches, and one court has used the fact that credit monitoring was provided as evidence of harm to consumers for standing analysis. Nevertheless, your organization may make a business decision that providing credit monitoring is necessary.

(D) Communications/Public Relations

When an incident occurs, your organization must be prepared to communicate quickly, effectively, and accurately with internal stakeholders (board of directors, executives, employees, and service providers) and external entities (customers, the media, and regulators). A robust marketing/communications department that is well prepared can often handle those objectives. The proactive creation of communications templates certainly helps reduce response burdens. Nevertheless, some organizations prefer to retain an outside public relations firm to assist in preparing for and responding to an incident. In vetting an outside public relations firm, some issues to consider are:

1. Do they have a group dedicated to crisis management or incident response?
2. How many breaches have they worked on and what was the average size of those incidents?
3. Will they provide references?

(E) Mailing/Call Centers

Is your organization equipped to mail notices to thousands (or tens of thousands) of individuals at one time? Is your organization prepared to respond to the telephone inquiries that follow when recipients of the breach notice have questions? (Statistics show that approximately 10% of breach notification recipients request additional information upon receiving notice). Depending on your answers to those questions, you may want to consider engaging a company in advance that can assist you in mailing the correspondence and responding to inquiries. Here are a few considerations in vetting that potential vendor:

1. In the event of a large breach, how quickly can the vendor prepare (i.e., convert from a template you provide and merge with addresses you provide) and mail data breach notification letters? How long would it take to prepare and mail 1,000 letters—100,000 letters?
2. How many follow up inquiries at the same time following the mailing of breach notification letters can the vendor handle?
3. What process has the vendor implemented to obtain necessary information about the incident, train call screeners, supervise calls, and how are calls escalated within the company and to clients?

(F) Cyber Insurance

You should not assume that your commercial general liability or errors and omissions policies cover the costs your organization would incur in the event of a data breach. Insurers now offer dedicated privacy, technology, and data breach insurance policies. Additionally, there are insurance brokers who specialize in helping companies find coverage in the event of a data breach.

Questions you should consider asking your carrier/broker when in the market for a cyber policy include:

1. What is the reputation of the carrier in the area of data breach response? How often do they deny coverage? How responsive and cooperative are they?
2. What proactive services does the carrier offer its insureds to minimize the risk of a data breach?
3. How much coverage does your organization need? (Factors include the organization's industry/sector, the amount of sensitive information in the organization's possession, the likelihood of litigation or regulatory enforcement actions, and the type of sensitive information in the organization's possession).
4. What losses will the policy cover? What losses are excluded?
5. Will the carrier allow you to select the incident response vendors of your choice? (TIP: Ensure that the names of your vendors are included as part of the insurance policy).

4. DRAFT NECESSARY POLICIES AND PROCEDURES

(A) Incident Response Plan

An incident response plan (IRP) provides a blueprint for responding to data security incidents and identifies who will be responsible in the event of an incident. It should be drafted by counsel in partnership with your company's information security officer(s).

A strong incident response plan does the following:

i. Identifies those who need to be involved.
   1. *Internally (the IRT)*
   2. *Externally (incident response vendors, law enforcement contacts, regulatory contacts)*

ii. Provides a centralized process within the organization for identifying, reporting, and escalating the incident.

iii. Provides a method for preliminarily screening the incident to determine the severity level and need to involve entire IRT or external incident response vendors.

iv. Provides a method for memorializing the incident, the response taken, and any remedial measures implemented as a result of the incident. (Again, the memorialization should be done by counsel).

v. Incorporates the application of attorney-client privilege and work product doctrine where appropriate.

vi. Helpful Appendices:
   1. *Breach notification templates*
   2. *Communication guidelines (and sample communication statements)*
   3. *Applicable laws/jurisdictions*
   4. *Contact information chart*
   5. *Workflow demonstrating the process of identifying, responding to, and resolving a data incident*
   6. *Different workflows depending on the nature of the incident (e.g., hacking, misuse of information, inside job, negligent loss of information, vendor issue, etc.)*

(B) Incident Response Policy

The incident response policy implements the incident response plan throughout the enterprise and provides employees with the procedures they should follow to identify and report potential data incidents. The policy defines a data incident, provides examples of incidents, and explains that disciplinary measures may be taken if employees fail to abide by the policy.

(C) Consumer-Facing Privacy Notice

This notice explains to consumers what information your organization collects, how you use and store the information, who you share the information with, how long you keep the information, and how a consumer can contact your organization to change/delete her information or retract consent to the collection of her information.

(D) Online Privacy Notice

The online privacy notice explains to visitors of your website or application what information the website/app collects about the user, what you do with that information, and how the website/app responds to various privacy enhancing technologies. A statement regarding the organization's use of tracking technologies is often contained within this notice as well.

(E) Internal Privacy Policy

The internal privacy policy defines personal information for your employees, the importance of handling personal information with care, the organization's rules on the appropriate handling, access and use of personal information, and disciplinary measures that may be taken should the policy be violated. The policy also governs the appropriate handling of employee personal/HR information, and provides a point of contact to whom employees can direct inquiries about how their information is handled by the company.

