SAMPLE INFORMATION SECURITY INCIDENT RESPONSE PLAN

Establishment date, effective date, and revision procedure

This plan was established and approved by [*Organization Name*] on [mm,dd,yyyy]. The [*Organization Name*] Incident Response Team Leader shall facilitate a review of this plan at least once a year, and at any additional time when there are changes that may affect corporate management with respect to incident response. In the event that amendment or repeal of this plan becomes necessary as a result of such review, the [*Organization Name*] Incident Response Team Leader shall prepare a draft and apply for authorization, and with prior confirmation of the Corporate Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [*Organization Name*] Incident Response Team Leader will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Contents

1 Overview

1.1 Purpose

This Incident Response Plan (IRP) provides the framework and guidance for managing and responding to Information Security Incidents. The purpose is to help business-critical services:

- Quickly and efficiently recover from incidents,
- Respond in a systematic and complete manner,
- Prevent or minimize disruption of critical information systems,
- Minimize loss or theft of sensitive or critical information, and
- Minimize harm to individuals affected by the incident and the organization.

This plan will govern the flow of communications among management and workforce, outside vendors (e.g. attorneys and IT forensic experts) and other organizations (e.g. law enforcement agencies and insurance companies). The plan is intended to be flexible; not all components of this plan will apply for every incident.

1.2 Scope

This plan applies to all employees, contractors, vendors, and others who process, store, transmit, or have access to sensitive information including personal information (PI) or other confidential information (CI). The IRP applies to both electronic and non-electronic information.

1.3 When to Use This Document

All workforce members should be trained to immediately report any suspected or known Information Security Incidents to a member of the IRT. When the IRT is engaged, this plan must be consulted, and the components appropriate to the specific incident must be followed.

2 Incident Response Team

Note to the user: Your incident response team (IRT) should include representatives from all of your organization’s functional groups. Since you cannot predict what parts of your organization will be impacted by a breach, include on the IRT a staff member from each functional group and train them how to respond to a potential data breach. They should know who to contact, from whom to take direction and what to do in the event of a data breach. Your internal IRT should include someone from IT, security, legal, privacy, compliance, communications, risk management, human resources, customer service, business continuity, finance and a member of the executive management team. The circumstances of the incident will dictate the appropriate team members and resources to be engaged, and the IRT members should possess authority to engage appropriate internal and external resources to respond to the incident.

2.1 Internal IRT

Internal IRT members have specific responsibilities with regard to the reporting and handling of Information Security Incidents. It is important that each member know his/her role in advance. Note that one person may serve in multiple roles. The IRT members and their contact information are contained in the Internal Incident Response Team Contacts document.

2.1.1 Incident Response Team Leader

The IRT Leader is responsible for managing the overall incident response and must possess strong project management skills to coordinate multiple, cross-functional tasks simultaneously. Primary responsibilities include:

- Ensuring the internal and external IRT contacts are current,
- Engaging the IRT members in the event of a security incident,
- Ensuring sufficient resources are allocated to the response,
- Assigning response tasks to appropriate internal and external resources,
- Coordinating and tracking the progress of response tasks from discovery to completion,
- Ensuring the response is documented in the Information Security Incident Report Form,
- Preparing a timeline for managing all response tasks,
- Preparing a budget and tracking response costs,
- Serving as a liaison between the IRT and senior management, and
- Conducting a post-incident review of the response and updating the IRP and training programs accordingly.

2.1.2 Executive Management

The designated representative from Executive Management will:

- Inform the Board and Executive Management of the status and potential impact of the incident,
- Evaluate and approve response strategies and determinations that may have significant impacts on the organization,
- Serve as the media representative or spokesperson for communications such as press releases (if necessary), and
- Approve and serve as signatory for notification letters to affected parties or third parties (if necessary).

2.1.3 Chief Information Officer (CIO)

The CIO oversees, directs, and has ultimate responsibility for managing data security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of confidential information or personal information.   This includes:

- Reviewing information system security issues that have organization-wide impact,
- Establishing and maintaining the Incident Response Plan,
- Handling and investigating all information security problems/incidents,
- Working with other system administrators to analyze and resolve security incidents,
- Communicating with the IRT and crisis communications/public relations,
- Evaluating and documenting investigation findings after resolving an incident,
- Recommending security strategies (e.g. use of intrusion detection tools, penetration testing, etc.),
- Promoting security awareness to the organization's workforce, contractors and vendors, and
- Overseeing the security related terms of the organization's agreements with its contractors and vendors.

