Response Plan



Advanced Threat Analytics Implementation Services

Prepared for

[Customer]

6/14/2016

Version Draft

Prepared by

**[Type Author Here]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 7](#_Toc453680712)

[2 How to use this plan 8](#_Toc453680713)

[3 Roles and responsibilities 9](#_Toc453680714)

[4 Security incident response process 12](#_Toc453680715)

[4.1 Assess 13](#_Toc453680716)

[4.1.1 Triage 13](#_Toc453680717)

[4.1.2 Classify 14](#_Toc453680718)

[4.1.3 Major Incidents 18](#_Toc453680719)

[4.2 Prepare 20](#_Toc453680720)

[4.2.1 Prioritize 20](#_Toc453680721)

[4.2.2 RACI 21](#_Toc453680722)

[4.2.3 Scheduling 22](#_Toc453680723)

[4.3 Communicate 23](#_Toc453680724)

[4.3.1 Executive communications and reporting 23](#_Toc453680725)

[4.3.2 Breach declaration 23](#_Toc453680726)

[4.3.3 External communications 24](#_Toc453680727)

[4.3.4 Internal communications 25](#_Toc453680728)

[4.4 Respond 25](#_Toc453680729)

[4.4.1 Investigate 25](#_Toc453680730)

[4.4.2 Containment 29](#_Toc453680731)

[4.4.3 Eradication 30](#_Toc453680732)

[4.4.4 Recovery 32](#_Toc453680733)

[4.5 Close 33](#_Toc453680734)

[4.5.1 Post mortem 33](#_Toc453680735)

[4.5.2 Documentation 34](#_Toc453680736)

[4.5.3 Process improvement 34](#_Toc453680737)

[5 Appendix B: Further Reading 35](#_Toc453680738)

We are very interested in your input!  If you have comments or would like to request an update to this document, please provide your feedback to the [SDM Suggestions alias](mailto:msdmods@microsoft.com).   Attach the document and clearly describe the changes you would like and explain why the changes are needed.

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

Template Guidance

Description:

1. Introduction

**Section Detail:** This section should provide the purpose of this response plan, any initiation guidelines, how to use this plan, detail on the contents of the document and the scope of this documents use.

All members of your IT environment should be aware of what to do in the event of an incident. The Security Incident Response team (SIR) will perform most actions in response to an incident, but all levels of your IT staff should be aware of how to report incidents internally. End users should report suspicious activity to the IT staff directly or through a help desk rather than directly to SIR.

Every team member should review the incident response plan in detail. Having the plan easily accessible to all IT staff will help to ensure that when an incident does occur, the right procedures are followed.

1. How to use this plan

**Section Detail:** This section should contain an explanation of the different levels of incident response in relation to ATA findings and corresponding escalation points. It should also provide detail regarding how this document should be used for each part of the response process.

This document outlines standard operating procedures for how the Security Incident Response team, in conjunction with other operations teams, will respond to events that are detected by the Microsoft Advanced Threat Analytics solution. This document will NOT explain in detail the Security Breach Response procedures and remediation scenarios except occasional contextual references as defined in the scope.

Keep in mind, the steps outlined in this plan are not purely sequential. Rather, they happen throughout the incident. For example, documentation starts at the very beginning and continues throughout the entire life cycle of the incident; communication also happens throughout the entire incident.

Other aspects of the process will work alongside each other. For example, as part of your initial assessment, you will gain an idea of the general nature of the attack. It is important to use this information to contain the damage and minimize risk as soon as possible. If you act quickly, you can help to save time and money, and your organization's reputation.

However, until you understand the type and severity of the compromise in more detail, you will not be able to be truly effective in containing the damage and minimizing the risk. An overzealous response could even cause more damage than the initial attack. By working these steps alongside each other, you will get the best compromise between swift and effective action.

**Note:**It is very important that you thoroughly test your incident response process before an incident occurs. Without thorough testing, you cannot be confident that the measures that you have in place will be effective in responding to incidents. Think of this in a similar manner to your disaster recovery plan. DR plans are often tested to provide faith that a secondary datacenter works in the event of failure. You should test the processes documented within this document in a similar manner. Using tabletop exercises, where you walk through a potential incident, is a very effective way to validate processes and procedures.

1. Roles and responsibilities

**Section Details:** This section is where we will provide a template for the incident response team at the customer and potentially how Microsoft fits into that. Theory is that this section becomes a template which is filled in as a result of the response planning workshop activity.

**Instruction:** Please update the following table to include members from your customer that will be included within each role. This table does not need to list a specific individual. A team name will suffice.

