

**IT INCIDENT RESPONSE PLAN**

This plan provides a consistent framework to prepare for, respond to, and remediate a potential or confirmed incident. It will help prevent or minimize disruption of critical information systems, minimize unauthorized access, and meet legal requirements.

13 Pages 20-1243



**IT Incident Response Plan**

1. **Purpose**

The [ORG] Incident Response Plan (“IRP”) provides a consistent framework for [ORG] to prepare for, respond to, and remediate a potential or confirmed Incident (as defined in Section 2). To facilitate a response in a systematic manner to Incidents, the IRP is designed to (a) prevent or minimize disruption of critical information systems; (b) minimize unauthorized access, loss or theft of Personal Information and proprietary information; (c) quickly and efficiently remediate and recover from Incidents; and (d) meet any potential legal obligations that may apply to a particular Incident.

1. **Definitions**

| **Term** | **Definition** |
| --- | --- |
| Information Security Event | An occurrence indicating a possible compromise of security policies or a failure of controls that may impact [ORG] data or operations. Please note that every potential incident reported is initially considered an Information Security Event and must be designated an Incident by the IRT Leader and IT Security Team.  |
| Incident | One or more Information Security Event(s) or other observable or reported occurrence that a preliminary investigation indicates (i) may compromise the integrity, operation or security of [ORG]’s assets or environments or vendor assets or environments that impact [ORG] data or operations; or (ii) may involve unauthorized access or acquisition of Confidential Information maintained by or for [ORG]. The occurrence may affect only internal systems, third-parties, or both.  |
| Personal Information | Any information that can be linked to an identified or identifiable person. Such information may include: name, phone number, email address, IP addresses, user name, login name or handle, passwords (clear text or hashed), date of birth, digitized or electronic signatures, and biometric data (such as electronic fingerprint or retinal scans), as well as any other categories of personal information that [ORG] determines may be covered by applicable data breach notice laws or other data breach notice requirements (e.g., contractual, or PCI rules). The term "Personal Information" also covers certain categories of "sensitive" Personal Information that often receive additional protections and/or may be subject to additional restrictions under privacy laws. Such data may include (generally in conjunction with first and last name):• Social security number (or non-US equivalent);• Financial account numbers, and credit or debit card numbers (with or without any required security code, access code, personal identification number or password);• Health information, including any information, that relates to: (i) the past, present, or future physical or mental health or condition of an individual, (ii) the provision of health care to an individual, or (iii) the past, present, or future payment for the provision of health care to an individual;• Driver's license or passport number• Taxpayer number• Digital signature • Mother's maiden name • User name / Password• Criminal history or background• Race or ethnic origin• Religion• Information about gender or sexual orientation• Political affiliation• Trade union membership.Note, however, the definition of “Personal Information” is subject to state notification laws and, therefore, the definition could include additional categories of information. Legal should be immediately notified if any Personal Information or information that might be sensitive may be involved in an Incident.  |
| Protected Proprietary Information | Sensitive company data, such as non-public financial information, research and development of new products, unannounced strategic or marketing plans, [ORG] technical policies and procedures, system configurations, physical security details, personnel records, agency or policy lists, [ORG] handbooks, manuals or guidelines, trade secrets, and sensitive company correspondence. |
| Confidential Information | Any information not generally known to the public that is related to [ORG]’s business, and generally encompasses both “Personal Information” about [ORG]’s customers and employees and “Protected Proprietary Information.” For additional guidance on these definitions, consult the [ORG] Privacy Program Manual. Legal should be consulted immediately with any concerns or questions regarding information that may be Confidential.  |

1. **Plan**

The IRP applies to Incidents involving any computing devices, network environments, and account credentials owned or used by [ORG] or any of its service providers and vendors that access, process, transfer, or store Personal Information or Protected Proprietary Information, as well as Incidents involving physical documents containing Personal Information or Protected Proprietary Information. The IRP is to be used by the Incident Response Team (“IRT”), employees, contractors, and partners, and in conjunction with any third party breach response provider (e.g., external legal counsel, forensics provider, or other service providers), during and throughout the lifecycle of an Incident.

This IRP is not intended to address availability, normal outages, or issues such as hardware failure arising from non-security related events.

