|  |  |  |  |
| --- | --- | --- | --- |
| **Title:** | Incident Response Plan | Date: |  |
| **Version:** | 1.0 |

# A. Purpose

The <Company> Information Security Incident Response Plan provides the consistent framework for <Company> to respond to a security event. This plan will serve as an enterprise-wide guide to facilitate a response in a systematic manner to security events and is designed to (a) prevent or minimize disruption of critical information systems; (b) minimize loss or theft of sensitive or critical information; and (c) quickly and efficiently remediate and recover from security events.

The use of the Information Security Incident Response Plan is mandatory for all employees, partners, and information processing components of <Company>, all computer networks and systems owned or operated by <Company>, and all systems or networks connected to the <Company> information technology infrastructure under the control of business or strategic partners.

# B. Audience

The following is the audience for the <Company> Security Incident Response Plan (Appendix A contains a list and contact information for current members):

* Information Security
* Incident Response Team (IRT)
* Human Resources
* Legal Department
* Corporate Communications / Media Relations
* Fraud Prevention Services
* Risk Management

# C. Terminology

| **Term** | **Definition** |
| --- | --- |
| Event | An “Event” is any observable or reported occurrence that a preliminary investigation indicates has a sufficient potential for adverse impact on the confidentiality, availability, or integrity of <Company>’s information technology or data, whether it is in paper or electronic form. Events include those that occur in departments other than IT, including HR, Accounting, Marketing, etc. |
| Incident Response Team (IRT) | The IRT or “Incident Response Team” is responsible for responding to Events, ensuring successful resolution, tracking Events, and advising Information Security on proactive measures to prevent future incidents. |

# D. References/Related Documents

| Title | Location |
| --- | --- |
| Incident Report Form 1.0 | <Company> Shared Drive |

# E. Information Security Incident Response Preparation

Information Security should develop incident response capabilities through the following:

## 1). Identifying service providers that may support <Company>’s efforts to detect and respond to an Event (e.g. external legal counsel, forensic investigation providers, crisis communication firms, call center and mailing vendor)(*see* Appendix B for a list of service providers approved by <Company>’s cyber insurance carrier to consider); and

## 2). Evaluating opportunities to procure incident response resources (e.g. hardware, software, storage media) that may be useful in responding to an Event.

# F. Information Security Incident Response Process

Upon classification of a scenario as an Event, Information Security shall initiate the following process to verify, investigate, contain, and remediate the Event. Because Events will vary, usage of the process may vary and certain steps in the process may not apply to all Events.

## Identification & Assessment

## a. When Information Security learns an Event may have occurred, Information Security shall:

## (i) Conduct initial analysis and validation to determine if the report represents an actual Event; and

## (ii) Based on initial analysis of the scope, nature, and potential impact of a verified Event, prepare initial prioritized approach for organizing and assembling an appropriate Incident Response Team. Response priority should consider current and future impact on technology and resources.

## b. The following threat classifications should be used to assist in the initial classification and validation of a potential security incident:

**Level 1.** A “Level 1” Event exists when the initial information shows a low severity and low likelihood of potential impact on core business functions, systems, or sensitive personal information. Examples may include attempted systematic web site or network perimeter probes, commodity malware infections, or unexplained system malfunctions of user workstations or other non-core production devices.

**Level 2.** A “Level 2” Escalated Event exists when the initial information indicates a potential impact to key business functions, systems, or sensitive personal information. Examples may include a lost unencrypted laptop believed to contain <Company> or customer data, a common point of purchase report related to payment card data, potential unauthorized access to elevated network administrator credentials, or unexplained malfunctions of security appliances.

**Level 3.** A “Level 3” Critical Event exists when the initial information shows a high likelihood of or confirmed unauthorized access to critical systems or access or acquisition of sensitive information. Examples include reports from third parties of confirmed theft of Social Security numbers or payment card data, cyber-extortion demands, or unexplained outbound data flow.

c. Forming the Incident Response Team:

(i) The team must include representatives from Information Security and Legal;

(ii) As appropriate, the team may also include: HR, Internal Infrastructure, Fraud Team, Executive Management Team, external counsel, and others as needed and depending on the nature of the event.