The following table highlights the roles and responsibilities that have been identified as a part of the Security Incident Response process. These roles and responsibilities identify who must be involved and what their responsibilities are during an incident response.

|  |  |  |
| --- | --- | --- |
| **Possible Role Names** | **Responsibilities/Competencies** | **Organizational Members** |
| SECURITY INCIDENT RESPONSE (SIR) TEAM | * Own the incident response * Perform initial security triage/assessment/classification * Provide management overview (communication) * Establish proper communication targets and channels * Coordinate the analyze activities with Ops Teams and SMEs   + Investigate   + Contain   + Eradicate   + Recover * Closure   + Post Mortem   + Documentation   + Process Improvement |  |
| INCIDENT MANAGER  (ASSIGNED BY SIR) | * Execute coordination activities for SIR team * Steward the incident through lifecycle activities * Decision point for SIR team |  |
| COMMUNICATIONS MANAGER | * Owns communication streams for incident response * Interfaces with Managers/Leadership to determine communication targets and channels |  |
| IT / OPERATIONS CONTACT(S) | * Detect possible vulnerability (monitor ATA tool) * Perform initial assessment based on guidance from tool(s) and training * Engage resources who can:   + Further analyze security alerts generated by ATA or other sources   + Triage alerts for validity, scope and security impact * Escalate security incidents to the SIR team, when further security investigation is warranted * Engage key resources from engineering, communications, operations and legal on a need-to-know (NTK) basis to expedite investigation process * Provide assistance to the SIR team in gathering evidence, conducting forensic examination, root cause analysis and accurately revising scope and impact of the incident * Design, prioritize and implement remediation capabilities and plans within the environment and drive process and technical improvements based on incident post mortem recommendations * Own and manage changes to the security-relevant configuration as part of the change management process |  |
| SUBJECT MATTER EXPERTS | Depending on the nature of the incident, the SIR team and operations teams may engage Subject Matter Experts (SMEs) from internal or external organizations for investigative assistance |  |
| LEGAL REPRESENTATIVE | * Legal representation familiar with established incident response policies * Determines how to proceed during an incident with minimal legal liability and maximum ability to prosecute offenders. * Coordinate all communication to outside law enforcement or external investigative agencies   Note: Before an incident occurs, the Legal Representative should have input on monitoring and response policies to ensure that the organization is not being put at legal risk during a cleanup or containment operation. It is very important to consider the legal implications of shutting down a system and potentially violating service level agreements or membership agreements with your customers, or not shutting down a comprised system and being liable for damages caused by attacks launched from that system. |  |
| MANAGEMENT/LEADERSHIP | * Approving and directing security policy * Determining the total impact (both financial and otherwise) of the incident on the organization * Directs the communications owner regarding what information should be disclosed to the media * Determines the level of interaction between legal representation and law enforcement agencies   Note: Depending on the particular incident, you might involve only departmental managers, or managers across the entire organization. The appropriate management individual(s) will vary according to the impact, location, severity, and type of incident. |  |

1. Security incident response process

The security incident response process begins with initial triage to determine validity, scope and impact. Once an issue is determined to be security relevant and has been evaluated for scope, impact and severity, further investigation is warranted. The investigative process, conducted by SIR and the operations team, will gather evidence, conduct forensic analysis and attempt to determine root cause. In addition, the scope, impact and severity will be continuously evaluated throughout the investigation and compliance and privacy impacts will also be determined. The outcome of this investigative process will be an incident classification, followed by prescriptive guidance for follow-on actions based on each type of incident classification. The process can be graphically represented in figure 1 below:

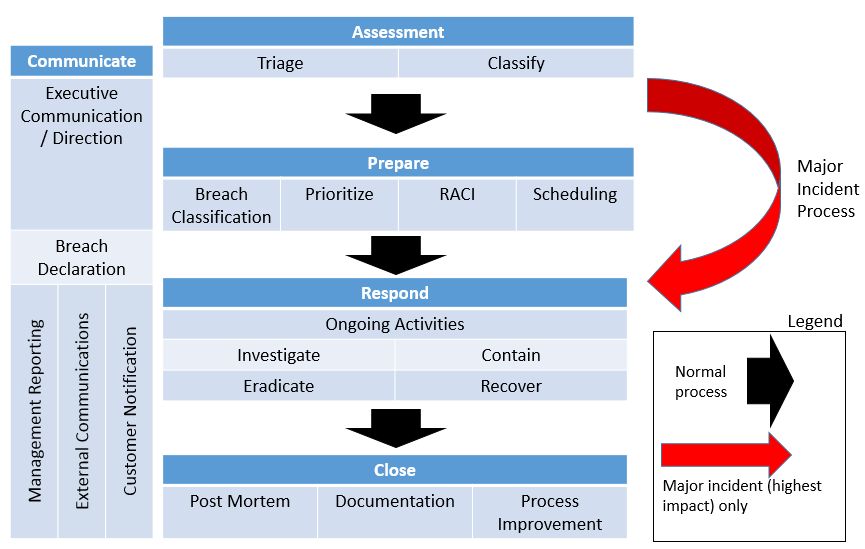


Figure Security Incident Response Process

The following subsections describe each of the phases in this process in more detail.