**3.1 Incident Response Organizational Structure**

The IRT has the responsibility for coordinating [ORG]’s Incident response efforts, which at a minimum consists of a representative from the IT Security Team and Legal. Additional support might be required from Human Capital, Infrastructure, the Technology Service Center (“TSC”), Corporate Communications, Compliance, IT Management, and Audit departments. Not every Incident will require all IRT members, and the composition of the IRT in a particular situation will depend on the factual circumstances of the Incident.

The Incident Response Team Leader (“IRT Leader”) and IT Security Team will determine the composition of the IRT based on the type, priority, and severity of an Incident. The Cybersecurity Manager will serve as the IRT Leader at the outset of an incident. However, there may be Incidents where two individuals serve as co-IRT Leaders or where the IRT Leader changes during the Incident based on circumstances, availability, and other factors.

The current structure of the IRT is set out below and will be updated periodically based on need and possible personnel changes. The main point of contact for the IRT will be the Cybersecurity Manager as the IRT Leader. If the Cybersecurity Manager / IRT Leader is unavailable, please reach out to [name], Senior Infrastructure Manager.

| **IRT Members and Title** | **Role** | **Responsibility** |
| --- | --- | --- |
| Senior Manager, Cyber and Risk Management | IRT Leader / Co-IR Coordinator | * Coordinate the activities of the IRT
* Report on status of Incident Response to executive management as appropriate;
* Identify when additional resources (internal and external) are needed for the IRT
* Ensure that the IRT strategy is carried out.
 |
| Shared by IRT Leader and Infrastructure Head | IRT Coordinator | * Coordinate meetings
* Track individual and departmental responsibilities and action-items to ensure progress and completion
* Assist with appropriate documentation of the Incident Response, and any other administrative and project management tasks necessary to support the IRT Leader and the IRT.
 |
| [name] title | Infrastructure Head/Co-IR Coordinator | * Provides review of IRT recommendations, evidence and activities.
* Will act as backup IRT Leader, in case the Cybersecurity Manager if unavailable.
 |
| [name] title | IT Management | * Provides review of IRT recommendations, evidence and activities.
 |
| [name] title  |
| [name] title  |
| [name] title | Legal  | * Provides legal advice to IRT and legal guidance for the Incident Response.
 |
| [name] title | Compliance | * Provides compliance advice and support to the IRT.
 |
| [name] title | Communications | * Provides internal and external communications for the Incident Response.
 |
| [name] title | Human Capital | * Provides review of IRT recommendations, evidence and activities; particularly if Human Capital systems or data are at risk.
 |
| [name] title | Audit | * Provides review of IRT recommendations, evidence and activities.
 |
| [name] title | Investor Relations | * Provides review of IRT recommendations, evidence and activities.
 |

The following is a list of activities to be undertaken by the IRT in support of its mission:

|  |  |
| --- | --- |
| **Activity** | **IRT Member Responsibility** |
| Determine the nature and scope of Incidents  | SERVICE OPS during intake of Information Security Event and then IRT Leader and the IT Security Team |
| Determine resources necessary to aid in Incident Response | IRT Leader; IR Coordinator |
| Coordinate Incident Response efforts | IR Coordinator |
| Oversee evidence gathering and preservation, chain of custody, and application and maintenance of attorney-client privilege | IRT Leader; Legal |
| Assess and escalate Incidents to Incident Response Service Providers (Cybersecurity Insurer and breach response provider) as appropriate | IR Coordinator; IT Management; Legal |
| Interface with other departments and locations | IR Coordinator; IT Management |
| Monitor and report on the progress of investigations to management | IR Coordinator; IT Management |
| Notify affected individuals and the appropriate authorities, as necessary and within appropriate timeframes | IRT Leader; Legal |
| Organize and participate in Post-Incident / Lessons Learned meetings, as appropriate | IR Coordinator |

**3.2 Incident Response Process**

The National Institute for Standards and Technology (“NIST”) recognizes four phases for the security handling lifecycle. This IRP has been developed to align with this framework.



Figure 1: NIST Incident Response Lifecycle

The IRT shall initiate the following general process to prepare for, identify, verify, investigate, contain, and remediate an Incident. Usage of the process may vary and certain steps in the process might not apply to all Incidents.