2.1.4 Chief Information Security Officer (CISO)

The CISO is responsible for:

- Implementing the overall response and recovery activities for incidents involving computing systems and networks,
- Providing guidance and assistance in determining the appropriate action to be taken,
- Updating the CIO of incident investigation findings,
- Notifying the CIO of significant incidents,
- Specifying the threat level of an incident and updating the threat level as needed, and
- Providing guidance and, possibly, materials to train all employees in the organization and contractors to the organization if such contractors access sensitive information.

2.1.5 Privacy Officer

Upon notice of an incident, the Privacy Officer shall:

- Coordinate an investigation to determine if PI has been, or is reasonably believed to have been accessed, used or disclosed;
- Evaluate with the advice of in-house legal and outside privacy counsel, whether notification is necessary under applicable state and federal laws;
- Develop a timeline for compliance with any notification requirements under federal or state law; and
- Evaluate other legal obligations arising from the incident with the advice of in-house legal and outside privacy counsel.

2.1.6 Risk Manager

Upon notice of an incident, the Risk Manager shall take the steps needed to protect the organization’s interest under any policies of insurance that may offer coverage including:

- Reviewing applicable insurance policies,
- Timely notifying insurance carriers, and
- Engaging resources available under insurance policies to assist in the response.

2.1.7 In-house Legal Counsel

Upon notice of an incident, the in-house legal counsel, with the advice of outside legal counsel, shall, among other things:

- Determine whether any federal or state agency, law enforcement or regulatory organization should be notified;
- Work with the internal and external legal team to determine the notification requirements, timeline, and implementation plan;
- Review contracts with vendors, customers and business partners to determine if there is a contractual obligation to notify third parties; and
- Work with outside legal counsel to identify other obligations under relevant federal and state laws and regulations.

2.1.8 Communications/Public Relations

Upon notice of an incident, the IRT Leader should engage the Communications/Public Relations Manager. The Communications/Public Relations Manager and in-house legal counsel, with the advice of outside legal counsel, should be involved in deciding when, where and how any announcements are made.

2.1.9 Customer Service

Customer service representatives may need to be prepared to handle incoming calls from affected (or potentially affected) persons. Internal customer support staff or an outside call center may be needed to answer questions, explain how to enroll in credit monitoring or identity theft protection programs, if offered, and similar issues.

2.1.10 Human Resources

If the incident involves employee data, Human Resources will work with the communications team to respond to employee inquiries. Human Resources may also be involved in incidents arising from employee errors or mistakes, as well as intentional actions taken by employees, which may require documentation, training or action.

2.1.11 Finance

Finance will assist in preparing the response budget and tracking and managing response costs.

2.1.12 Business Continuity Management

Business Continuity must ensure that response actions are consistent with the organization's Business Continuity Plan (if any) and designed to minimize disruption to business operations.

2.2 External IRT, Stakeholders and Resources

Depending upon the circumstances of the incident, external parties such as insurance carriers, regulators, law enforcement, legal counsel, forensic investigators, crisis communications/PR firms, and/or response vendors may need to be notified and/or engaged.

Prior to an incident, external contacts should be identified and contracts with vendors should be negotiated in order to save time during an incident response. Contact information for external resources and stakeholders is contained in the External Incident Response Team and Resources.

3 Response Process Overview

3.1 Four (4) Stages of Incident Response

While every Information Security Incident is different, there are generally four (4) stages of response:

1) **Detection and Reporting**. Suspected or confirmed incidents must be promptly reported to the IRT.
2) **IRT Engagement and Initial Analysis**. Upon receiving notice of an incident, the IRT Leader will engage appropriate IRT members and begin investigating the incident. The objective of the IRT's initial analysis is to prioritize the incident to ensure adequate response resources are deployed.
3) **Responding to the Incident**. Depending upon the circumstances, the IRT will take actions as appropriate to respond to the incident and mitigate harm to the organization and affected persons.
4) **Post Incident Review, Documentation, and Follow Up**. The IRT should make recommendations to improve the plan and mitigate the risk and harm from future incidents.