(F) Written Information Security Plan

The Written Information Security Plan (WISP) describes the administrative, technical, and physical safeguards that the organization implements to protect sensitive data and minimize the risk of a data breach. Following a data breach, regulators will often ask an organization for its WISP. Massachusetts, for example, has specific WISP requirements for organizations that collect personal information about Massachusetts residents.

5. TRAINING

The most effective way to minimize the risk of a data breach is through awareness and training about information security risks. Every data breach has a human element, whether it's clicking on a malicious link in an email, losing a laptop, or sending an email to the wrong recipient. While most individuals have heard of data breaches, they assume breaches occur only through sophisticated cyberattacks. Many employees are unaware of the definition of "personal information" and the consequences their company may face if the information is accessed without authorization. It is therefore important to train both executives and "front-line" employees alike on these risks, and document the training to be able to demonstrate to regulators that your organization takes the training of employees on privacy and data security issues seriously.

Here are some training modules/techniques your organization should develop:

(A) Board-Level Training

- Communicate in a "plain spoken" way, potential legal and business risks and strategies for mitigating those risks.
- Identify how the most common security incidents occur and best practices for minimizing the risks of their occurrence.
- Inform of steps already taken to minimize the risks within the organization.

(B) Executive-Level Training

- Identify information security risks and ways to minimize them.
- Ensure familiarity with organization's privacy and data security policies.
- Understand how to escalate potential information security risks appropriately.
- Know when and how to sanction employees for violation of privacy and data security policies.

(C) "Frontline" Training

- Provide general training on privacy and data security risks.
- Conduct role-based training based on how the employee may encounter sensitive information.
- Ensure understanding of how to identify and report potential data security incidents and violations of policies.

(D) Enterprise-Wide Awareness

- Require annual "refresher" training.
- Use bulletins and short updates to remind employees about privacy and data security risks.
- Conduct blind email phishing and other exercises targeting employees to determine how well they react to potential data security risks.

6. TESTING, AUDITING, AND MONITORING

After the organization's collected data has been inventoried, compliance with applicable laws can be confirmed, and an incident response plan is in place, it is important to regularly test the plan and make updates where appropriate. One of the most effective techniques for identifying and implementing these changes is through annual tabletop exercises, led by a third-party information security vendor and directed by outside counsel. An effective tabletop exercise will evaluate existing documentation, provide best practices and benchmarking on security risk minimization, test the IRT through a series of real-time data breach exercises, provide post-exercise assessment, and identify remedial measures through a deliverable prepared by the information security vendor at the direction of counsel.

7. VENDOR MANAGEMENT

An organization's weakest security link is often with its service providers. At minimum, your organization should be undertaking the following steps to minimize the risks of a vendor's data breach:

(A) Conduct Thorough Due Diligence

Before your organization engages a vendor, due diligence must be undertaken to assess the vendor's security risks and identify potential compliance issues the vendor may have with respect to privacy and data security laws. Regulations usually place accountability with the organization at the top of the data chain, rendering your company ultimately responsible for your vendor's compliance with privacy and data security laws, and the security controls it implements (or fails to implement). It is therefore important that you identify the risks before engaging the vendor.

(B) Contracting with the Vendor

Ensure that your master service agreement with the vendor has privacy and data security provisions that will protect you. For example:

- Indemnification if your organization suffers damages as a result of the vendor's data incident, or at a minimum require the vendor to purchase insurance that will cover losses your organization suffers as a result of the incident.
- Immediate notification (within 48 hours) of a potential data security incident, and agreement to cooperate in an investigation of the incident.
- Compliance with applicable state, federal, and international privacy and data security laws relevant to the nature of the services being provided.

- The right to audit the vendor's data security controls, or at the very least third-party independent certification of compliance with a recognized data security framework (e.g., ISO, NIST, SOC-2, SOC-3).
- In some circumstances, where highly sensitive data is involved, it may be necessary to include specific security controls within the contract, like encryption at rest and in transit, limitations on access to information, background screening requirements (where permitted), and data segmentation.
- Ownership in the data such that you have an unrestricted and unqualified right of access to your own data under all circumstances. This includes a unilateral right to return of the data, on demand, within a reasonable time and in a specified or reasonably useable format.
- The right to be notified where a third-party requests access to your information.
- Confidentiality of sensitive information.

(C) Monitoring

After the relationship has been established, it is important that the vendor's compliance with the agreed-to privacy and data security safeguards be monitored and, where appropriate, remediated.

CONCLUSION

This primer merely provides a high-level overview of the issues. Effective incident response planning is different for each company depending on their industry, the jurisdictions from which they collect information, their regulatory authorities, and their business model.

Shook, Hardy & Bacon's Privacy and Data Security Practice is available to assist your organization in tailoring a plan and preparing for and minimizing the risks of a data breach.

For additional information regarding incident response planning and preparation, please contact:

Al Saikali
Partner | Miami
Chair, Privacy and Data Security Practice
305.960.6923
asaikali@shb.com

Colman McCarthy
Associate | Kansas City
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate | Tampa
813.202.7151
kpaine@shb.com

Ben Patton
Associate | Seattle
206.344.7625
bpatton@shb.com