1. **Preparation**: Review and update IRP. Develop response capabilities. Test response plan through tabletops and training. Promote awareness of plan.
2. **Detection & Analysis**: Initial Incident detection, triage and escalation to appropriate stakeholders. Formation of appropriate response team. Determine need to notify external parties. Conduct analysis necessary to properly prioritize response activities, including resource needs. Form communication and containment action plans. Assess preservation and mitigation needs.
3. **Containment, Eradication, & Recover:** Take Incident specific actions to stop the Incident and / or contain its impact. Determine and eliminate the cause of the Incident (while preserving evidence needed for next steps). Repair any unauthorized changes. Finalize mitigation of Incident and restore system to normal operational state and implement any measures to prevent Incident reoccurrence.
4. **Post-Incident**: Analyze plan effectiveness and areas for enhancing response and security measures to minimize the likelihood of future Incident(s) and continually optimize response preparedness.

**3.3 Incident Classification**

For purposes of this IRP, if an Information Security Event is designated as an Incident by the IT Security Team, Incidents will then be classified by priority level based on magnitude of the potential impact to [ORG]’s operations, potential compromise of Confidential Information, potential legal or regulatory implications for [ORG], potential effect on [ORG]’s customers and partners, and [ORG]’s ability to recover from the Incident.

The IT Security Team is responsible for reporting, detecting, assessing, and classifying Incidents after the initial reporting of an Information Security Event to TSC. The IT Security Team is responsible for determining if Information Security Events should be classified as Incidents. Once an Information Security Event has been classified as an Incident, the IT Security Team is then responsible for determining the initial classification of such Incident.

The IT Security Team assigns a risk classification at the initial assessment based on the criteria set out in the table below. At appropriate times throughout the response, the risk classification and potential impact of the Incident may change as more information is learned about the Incident.

| **Priority Level** | **Definition** | **Examples** |
| --- | --- | --- |
| Critical | An Information Security Event designated as an Incident that will cause the disruption of business activities due to loss of business-critical applications, infrastructure, or network availability for more than one [ORG] site; or where the initial information shows a high likelihood of, or confirmed, unauthorized access to critical systems, Personal Information or Protected Proprietary Information.  | Examples of Critical priority security incidents are:* Confirmed unauthorized access to sustainability, financial or manufacturing control systems (hacking; cyber-extortion threat[[1]](#footnote-1)).
* Intentional flooding of website/servers to prevent use of resource (denial of service attack).
* Malware Epidemic (ransomware) which impacts sustainability, financial, manufacturing control systems and/or organizational resources who manage or operate said systems.
* Financial or material impact to [ORG] daily operations.
 |
| High | An Information Security Event designated as an Incident that has a moderate likelihood to cause the disruption of business activities due to loss of business-critical applications, infrastructure, or network availability for more than one [ORG] site; or where initial information indicates potential unauthorized access to, or acquisition of, Personal Information or Proprietary Company Information.  |

|  |
| --- |
| Examples of High priority security incidents are: * Breach of Personal Information (credentials) which grant access to unauthorized actors.
* Loss of confidential or Protected Proprietary Information (industrial designs, industrial secrets, trade secrets, etc.).
* Loss of operation at minimum of one plant or port where a remote resolution is not possible.
* Suspected fraudulent attempts to change or influence sustainability or financial information
 |

 |
| Medium  | An Information Security Event designated as an Incident that minimally affects business activities due to loss of applications, infrastructure, or network availability to one [ORG] site or user; or where initial information indicates a low likelihood of potential impact on Personal Information or Proprietary Company Information.  | Examples of Medium priority Incidents are:* Commodity malware infections, unexplained malfunctions on user workstations or other non-critical systems.
* Loss of encrypted portable device.
 |
| Low | An Information Security Event designated as an Incident that has no significant business impact.  | Examples of Low priority Incidents are: * Loss of localized services on PC.
* Spear Phishing emails that are detected and not acted upon by the affected individual.
* Attempted systematic website or perimeter probes.
 |

**3.4 Preparation**

To work to address evolving risks, the IRT will consider how to develop and enhance response capabilities through the following:

* Identifying service providers that may support [ORG]’s efforts to detect and respond to an Incident (e.g., external legal counsel, forensic investigation providers, crisis communication firms, call center and mailing vendor; breach response providers);
* Evaluating opportunities to procure incident response resources (e.g. logging tools, storage media, and personnel) that may be useful in responding to an Incident;
* Maintaining network diagrams, lists of critical systems, and clean images and code;
* Conducting tabletop exercises;
* Implementing personnel awareness and training; and
* Reviewing this plan annually and in the event of material changes to other internal plans.