Understanding each stage leads to a better and more efficient response, and helps key staff understand the process of responding so that they can address unexpected aspects of incidents they may face.

3.2 Flow Chart and Checklist

The Information Security Incident Response Flow Chart and Checklist can be used to guide the IRT through all stages of the incident response. Flexibility is important since circumstances and relative risks posed by each incident may vary.

4 Incident Detection & Reporting

4.1 Detection and Reporting

All workforce members should be trained to identify Information Security Incidents and report them to a member of the Incident Response Team. An “Information Security Incident" means any adverse event or activity (observable occurrence) that threatens: (i) the confidentiality, integrity, and/or availability of information the organization possesses, and/or (ii) information systems (including applications and data) or networks of the organization. Examples of incidents that should be reported include:

- Malicious code (e.g. viruses, worms, Trojans, bots)
- Unauthorized access to information assets (e.g. computer or network)
- Network attacks (e.g. denial of service)
- Probe, scan, unauthorized electronic monitoring (e.g. sniffers)
- Theft of source or programming code
- A violation of privacy or data security policies or procedures
- Abuse/misuse (e.g. inappropriate usage) of information assets
- Misuse or accidental disclosure of personal information (e.g. posting on a website or public forum, email sent to wrong person or without encryption)
- Compromised system or user credentials
- Social engineering (e.g. phishing)
- Establishment of an unauthorized account for a computer or application
- Loss or theft of a PC, laptop, cell phone, or other electronic storage device
- Lost, stolen, or missing hard-copy documents or media
- Other circumstances that your organization deems sufficiently suspicious, like erratic behavior associated with a server or employee work station

4.2 Documenting the Incident

Thorough documentation of the incident and investigation is critical especially if regulatory investigations or lawsuits arise from the incident. The employee who discovers the incident should document all known facts including:

- Date and time of incident detection and notification
- Incident detector’s contact information
- Location of the incident
- Systems, applications, services, data and networks possibly at risk

- Type of incident detected
- General description of incident
- Names and contact information of others involved
- Any actions taken since incident discovery
- Any additional relevant information known at the time

The IRT Leader should ensure that each step taken from the time the incident was detected to its final resolution is documented in the Information Security Incident Response Report document.

The IRT should safeguard and restrict access to the incident data because it often contains sensitive information such as data on exploited vulnerabilities, recent security incidents, and users that may have performed inappropriate actions.

4.3 Preserving Evidence

Preservation of the evidence is critical to resolving the incident and may also be necessary for legal proceedings. All evidence should be preserved and collected at the direction of counsel so the information can be analyzed to assess the nature of the incident and appropriate remediation steps. The following steps should be taken to preserve evidence:

- Do not turn off or reboot any potentially affected systems.
- Record critical facts regarding the incident (e.g. date and time when the incident was discovered, who discovered the incident, what occurred, what systems and information were potentially compromised).
- Secure the scene and restrict access to affected systems to maintain the integrity of the evidence.
- Preserve all evidence including logs and surveillance tapes.
- Image the affected computers (if possible) to preserve a record of the system at the time of the incident for later analysis and as evidence at trial.
- Send preservation letters to third parties (e.g. vendors, service and cloud providers).
- Track the chain of custody (e.g. list everyone who had access to the systems, in order, as well as actions taken) for all physical and digital data.
- Identify the systems, applications, and data (type and classification) compromised and back up affected systems to allow future analysis of the system, including any forensic analysis (if needed).

Evidence should be collected according to procedures that meet all applicable laws and regulations. Clearly document how all evidence has been preserved and account for the evidence at all times. Whenever evidence is transferred from person-to-person, chain of custody forms should detail the transfer and include each party’s signature.

Because collecting evidence from computer systems can present challenges, consult with legal counsel and consider engaging forensic experts.