(iii) An Event Manager shall be appointed to lead the response to the Event. The Event Manager will have the following responsibilities: (1) coordinating the activities of the Incident Response Team; (2) reporting on status of Event response to executive management as appropriate; (3) identifying when additional resources are needed for the Incident Response Team; and (4) ensuring that the Incident Response Team strategy is carried out.

(iv) Incident Response Team members are expected to devote appropriate time to the response. Internal departments will be expected to supply the necessary resources.

(v) Legal will maintain a list of the members of the Incident Response Team. All members of the Incident Response Team must receive the Incident Response Team Member instructions form from Legal upon joining the team, which should, among other things as appropriate, advise members to preserve information related to the Event and not to share details with anyone outside of the team unless doing so is explicitly approved by Information Security and Legal. After obtaining approval to share information, the amount of information shared should be limited to the information necessary to accomplish the task.

(vi) The Event Manager should assign a name to the Event (e.g. “Project Orange”) and initiate the Event tracking process. All subsequent written communications concerning the Event shall include “Attorney-Client Privileged Communication – Project \_\_\_\_\_” in the Subject line and be limited to fact-based information necessary for the Event response. Depending on the nature of the Event, consideration should be given to using out-of-band communication to avoid interception by any unauthorized person who may have system access.

d. Prepare a preliminary containment plan based on appropriate considerations, including: (1) The potential scope of the Event; and (2) the potential impact/risk of the Event on <Company>’s systems or data. Additional considerations and guidelines are contained in Appendix C.

### e. Consider preparing a brief, fact-based summary of what is believed to have occurred to the attention of the Incident Response Team Legal representative with copies to appropriate Incident Response Team members.

### f. Develop a process to preserve evidence, including: (1) impacted devices, servers, etc.; (2) relevant logs; and (3) timeline of the Event and response actions taken.

## Containment, Eradication, & Recovery

a. Upon formation of the Incident Response Team, the team should develop a plan to contain the Event based on the following considerations where appropriate:

(i) potential damage to or loss of resources or data;

(ii) the need for forensic analysis of the root cause;

(iii) the need for preservation of evidence;

(iv) time and resources necessary to enact the containment plan; and

(v) the projected effectiveness of the plan.

b. When an Event has been contained, the Incident Response Team should develop a recovery plan to eliminate effects of the Event and return assets and business processes to an operational state based on the following considerations, where appropriate:

(i) eradication work that was completed during the containment phase;

(ii) a determination of the overall impact of the recovery plan and the “next steps” necessary to enact the plan;

(iii) necessary internal resources and communications to form and accomplish the plan;

(iv) necessary external resources to accomplish the plan; and

(v) the impact of the plan on the ability to investigate the Event.

## Communication & Notification

### Development of the communication plan should consider the following:

### (i) State, federal, and international regulatory obligations, such as state breach notification laws and SEC disclosure requirements; and

### (ii) contractual notice obligations, such as card networks.

### Legal is responsible for the development of, and must approve all communications to parties outside of the <Company> organization. Legal may involve Corporate Communication in developing appropriate communications. A notification checklist is contained in Appendix D.

## Special Considerations

### a. If personal information of individuals (e.g. a person’s name associated with a SSN, driver’s license number, passport, national identification number, bank account, credit card or username/password), may be involved in the Event, Legal should be notified immediately so they may:

### (i) begin to assess whether there are any US or international law notification obligations; and

(ii) the timing of any required or recommended notification.

### b. If payment card data may be involved in the Event, assess notification obligations. Credit card associations have specific requirements for reporting and investigating potential account data compromise events, evidence preservation, reporting security incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of detecting the incident. Applicable guidance from Visa and MasterCard may be found at:

<http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html>

<http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf>

### c. If an internal user (authorized or unauthorized associate, contractor, consultant, etc.) is suspected to have been involved in the Incident, notify Human Resources.

### d. Credit Monitoring—Legal will determine if credit monitoring is appropriate.

e. Risk Management will coordinate with the insurance broker and carrier to maximize insurance coverage under <Company>’s cyber insurance policy.

