Data Security Incident Response Plan

Dated: [Month] & [Year]

[Insert Organization Name]

Introduction

Purpose

This data security incident response plan provides the framework to respond to a security incident. This plan will help business-critical services (a) quickly and efficiently recover from security incidents; (b) respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; (c) prevent or minimize disruption of critical information systems; and (d) minimize loss or theft of sensitive or critical information. This plan will also 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).

Scope

This plan applies to all employees, contractors, vendors, and others who process, store, transmit, or have access to sensitive information including organization confidential information, personal information (PI) (defined in the Glossary in Appendix A) or other confidential information.

Data Security Incident Response Team (Roles and Responsibilities)

[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, compliance, communications and customer service and a member of the executive management team].

Each member of the incident response team (IRT) has responsibilities related to the security of all the organization's sensitive information. The IRT members listed below have specific responsibilities with regard to the reporting and handling of data security incidents. It is important for each IRT member to know his/her role in advance. Note that one person may serve in multiple roles.

Chief Information Officer (CIO) [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Chief Information Security Officer (CISO) [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Information Security Liaison [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Privacy Officer [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

In-House Legal Counsel [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________

Evening/After hours telephones: home: ____________; other: _______________

Insurance Risk Manager [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Crisis Management/Public Relations [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Customer Service [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Notification Vendor [insert names]—contact information:
Daytime telephones: office: __________; mobile: ____________; other: _______________
Email: ________________________
Evening/After hours telephones: home: ____________; other: _______________

Chief Information Officer (CIO) [*or other management-level executive*]

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 PI. This includes:

- Reviewing information system security issues that have organization-wide impact;
- Establishing and maintaining the data security incident response plan;
- Handling and investigating all information security problems/incidents;
- Working with Information Security Liaisons (see section 2.3) and/or other system administrators to analyze and resolve security incidents;
- Communicating with the IRT and crisis management/public relations;
- Evaluating and documenting investigation findings after resolving an incident;
- Recommending security strategies (e.g. use of intrusion detection tools, penetration testing, etc.) to appropriate executive management;
- Providing regular updates on the status of the breach response to the executive management team;
- 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.

Chief Information Security Officer (CISO)

The CISO is responsible for:

- Implementation of the overall response and recovery activities for data security incidents involving computing systems and networks;
- Providing guidance and assistance in determining the appropriate action taken;

- Developing a timeline for compliance with any notification requirements under federal or state law;
- 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;
- Providing the Information Security Liaison(s) with guidance and, possibly, materials to train all employees in the organization and contractors to the organization if such contractors have access to any PI. Employee training includes:
    - Protecting all PI in every form, from paper to electronic files;
    - How to spot unusual system behavior, which may indicate a data security incident in progress;
    - Identifying the types of data security incidents; and,
    - How to report suspected or known incidents (e.g., lost or stolen files, information sent by email to the wrong person, accidental disclosures of PI, a virus infection, a system compromise, or a denial of service incident, which may be detected by resident software on the system user's workstation) to the IRT.

Information Security Liaison

Each department within the organization must designate an Information Security Liaison who will be involved in the detection, analysis and resolution of data security incidents. The Information Security Liaison is responsible for reporting incidents to both the CIO and CISO immediately, as well as supporting the CISO as needed to determine and implement a solution, when possible.

The Information Security Liaison shall do the following if there is a suspicion that a data security incident may have occurred:

- Report potential incidents to the CIO and CISO;
- Log the date and time of all actions, including first notice of incident, etc., with a description of facts and observations (what triggered the suspicion, etc.); and,
- Discuss with the CIO and CISO whether any affected services or resources should be disconnected from the network in light of relevant business considerations and disconnect if appropriate.

Privacy Officer

Upon notice of a data security incident, the Privacy Officer shall:

- Coordinate an investigation to determine if personal information (PI) has been, or is reasonably believed to have been accessed, used or disclosed, and
- Evaluate with the advice of in-house legal and outside privacy counsel, whether notification is necessary under applicable state and federal laws.

Risk Manager

Upon notice of a data security incident, the Risk Manager shall take the steps needed to protect the organization’s interest under any policies of insurance that may offer coverage.

In-House Legal Counsel

Upon notice of a data security 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 CISO and Privacy Officer to determine notification requirements, timeline and implementation plan;
- Review contracts with vendors, customers and business partners to determine if there is a contractual obligation to notify such vendors, customers, business partners or others.

Crisis Management / Public Relations

Upon notice of a data security incident, the CIO should notify crisis management/public relations. Since the timing and posture of any announcement related to a data breach can have significant business ramifications, in-house legal counsel, with the advice of outside legal counsel, should be involved in deciding when, where and how any announcement should be made. Since this is a difficult aspect of the data breach response and every situation will be different, carefully consider all the issues and obtain input from other IRT members. Consider retaining an outside firm that specializes in crisis communications to handle external communications.

Customer Service

Customer service staff needs to prepare for handling incoming calls from customers affected (or potentially affected) by the breach. Customer service staff will answer questions, explain how to enroll in credit monitoring or identity theft management programs, if offered, and similar issues. With a large volume breach, consider engaging a call center with a dedicated hotline or provide a website that answers FAQs and provides information on fraud and identity theft protection instead of using call center services.

Notification / Fulfillment House Vendor

Upon notice of a Threat Level 3 data security incident (see threat level definitions below), the CIO should notify the Notification Vendor and internal marketing resources with instructions to coordinate the delivery of logos and other materials that the notification vendor will need if it is determined that written notification will be required.

Threat Levels

Level 1. A data security incident is defined as a “Level 1” threat if it can be determined that no mission critical systems or resources are at risk, and no confidential information or PI have been accessed.