**3.5 Detection and Initial Reporting**

When a person suspects an Information Security Event (i.e.: breach of their corporate email account, malware infection, loss of a laptop containing access to Personal Information or Protected Proprietary Information, or other type of Information Security Event), that person should notify SERVICE OPS immediately. The table below outlines the actions to follow. Based on the initial report given to the IT Security Team by TSC, a member of the IT Security Team will provide instruction to SERVICE OPS on whether the report should be documented as a normal SERVICE OPS ticket, documented using the form the IRT uses for managing Information Security Events, or documented in a secure location designated by the IRT for High and Critical Incidents.

|  |  |
| --- | --- |
| Step | Action |
| 1 | Notify the SERVICE OPS at [ORG] |
| 2 | The SERVICE OPS representative receiving the report records the details of the Information Security Event in the ITSM platform and notifies the IT Security team by phone. |
| 3 | The SERVICE OPS representative should treat the Information Security Event as a confidential matter. |

**3.6 Incident Intake Process Steps**

Once the IT Security Team representative has collected and captured all required information, the IRT will manage the response according to this policy as well as related information security policies, procedures, insurance agreement, and standards.

**3.7 Validation and Analysis**

For Low Incidents, the IRT will not be immediately notified. The IT Security team will independently execute response measures based on their information security policies, standards, and procedures. If a Low Incident changes to Medium or higher during the IT Security Team’s review, the IT Security Team will notify the IRT Leader immediately.

When an Incident is initially designated as Medium or higher, the IT Security Team shall immediately notify the IRT Leader and both shall perform another validation to confirm that the initial classification of the Incident was accurate. Legal will also be notified for Incidents classified as Medium or higher. After validating, the IT Security Team and IRT Leader should:

* For Critical Incidents, consider preparing a brief, fact-based summary of what is believed to have occurred to the attention of the IRT Legal representative (expressly requesting legal advice) copying appropriate IRT members. See **Appendix C** for the Incident Response Form for use with High and Critical Incidents.
* For Critical Incidents, follow the IRP in conjunction with the Communication Department’s Crisis Protocol. For Critical Incidents that involve the potential or actual unavailability of information systems that support critical business operations: follow the IRP, determine if a business continuity plan(s) exists for the effected departments, and, implement the general guidelines that the IT Security Team has developed for addressing security incidents.
* For Incidents preliminarily classified as High or Critical priority Incidents, all available members of the IRT should be assembled for an initial meeting.
* For Medium Incidents, the IRT Leader should be engaged by the IT Security Team to assess whether the Incident is truly Medium or whether a High or Critical prioritization should be assigned to the Incident.
* For Medium or Low Incidents, only select IRT members will assemble as identified by the IRT Leader. Medium or Low Incidents do not require the full IRT.
* At all times, the IT Security Team will maintain logs that will be provided to and reviewed by the members of the IRT upon request.

During the initial IRT meeting and any subsequent IRT meetings, the IRT should consider the following:

* Focus on analyzing the scope, nature, and potential impact of the Incident. Begin to assess whether personal information may be affected.
* Confirm the prioritization level of the Incident based upon the guidelines identified in Section 3.4.
* Decide if notice to current cybersecurity insurer, if any, should or must be provided and the timing of the notice.
* Determine whether outside legal counsel may need to be engaged (conferring with insurer for approved providers, where applicable).
* Determine whether any third party service providers need to be engaged (e.g., forensics provider, PR / communications providers, call center providers) and engage under privilege (conferring with insurer for approved providers, where applicable).
* IRT members should take steps to conduct Incident investigations under attorney-client privilege.
* Prepare a preliminary containment plan based on appropriate considerations, including: (i) the potential scope of the Incident, and (ii) the potential impact/risk of the Incident on [ORG]’s systems, business operations or personal and proprietary data. Often, for technical security incidents, consultation with external legal firm and/or a breach response provider, may be warranted before implementing a containment plan.
* For Incidents that involve the potential or actual unavailability of technology or information systems, develop a strategy for preserving or restoring the availability, and continued operation of the systems involved.
* Identify and organize the appropriate IRT and supporting team members to assist in the response.
* Identify an IRT Leader, if IRT Leader will be different than the Cybersecurity Lead.
* Determine whether and when to obtain assistance from a breach response provider in coordination with the Cybersecurity Insurance provider. Contact information for [ORG]’s Incident Response Service Providers is located at **Appendix A**.
	+ Determine whether to engage any such providers and whether the additional support should be under attorney-client privilege.
* Determine the frequency of IRT meetings.
* Determine the appropriate members of [ORG] management outside of the IRT that should be notified of the Incident.
* Consider whether, when, and to whom to provide threat indicators and whether/when to notify law enforcement (either directly or with the assistance of external legal counsel).
* Consider using out-of-band communication to avoid interception by unauthorized person with system access.
* Document all facts concerning the Incident analysis, the effects of the Incident, and any remedial actions that were or were not taken in an attorney-client privileged report.

The IR Coordinator will maintain a list of the members of the IRT. This list may be used to consider an Incident in conjunction with [ORG]’s insider trading policy. The IRT Leader should assign an identifier to the Incident and work with the IR Coordinator to continue tracking the response to the Incident (see **Appendix C for High and Critical Incidents**). Communications via email and in writing should be limited to the IRT and should be limited to objective / factual information. Subjective observations or concerns should generally not be discussed via email or other non-verbal means.

**3.8 Containment**

Once an Incident has been validated and classified by the IRT, it is vital to contain the Incident as soon as possible to limit the potential impact. The IRT should plan its containment procedures and strategies so as to help coordinate its actions and increase responsiveness during a confirmed Incident. To choose the correct containment strategy, the IRT should consider the following:

|  |  |
| --- | --- |
| **Considerations** | **Responsible IRT Members** |
| What caused the Incident and what measures are necessary to stop the Incident from continuing?  | IRT Leader and IR Coordinator. |
| What is the potential impact to affected resources and business operations?  | IRT Leader; IT Management; Leadership for the affected departments. |
| What evidence is available and has it been preserved? How important is the preservation of evidence?  | IRT Leader; IR Coordinator; Legal. |
| Is it necessary to maintain network and service availability? (e.g., network connectivity, services to partners or external parties)?  | IRT Leader; IR Coordinator; Legal. |
| How much time and effort will be needed to implement the containment strategy?  | IRT Leader; IR Coordinator; Managed Service Provider if applicable. |
| How effective is the containment strategy? Does it partially or fully contain the incident?  | IRT Leader; IR Coordinator; Managed Service Provider if applicable. |
| How long will the strategy be effective? Is it temporary or permanent?  | IRT Leader; IR Coordinator; Managed Service Provider if applicable. |

**3.9 Eradication and Recovery**

After an Incident has been contained, the IRT should begin eradication and recovery procedures. During eradication, the root cause of the Incident should be resolved. Solutions implemented as part of the eradication should be designed to solve the underlying problem and prevent the Incident from occurring again. Once the problem has been resolved, the organization should restore normal business functionality as soon as reasonable. This includes reversing damage caused by the security incident and response (e.g., restored lost data from backups, or removal of temporary firewall rules). To confirm that the eradication and recovery has been completed appropriately, assistance of an external forensics / security provider may be needed.

The following steps should be considered during eradication and recovery:

* Plan and execute an eradication strategy to ensure a complete, effective, and efficient removal of the threat(s) and to prevent attackers from launching the same attack (e.g., delete malicious code, disable breached accounts, force account password changes, patch vulnerabilities and correct misconfigurations; add long-term firewall / IPS rules, system / software updates). Eradication actions sometimes impact business operations and would follow standard emergency change and communication policies.
* Remove artifacts left over by the Incident (e.g., extraneous files).
* Determine whether and how to enhance security across the entire organization to prevent similar attacks from exploiting the same vulnerabilities. For example:
	+ Increase password complexity requirements.
	+ Change network segmentation or update firewall rules or ACLs.
	+ Reevaluate patching and vulnerability management tools and processes.
	+ Reconfigure monitoring tools to detect specific anomalies in network and system usage.
	+ Restore systems using clean backups or build images.
	+ Reconnect systems to the network.
	+ Test restored systems and applications to verify full recovery of business functionality.
	+ Enable or improve detection or logging on network systems and firewalls.