## Final Steps

Following a security incident, <Company> should consider the following:

• Analyzing the root causes of event

• Remedial measures taken

• Lessons learned

• Whether revisions to this policy should be made

• Whether policies and processes should be modified to meet new or different risks

# 6. Revision History

| **Date** | **Version** | **Name** | **Description of Change** |
| --- | --- | --- | --- |
| 1/1/2015 | 1.0 | <Company>’s Incident Response Plan | Initial Incident Response Plan |
|  |  |  |  |

**APPENDIX A**

**INCIDENT RESPONSE TEAM MEMBERS & CONTACT INFORMATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title | Name | Office Phone | Alternate Phone | E-mail |
| **Chief Information Officer** |  |  |  |  |
| **Chief Security Officer** |  |  |  |  |
| **IT Systems** |  |  |  |  |
| **Corporate Communications** |  |  |  |  |
| **General Counsel** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**APPENDIX B**

**INCIDENT RESPONSE SERVICE PROVIDERS**

**Forensic Investigation**

Forensic Investigation Inc.  
<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

**Crisis Communications**

Crisis Communications Inc.

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

**Mailing/Call Center/Credit Monitoring**

Mailing, Inc.

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

Call Center Inc.

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

Credit Monitoring Inc.

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

**Legal**

Law Firm

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

**Law Enforcement**

Local Law Enforcement

<Address 1>

<Address 2>

Contact Name: <Contact Name>

Phone No.: (555) 555-5555

**APPENDIX C**

**ADDITIONAL GUIDELINES/CONSIDERATIONS**

1. Don't panic. Be as calm and methodical as you can, and think about your course of action. Involve a second person to assist and observe all actions you take.

2. Do a quick assessment. Do not immediately shut down the machine, as you may lose important information that resides only in system memory. Consider disconnecting it from the network but leaving the power on.

3. Report the problem. Call the <IR Team> at <Contact Phone Number>. Alternatively, you can send a message (using a different PC) to <IR Email Address>.

4. Gather and preserve all relevant information. This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs. Copy them to a safe location (that will not be deleted or over-written), so that you can study them later.

5. Take notes. Record key **factual** events, including things you observed, actions you took, dates and times, and the like. It is best to log your activities as they occur. Over time, your actions and the order in which they were executed may not be easily remembered.

**APPENDIX D**

**Notification Checklist**

* Consider internal and/or external forensics analysis. Engage forensic firm through legal counsel.
* Determine the universe of affected individuals and the data elements for those affected individuals. Identify minors, deceased, U.S. residents, Canadian residents, persons residing outside of the U.S. or Canada.
* Analyze the data elements to determine if notification is required under federal and state laws.
* Determine if we should involve law enforcement.
* Determine which regulators, if any, need to be notified.
* Determine if a crisis management firm needs to be engaged (consider sensitivity of data, number of people involved, etc.).
* Prepare and continue to update a media hold statement or press release in conjunction with client’s PR team (and possibly a crisis management firm—engage crisis management firm through legal counsel).
* Determine if notification vendor (for mailing and operating a call center) is to be used.
* Assess if credit monitoring should be offered and to whom (minors and adults)
* If mailing will occur, prepare a spreadsheet of affected individual with name, address, and possibly nature of data elements. Identify minors, deceased, U.S. residents, Canadian residents, persons residing outside of the U.S. or Canada.
* Prepare notification letter(s) based on type of person affected (customer, employee, etc.) and data elements (name, SSN, DOB, payment card, etc.).
* For mailing, send logo (.jpeg), signature (.jpeg), address list of affected persons to notification vendor.
* If mailing and offering credit monitoring, purchase codes from credit monitoring provider.
* Prepare FAQs for call center.
* Prepare any regulatory letters (AG notices, state offices, CRAs, if there are other states involved).
* Receive and approve proofs of letters from notification vendor.
* Prepare internal communications to board, leaders, and employees.
* Prepare website posting and in-store notices if necessary.
* Determine if substitute notice is necessary (typically email, website posting, and media notice).
* Establish call center escalation process.
* Print and mail letters.
* Ongoing media relations, as needed.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.