4.4 Handling Communications

Proper handling of internal and external communications is critical especially in the initial stages of an incident. To reduce potential liability, exercise caution in communicating about the incident as follows:

- Handle incident communications on a need-to-know basis.
- Strictly follow reporting procedures; do not discuss the incident with other employees, family, the media, or any other person outside the scope of this procedure until authorized to do so.
- Direct all inquiries to a designated IRT member for response.
- Do not use the term “breach” which may require a legal conclusion. Early in the process, there is rarely enough information to make this conclusion. Instead, call it a “privacy incident”, “security incident” or what it is (e.g. “a lost laptop” or “possible malware intrusion”).
- Avoid using email to communicate about sensitive information including the incident in the event that email and electronic systems have been compromised; use telephone instead.
- If you must communicate via writing, copy your in-house legal counsel (or your outside attorney).
- Mark all written communications and reports as follows: “Privileged and Confidential: Attorney-Client Privileged Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice.”
- Written communications such as emails and other documents should be encrypted or otherwise protected so that only authorized personnel can read them.

5 IRT Engagement and Initial Analysis

5.1 Initial Analysis

Upon receiving notification of a potential or actual privacy or data security incident, appropriate members of the IRT shall promptly analyze the incident, documenting each step.

The IRT’s initial assessment should seek to determine the nature and scope of the incident such as determining whether the incident is a malicious act or a technological glitch. Using log information, the IRT should attempt to identify:

- The affected networks, systems, and applications
- The apparent origin of the incident, intrusion, or attack
- How the incident is occurring (e.g. what malware, tools or attack methods are being used and what vulnerabilities are being exploited)
- Any remote servers to which data were sent (if information was exfiltrated)
- The identity of other victim organizations (if such data is apparent in logged data)
- What data has been compromised and the potential impact of the incident

The goal is to gather enough information to prioritize subsequent activities, such as containment of the incident and a deeper analysis of the effects of the incident.

5.1.1 Identification of Impacted Systems

Assess the types of systems impacted:

- **If the threat relates to non-electronic and/or physical security**, report the incident to the physical security department for action and document the investigation in the Information Security Incident Report Form.
- **If the threat is directed at electronic information and /or IT systems**, consider whether to engage outside forensic experts to conduct an investigation, and document the investigation in the Information Security Incident Report Form, taking care to protect and preserve the evidence.

5.1.2 Identification of Impacted Information

Analyze whether the incident relates to confidential information (CI) or personal information (PI).

5.2 Incident Classification

All incidents should be classified by the IRT to inform those involved of the severity and potential impact and ensure that the incident receives the appropriate level of attention. The incident classification is a dynamic process, and the threat level may change as new information emerges.

- **Level 1 Threat**. An incident is defined as a “Level 1” threat if it is determined that no mission critical systems or resources are at risk, and no CI or PI has been accessed by unknown, untrusted, or unauthorized individuals.
- **Level 2 Threat**. An incident is defined as a “Level 2” threat if mission critical systems or resources may be at risk, or if CI or PI may have been accessed by unknown, untrusted, or unauthorized individuals.
- **Level 3 Threat**. An incident is defined as a “Level 3” threat if it is determined that mission critical systems or resources are at risk, or CI or PI was accessed by an unknown, untrusted, or unauthorized individuals.

Once the incident has been classified by threat level, the IRT can determine the type of assistance that will be needed to address the incident and the type of damage and remedial efforts that may be required. Prioritizing the incident is one of the most critical decision points in the incident response process.

5.2.1 Level 1 Threat Response Actions

Consult with legal counsel to determine whether the incident violated any laws or triggered legal obligations.

- If it is determined that there has been no violation of applicable regulations or laws and there are no legal obligations arising from the event, document the analysis and conclusion, and no further action is required.
- If a violation of regulations or laws is possible or confirmed, take appropriate steps as may be required (e.g. conducting an incident risk assessment and/or notifying third parties.) If there is a duty to notify or other required action, evaluate whether to notify the insurance carrier of the incident and engage outside counsel.

5.2.2 Level 2 Threat Response Actions

Assess whether external forensic investigators will be needed to determine whether mission critical systems and/or CI/PI have been compromised.

- **Threat Denied.** If no compromise of CI/PI has occurred, determine whether potential violations of laws or regulations have occurred or whether there are legal duties to notify third parties or take further actions, and document this analysis and findings.
- **Unable to Confirm/Deny Threat.** If a threat cannot be confirmed or denied, the IRT shall reconvene to discuss next steps and evaluate whether to engage external IRT members or outside assistance (e.g. legal, forensic, law enforcement). If engaging legal counsel or forensic investigators, notify the insurance carrier to identify available resources.
- **Threat Confirmed.** If a threat to CI/PI is confirmed, proceed to Level 3 Response Actions, and document all findings in the Information Security Incident Report Form.