**3.10 Communication & Notification**

Should an investigation determine that Personal Information or Protected Proprietary Information is at risk, Legal (with, where appropriate, with assistance of external legal counsel) will address whether notification is required to potentially affected individuals, regulatory authorities or other third parties. When assessing notification obligations and developing the communication plan, the following should be considered:

* If this step has not already been taken, coordinate with the cybersecurity insurer to address insurance coverage under [ORG]’s policies and determine whether a breach response provider is necessary. If so, the breach response provider may assist with the following;
	+ State, federal, and international laws, state department of insurance and financial services notification guidelines and requirements, and SEC regulations regarding material events (noting that certain regulatory obligations impose specific timeframes for issuing notifications);
	+ Whether to notify the FBI, Secret Service, or other law enforcement entities, if such notification has not already occurred;
	+ Communicate to the to the CEO, CFO, General Counsel, and Audit Committee if a Critical level incident occurs and, in particular, if a ransom payment is demanded to resolve/remediate the Incident;
	+ Contractual notice obligations, such as business partners and customers;
	+ If an associate is suspected to have been involved in the Incident or Personal Information about associates may be implicated, notify Human Capital; for a contractor or consultant, contact the [ORG] point of contact;
	+ If public awareness of the Incident is possible and/or a public statement may be needed, contact Corporate Communications;
	+ What internal communications should be made to associates about the Incident; and
	+ In communicating with employees and other internal stakeholders:
		- Limit communications regarding the details of the Incident on a need-to-know basis.
		- Issue a policy statement to employees reminding them of [ORG]’s external communications policies.

Once Legal has decided that a notification is required for potentially affected individuals or third parties, the following notification process will occur involving the following [ORG] groups (generally with assistance of external legal counsel as well as an external service provider):

* The IRT is responsible for the development of communications to parties, internal or external. The IRT will include the CFO to determine if credit monitoring, identity theft resolution, or other services are necessary. Legal will assist with determining legal requirements and review all communications.
* Legal, Corporate Communications, IT, business unit coordinators and other groups as needed, will assess the total impact and exposure, request post-notification support to address inquiries, and prepare a communications timeline for notifying stakeholders and affected individuals or entities.
* If law enforcement notification has not been made or as follow-up engagement with law enforcement, if notification has been made, IT Security will continue work with Legal (and, where appropriate, external legal counsel) to consider contacting law enforcement to determine if notification would impede a criminal investigation. Senior management will be informed prior to contacting law enforcement.
* Legal, Corporate Communications, Human Capital, and IT will work together to notify affected individuals and third parties, as well as prepare responses to external and regulator inquiries.

A notification checklist is contained in **Appendix B**.

**3.11 Post Incident Review**

After an Incident is contained and closed, the IRT should consider the following:

* Analyzing the root cause of the Incident to identify what happened, how it happened, why it happened, and how to prevent the same or a similar Incident.
* Confirm remedial measures were taken.
* Hold a “lessons learned” meeting with all involved parties after a Critical / High priority incident, and periodically after Medium / Low incidents. Some questions that may be addressed during the meeting include:
	+ What information should have been provided to prevent the Incident?
	+ What information should have been provided sooner that could have expedited the containment and remediation process?
	+ Were there any steps or actions taken that might have inhibited the recovery process?
	+ What corrective actions could prevent similar incidents from occurring in the future?
	+ What could the IRT and key stakeholders do differently the next time a similar incident occurs?
	+ What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
* Determining whether revisions to this IRP should be made.
* Determining whether policies and procedures should be modified to meet new or different risks.
* If the Incident involved third-party service providers, review third-party service provider’s compliance with relevant privacy or data security requirements, assess the need for additional or revised contractual provisions, determine if the service provide should indemnify costs related to the Incident, and whether any potential issues need to be addressed.

**3.12 Testing of This Plan**

This IRP should be reviewed annually and tested every 2-3 years. A test consists of, at a minimum, a meeting of the IRT to conduct a table-top exercise, including a review of IRP for any needed revisions or updates based upon lessons learned from the table-top exercise as well as identification of new threats.