Level 2. A data security incident is defined as a “Level 2” threat if mission critical systems or resources may be at risk, or if confidential information or PI may have been accessed.

Level 3. A data security incident is defined as a “Level 3” threat if mission critical systems or resources are at risk, or after determination that confidential information or PI was, in fact, accessed by an unauthorized individual.

Legal Incidents

Legal incidents are attacks directly against the organization or a vulnerability that can be exploited. They include situations where state or federal law enforcement agents are involved. This may include, but is not limited to, agents entering a building with a warrant and confiscating hardware that has been involved in a data security incident. In the event of a legal incident:

- Notify in-house counsel immediately and
- Notify the IRT as soon as possible.

Procedures for Responding to Incidents

Preparation

Being prepared to respond to a data security incident before it occurs is critical. This advanced preparation avoids disorganized and confused responses to incidents. It also limits the potential for damage by ensuring that response plans are familiar to all staff, thus making coordination easier.
All workforce members should be trained to report any suspected data security incident to their respective Information Security Liaison who will, in turn, notify the CISO. The CISO will activate the IRT unless the CISO can evaluate and deny the threat without help from the IRT.

We have planned for emergency communications needs. Should an incident adversely affect regular communication channels, the IRT member list provides home telephone numbers, mobile telephone and pager numbers.

Appropriate training will be provided to all IRT members and other appropriate staff on a regular basis. Training helps update their knowledge and skills in handling data security incidents. Workforce members will be trained to identify incidents and report them to their department Information Security Liaison.

Incident Response

There are five (5) stages of response relating to a data security incident:

1. Discovery & Reporting;
2. IRT Investigation;
3. Responding to the Incident;
4. Containment, Restoration, Recovery; and
5. Post Incident Review & Follow-up.

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

Flow Chart

The accompanying Incident Response Plan Flow Chart can be used to guide the IRT through all 5 stages of the incident response. Flexibility is important since circumstances will vary from incident to incident.

Immediate Response to Incident – 9 Steps

The following steps should be followed in the case of an actual or potential information security breach, including: (a) all losses or disclosures of confidential or sensitive information, (b) all information security violations and problems, (c) all suspected information security problems, vulnerabilities, and incidents, (d) any damage to or loss of Company computer hardware, software, or information that has been entrusted to their care.

Step 1. Do not panic! Do not turn off or reboot any systems. Take notes (date; time; who discovered; what tripped the alarm);

Step 2. Report the incident to: (A) designated person per Company policy; (B) a member of the Incident Response Team;

Step 3. Initiate the Security Incident Report Form;

Step 4. The Incident Response Team should confirm the incident and inform senior management;

Step 5. Submit Insurance Claim & Engage Legal Counsel

Step 6. After confirmation, secure the scene. Do not allow anyone to take any action on affected systems;

Step 7. Identify the systems, applications, and data (type & classification) compromised then, backup affected systems to allow future analysis of the system, including any forensic analysis needed;

Step 8. Determine if security of sensitive data was breached and, if so, what data elements were included (e.g. name, age, DOB, SSN, medical information); and,

Step 9. Preserve and protect the evidence.

Annual Review and Updates

Every 12 months the CISO will review how well the organization has responded to data security incidents and provide a written report to the IRT. The report will respond to the following questions:

- 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 data security 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?

After comment from the IRT, the CIO will revise this data incident response plan and, as needed, all (a) security policies and procedures, (b) administrative, physical, or technical safeguards, and (c) all training programs in light of experience.

Conclusion

This data security incident response plan provides reasonable methods for limiting the possibility of an adverse effect on the organization due to the occurrence of a data security incident, and for facilitating the rapid and successful recovery from an incident, should one occur.

Appendix A: Glossary of Terms

Confidential Information

Confidential information shall be broadly interpreted to include non-public information that is owned by the employer organization and is intended to remain confidential or proprietary, including trade secrets, financial information, business plans, marketing strategies, etc.

Denial of Service (DoS) Attack

A DoS attack is normally an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to interrupt or suspend services of a host connected to the Internet.

Encryption

Using encryption renders information unintelligible in a manner that allows the information to be decrypted into its original form - the process of transforming plaintext into cipher text.

Event

Any observable occurrence in a computer system or network, e.g., the system boot sequence, port scan, a system crash, or packet flooding within a network. Events sometimes provide an indication that an incident is occurring, although not necessarily.

Firewall

Used to control access to or from a protected network. Enforces a network access policy by forcing connections to pass through this system, where they can be examined and evaluated. The system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnets.

Integrity

(1) A sub-goal of computer security which pertains to ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations.

(2) A sub-goal of computer security which pertains to ensuring that information retains its original level of accuracy. Data integrity is that attribute of data relating to the preservation of:

a) its meaning and completeness,

b) the consistency of its representation(s), and

c) correspondence to what it represents.

Intrusion

Unauthorized access to a system or network

Malicious Code Attacks

Include attacks by programs such as viruses, Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity.

Misuse

Misuse occurs when someone uses data for other than official or authorized purposes.

Personal Information

Personal Information (PI) may include a person’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account.

In some jurisdictions, a user name or email address, in combination with a password or security question and answer that would permit access to an online account, may also be considered personal information under the law.

Unauthorized access

Unauthorized access encompasses a range of incidents from taking paper records, disposing of paper or electronic records or file, improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories possibly by obtaining "super-user" privileges. Unauthorized access also includes access to network data gained by planting an unauthorized "sniffer" program (or some such device) to capture all packets traversing the network at a particular point.

Vulnerability

A weakness in an information system, cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.