Carefully evaluate any action involving a potentially compromised IT asset. In order to preserve evidence and mitigate further harm, wait for expert support prior to attempting to log in, power down, or take further actions.

5.2.3 Level 3 Threat Response Actions

Determine whether external resources are needed to launch an in-depth forensic investigation to assess the nature, scope and impact of the incident; implement steps necessary to contain the incident; and formulate a response strategy designed to mitigate harmful impacts to the organization and those affected by the incident.

6 Responding to the Incident

Depending on the circumstances, the IRT must perform many tasks to assess the incident and legal obligations, contain the incident, and mitigate harm to the organization and those affected. Many tasks will take place simultaneously.

The IRT should prioritize incidents based on the potential business, reputational and financial impacts and respond accordingly. Factors such as the type of information compromised, scope of the incident, and potential impact to the organization and those affected will influence decisions regarding many tasks.

Identifying the organization's objectives will also guide the response strategy. Examples of objectives include minimizing reputational harm, protecting affected persons, and/or controlling costs.

6.1 Engaging External Resources

Evaluate the need to engage external parties including but not limited to:

- **Insurance Carriers**. Take steps needed to protect the organization's interest under any policies of insurance that may offer coverage including promptly notifying insurance carriers (if notice has not yet been provided) and identifying resources offered by insurance carriers.

- **Outside Counsel.** With the assistance of in-house and outside counsel, identify breach notification requirements and other legal obligations under relevant federal and state laws. Given the potential liability issues and variances in notification laws, consult with outside counsel with experience responding to privacy and data breaches. Consult with the insurance carrier for approved legal counsel.

- **Forensic Investigators**. Determine whether internal IT resources possess the expertise to conduct an in-depth forensic investigation into the cause, scope and impact of the incident while preserving the evidence. If external forensic investigators will be needed, identify resources available under insurance policies. Consult with legal counsel to determine whether the investigation will proceed under the direction of counsel in an effort to preserve legal privileges.

- **Regulators**. Depending on the circumstances of the incident, notification to federal and/or state regulators may be required. Consult with legal counsel regarding such notification.

- **Law Enforcement**. Consult with legal counsel regarding whether to engage law enforcement and, if so, to identify appropriate authorities (e.g. FBI, Secret Service, local police).

- **Crisis Communications/Public Relations**. Depending on the incident and potential media coverage, a crisis communications expert may be needed to develop effective communications strategies and messages to the media, public and affected persons.

- **Response Vendors**. Depending on the incident, external vendors may be needed to assist with notification, call center, and the provision of identity protection services.

- **Other Third Parties**. Evaluate whether other stakeholders (e.g. business associates, business partners, licensing agencies, vendors, and payment card merchant banks/brands) must be notified.

6.2 Conducting a Forensic Investigation

Work with internal and external forensics teams to determine the nature and scope of the compromise, identify the systems and data compromised, identify the threat actor (if possible), assess the potential impact, and formulate strategies to contain the incident and recover any compromised systems and data.

Consider having legal counsel retain external forensic experts in an effort to preserve legal privileges.

Take care to preserve evidence, maintain the chain-of-custody and document all critical facts discovered and actions taken.

Examples of key questions the forensics team will seek to answer include:

- What systems, applications, and data (type and classification) were compromised?
- What data elements were compromised (e.g. name, DOB, SSN, medical information)?
- How many persons or records were affected?
- What is the severity of the potential impact (minimal, serious, or critical)?
- What is the name of the system targeted, along with operating system, IP address, and location?
- What is the IP address and any information about the origin of the attack?
- Is the incident inside the trusted network?
- Will the response alert the attacker?
- What type of incident is this (e.g., virus, worm, intrusion, abuse, damage)?
- What is the source or identity of the suspects involved in the event?
- What steps must be taken to contain the incident, prevent further harm, and recover affected systems and data?

6.3 Containing, Eradicating and Recovering from the Incident

Take appropriate steps to contain the harm and prevent further data compromises, restore any loss of information, recover any corrupted data, and return systems/operations to normal.