**Record of Changes**

| **Date**   | **Revision Number**  | **Description of Change(s)**  | **Name(s) of Reviser(s)**  | **Status**   | **Approved by**  |
| --- | --- | --- | --- | --- | --- |

**APPENDIX A**

**INCIDENT RESPONSE EMPLOYEES AND SERVICE PROVIDERS**

For reference:

<IT governance documents here>

**APPENDIX B**

**Notification Checklist**

1. Consider internal and / or external forensics analysis. Engage forensic firm through legal counsel.
2. Determine the universe of affected individuals and third parties and the data elements for those affected. Identify minors, deceased, U.S. and non-U.S. residents.
3. Analyze data elements to determine if notification is required under federal and state laws.
4. Determine if law enforcement should be notified.
5. Determine if regulators need to be notified.
6. Prepare and continue to update a media hold statement or press release in conjunction with [ORG]’s Corporate Communications team (and possibly a crisis management firm / engage crisis management firm through legal counsel).
7. Determine if a crisis management firm needs to be engaged.
8. Determine if notification vendor (for mailing and operating a call center) is to be used. Work with vendor to develop response plan (call center FAQ, escalation)
9. Assess if credit monitoring should be offered and to whom.
10. If mailing will occur, prepare an inventory of affected individuals with relevant information necessary to contact.
11. Prepare notification letter(s) based on type of person affected and data elements.
12. Prepare letters for regulators.
13. Prepare internal communications to board, management, and employees.
14. Determine if substitute notice is necessary (email, website posting, and media notice).

**APPENDIX C**

**INCIDENT REPORT FORM**

To assist [ORG]’s Legal Department in providing advice to [ORG] in anticipation of potential litigation or regulatory enforcement actions that may arise from an incident, the below Incident Report Form template tracks the actions of the IRT. The Incident Report should track key facts associated with the response on one document that is updated throughout the investigation and reviewed with [ORG]’s Legal Department. If a row is not applicable, it should not be left blank. Identify as not applicable with a short explanation why.

**ATTORNEY CLIENT PRIVILEGE \*\*\*FOR THE PURPOSE OF LEGAL ADVICE**

**TO: IRT and Legal**

**FROM: IRT Leader**

**RE: [incident name]**

|  |
| --- |
| Incident Name and Number: |
| Date / Time Initiated:Date / Time Completed:  | Date / Time Incident Opened:Date / Time Incident Closed: |
| Action Item | Assigned To | Summary of Steps Taken to Complete | Date Started | Date Completed | Challenges Encountered Completing Action Item | Mitigations | Location of Evidence Stored |
| 1. Activation of Incident Response Team
 |  |  |  |  |  |  |  |
| 1. Open bridge & initial assessment
 |  |  |  |  |  |  |  |
| 1. Engage external service providers
 |  |  |  |  |  |  |  |
| 1. Initial Reporting to IRT
 |  |  |  |  |  |  |  |
| 1. Prepare Initial Coordination Plan
 |  |  |  |  |  |  |  |
| 1. Incident description (e.g. how detected and what occurred)
 |  |  |  |  |  |  |  |
| 1. Description of affected resources
 |  |  |  |  |  |  |  |
| 1. Detection items completed
 |  |  |  |  |  |  |  |
| 1. Analysis items completed
 |  |  |  |  |  |  |  |
| 1. Containment items completed
 |  |  |  |  |  |  |  |
| 1. Eradication items completed
 |  |  |  |  |  |  |  |
| 1. Recovery / remediation items completed
 |  |  |  |  |  |  |  |
| 1. Investigation items completed
 |  |  |  |  |  |  |  |
| 1. Actions taken in IT and cyber defenses to prevent a similar incident again
 |  |  |  |  |  |  |  |

1. Cyber-extortion threats include attempts by a party to: disrupt the network to impair business operations of [ORG]; alter, damage, or destroy data stored on the network; use the network to generate and transmit malware to third parties; deface [ORG]’s website; access or release data, including Personal Information and Proprietary Company Information stored or previously stored on the network; refuse to return data stolen from the network; or prevent access to the network or data by using encryption and withholding the decryption key. [↑](#footnote-ref-1)