Carefully evaluate any action involving a potentially compromised IT asset and wait for expert support prior to attempting to log in, power down, or take further action.

6.3.1 Containment

Take immediate action to limit the scope and magnitude of the incident, secure any affected IT/IS systems or information, and mitigate harmful effects of the data security incident.

Consult with IT and legal teams to formulate the appropriate containment strategy for the incident. Containment strategies will vary based on the type of incident, and an essential part of containment is decision-making (e.g. shut down a system, disconnect it from a network, and disable certain functions; re-route network traffic, filter or block a distributed denial-of-service attack or isolate all or parts of the compromised network). Criteria for determining the appropriate containment strategy include:

- Potential damage to resources
- Need for preservation of evidence
- Service availability (e.g. network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g. partial v. full containment)
- Duration of the solution (e.g. temporary workaround v. permanent solution)

If proper preparations were made and a backup copy of critical data exists, evaluate whether it is appropriate to abandon the network in its current state and to restore it to a prior state. If electing to restore a backup version of data, ensure that the backup is not compromised as well.

6.3.2 Eradication

After an incident has been contained, it may be necessary to eradicate components of the incident, such as deleting malware, disabling breached user accounts, and/or identifying and mitigating all vulnerabilities that were exploited. Identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication may not be necessary or may be performed during recovery.

Remain vigilant even after the incident appears to be under control. Continue monitoring systems for anomalous activity to ensure the intruder has been expelled and you have regained control of your network.

6.3.3 Recovery

Take actions to restore any loss of information, return to normal operations and secure functioning IT/IS systems and business operations affected by the incident. If data was corrupted or destroyed, special steps may be needed in order to perform a reliable recovery. For example, recovery may involve restoring systems from clean backups or rebuilding systems from scratch. Recovery procedures should be executed timely to ensure restoration of systems and data affected by the incident.

6.4 Determining Legal Obligations

With the assistance of in-house counsel and outside counsel, identify obligations and timelines under relevant federal and state laws including, but not limited to, the notification to third parties such as affected persons, media, and regulators.

Most states have data breach notification laws, and the laws vary on many factors including the content, timing, and notice required to regulators, the media, and third parties. State breach notification laws are based on the jurisdiction where the affected individuals reside; therefore, it is imperative to identify the states where the affected persons reside to assess legal obligations arising from the incident. Key determinations include:

- Identifying relevant state and federal privacy and data security laws.
- Determining obligations to notify third parties (e.g. affected persons, regulators, law enforcement, media, credit reporting agencies, and other third parties under applicable laws).
- Determining regulatory timelines for notification.
- Identifying other required actions (e.g. conducting an incident risk assessment).

Consult with outside counsel with experience in privacy and data breach notification laws given the potential legal ramifications.

6.5 Determining Remediation Strategies for Affected Persons

In the event notification is required to affected persons, decide whether identity protection services will be provided. Consult with legal counsel regarding legal obligations as well as regulators’ preferences regarding the provision of such services.

If identity protection services will be offered to affected persons, work with counsel and an identity theft protection services vendor to determine the appropriate protection to address the risks posed by the compromised data elements.

6.6 Developing Communication Strategies

Internal Communications. Use caution when discussing the incident and handle communications on a need-to-know basis, especially early in the investigation. IRT members and employees with knowledge of the event should be instructed not to discuss the incident with any person outside the scope of this procedure and to direct all inquiries to a designated IRT member for response.

Prepare internal communications to employees, senior management, and directors, and train internal resources for media responses.

External Communications. With the assistance of internal and external PR experts, draft an effective and consistent message to affected persons, the media, the public, and regulators to preserve the organization's brand.

Since the timing and posture of any announcement related to a data breach can have significant business ramifications, in-house counsel, with the advice of outside counsel, should be involved in deciding when, where, and how any announcement should be made. Obtain input from IRT members and consider retaining a crisis communications expert.

Implement a communications plan for responding to email inquiries and social media posts regarding the incident to ensure that the messages and responses are consistent.

Designate a single point of contact for discussing events with the media. The following steps are recommended for preparing the media contact:

- Conduct training sessions on interacting with the media regarding incidents. This should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Hold mock interviews and press conferences to determine how common questions will be handled including:
    - What happened?
    - Who attacked you and why?
    - How did the attack occur and why was is successful?
    - How widespread is the incident?
    - What measures are you taking to determine what happened and prevent against future occurrences?
    - What is the impact of this incident?
    - Was any personally identifiable information compromised?
    - What steps are you taking to contain the harm and protect those affected?
    - What is the estimated cost of this incident?

6.7 Preparing Call Center/Customer Support

Work closely with customer support staff to prepare to handle calls from persons affected (or potentially affected) by the incident.

Based upon the circumstances and scope of the event, determine whether to engage an external call center. This determination will likely depend upon whether there is sufficient capacity to respond to a large volume of calls and whether the internal customer support agents possess the skills to answer questions regarding the incident, explain how to enroll in credit monitoring or identity theft protection programs, if offered, and similar issues.

With a large scale breach, consider engaging a call center with a dedicated hotline and providing a website that answers FAQs and provides information on fraud and identity theft protection.

Work with internal and external call center resources to prepare scripts for agents to use when communicating with callers and responses to FAQs. Messaging and responses should be carefully drafted to ease callers' minds and protect the organization's reputation.

Coordinate the timing for the call center with any press releases or notifications.

6.8 Notifying Affected Persons and Third Parties

If notification is required under applicable federal and/or state laws, the IRT must coordinate numerous tasks for the notification process including:

- Identifying relevant federal and state notification laws
- Preparing a timeline for notifications
- Determining how notifications will be made (e.g. via mail, email or substitute notice)
- Determining whether to mail letters in-house or retain an external notification vendor
- Preparing address/mailing lists
- Preparing notification materials (e.g. logo, signature graphic)
- Preparing notification letter templates (or material for substitute notice)

For larger scale events, consider outsourcing notifications to a vendor and review resources available under insurance policies.

Work with legal counsel, marketing resources, and the notification vendor to coordinate the delivery of logos, signature graphics, address lists, and other notification materials.

Preparation of the address list can be time consuming and challenging; therefore, designate a team member who is skilled with using the designated address file format to oversee the preparation and delivery of the mailing/address list to the notification vendor.

For mail notifications, evaluate whether addresses are current or if address verification and cleansing services are needed.

Given the significant liability issues and variances in data breach notification laws, consult with a breach coach to ensure compliance.

7 Post Incident Review, Documentation, and Wrap Up

7.1 Post Incident Review

Gather relevant parties to evaluate the organization's response and assess the strengths and weaknesses of its performance. The goals for this meeting are to:

- Understand the cause of the incident.
- Evaluate administrative, technical and physical safeguards and strengthen as needed.
- Review information security systems, policies, procedures and workflows.
- Review physical security systems, policies, procedures and workflows.
- Update training programs to reflect changes and improvements in safeguards, policies, procedures and workflows.
- Summarize and document all lessons learned.
- Evaluate the IRT communications plan to assess how well it worked and how it can be improved.
- Update the IRP based upon findings.
- Review and update the organization's risk assessment to reflect the new information learned from this incident.

7.2 Documentation of the Incident

Ensure that all evidence is preserved, and all pertinent facts are documented in the Information Security Incident Report Form.

7.3 Annual Review and Updates

Every 12 months, review how well the organization has responded to privacy and data security incidents and provide a written report to the IRT addressing the following:

- Was there sufficient preparation for each incident?
- Do any administrative, physical or technical safeguards need to be modified?
- Should training programs be updated?
- Did detection occur promptly or, if not, why not?
- Could additional tools have helped the detection and eradication process?
- Was each incident sufficiently contained?
- Was communication adequate or could it have been better?
- What practical difficulties were encountered?

- What was the monetary cost associated with the incident(s)?
- How much did the incident(s) disrupt ongoing operations?
- Was any data irrecoverably lost, and, if so, what was the value of the data?
- Was any hardware damaged, and, if so, what was the cost?

As part of this assessment, ascertain whether each of the steps in this IRP was followed and, if not, why not. Discuss any deficiencies and gaps in responses and take remedial actions including reviewing and updating (as needed): (a) this plan; (b) security policies and procedures; (c) administrative, physical, or technical safeguards; and (d) training programs.