* 1. Assess
     1. Triage

As every escalation may not be a security incident, operations must perform triage activities to examine each escalation and make a determination of whether a security incident occurred. Numerous activities may be included across the incident management process beginning with triaging the issue to identify what situation you are facing.

Operations teams should triage an issue before escalation to SIR. Once an issue is escalated, the SIR team will conduct preliminary review of escalation for technical artifacts and to gain situational awareness. Key things to consider during this phase are the incident background and scope. The tables below provide common questions asked while assessing a security incident.

|  |
| --- |
| **Incident Background** |
| What is the nature of the problem, as it has been observed so far? |
| What’s the problem initially detected?  What was it detected and by whom and/or what system? |
| What security infrastructure components exist in the affected environment? (e.g. firewall, anti-virus, etc.) |
| What is the security posture of the affected IT Infrastructure components? How recently, if ever, was it assessed for vulnerabilities? |
| What groups or organizations were affected by the incident? Are they aware of the incident? |
| Were other security incidents observed on the affected environment or the organization recently? |

|  |
| --- |
| **Incident Scope** |
| Who is designated as the incident manager? |
| What IT infrastructure components (Active Directory Domain Services domain controllers, highly sensitive credentials, servers, websites, networks, etc.) are directly affected by the incident? |
| What applications and data processes make use of the affected IT infrastructure components? |
| Are we aware of compliance or legal obligations tied to the incident (e.g. PCI, breach notification laws, etc.)? |
| What are the possible ingress and egress points for the affected environment? |
| What theories exist for how the initial compromise occurred? |
| Does the affected infrastructure pose any threats to other organizations? |

Modified from: <https://zeltser.com/security-incident-questionnaire-cheat-sheet/>

|  |
| --- |
| **Communications considerations** |
| Who is designated as the communications manager? |
| Which individuals are aware of the incident? What are their names and group or company affiliations? |
| Which executive needs to be engaged first; for notification and direction? |
| What mechanisms will the team use to communicate when handling the incident? (e.g. email, conference call, etc.)? What encryption capabilities should be used? |
| What is the schedule of internal regular progress updates? Who is responsible for them? |
| Do you have outside council to guide you through communicating internally to employees or externally to vendors or customers? |
| What should you share and will your message help your situation or be a potential cause of further reputational damage? |

|  |
| --- |
| **Other considerations** |
| Has this event been seen and handled in the past? Is there existing documentation to reference? |
| Are there known, existing risk mitigations? |
| Are there know, existing contingencies? |
| Who is authorized to make business decisions regarding the affected operations? |
| Is there a collaboration site being used? Is it isolated and secure? What about protecting all data at rest that is being used for response? |
| Who will conduct “in the field” examination of the affected IT infrastructure? Note their name, title, phone, and email details. |

Modified from: <https://zeltser.com/security-incident-questionnaire-cheat-sheet/>

* + 1. Classify

A security incident should be classified to map the level of response required for that incident, to identify appropriate resources for response and to establish a timeline of actions based on the [Customer] agreements and regulatory obligations. Ultimately, the classification relates specifically to the risk the incident poses on the business. SIR, in consultation with operations teams, will classify the security incident and assign a severity level based on the artifacts known and the impact associated with them.

The table below provides sample severities and nature of compromise. Your SIR team should update these severities, and if necessary add net new definitions, based on your own requirements and interpretation of what the impact is to your business.

Note: Consultants should help guide customers through the process of classifying a security incident, using the table below. Customers should think through these levels and provide business impacting scenarios updating the definitions to be more relevant to their organization.

|  |  |
| --- | --- |
| Severity | Nature of Compromise |
| Critical  Sev 0 | Tampering or disclosure of HBI data, cross-service denial of service, elevation of privilege in system intended to handle HBI data, elevation to service administrator or cross-tenant elevation of privilege, successful or suspected exfiltration attempts to HBI or credentials. |
| High  Sev 1 | Spoofing, tampering of MBI/LBI/PII, tampering audit trail, disclosure of MBI/PII, Scoped Denial of Service, elevation of privilege on a system NOT handling HBI or successful or suspected exfiltration attempts to non-sensitive data |
| Medium  Sev 2 | Spoofing with the need for user intervention, moderate service audit trail, disclosure of LBI or Internal system information, limited Denial of Service, compromise of asset which can lead to access HBI/MBI |
| Low  Sev 3 | Adversary is conducting reconnaissance against a server/service or unsuccessful attempts to exploit assets with access to HBI/MBI/PII |

* + - 1. Classifying ATA Suspicious Activities

Microsoft Advanced Threat Analytics (ATA) focuses on detecting a variety of threats relating to your Active Directory Domain Service credentials. ATA categorizes these threats as follows:

* **Malicious Attacks** – detection of known malicious attack patterns attackers use to gain control over highly valuable credentials in your environment
* **Known Security Issues and Risks** – detection of known security issues and risks which may still be relevant in your environment potentially opening the possibility to compromise

**Abnormal Behavior** – behavioral analytics uncovers suspicious activities and abnormal behavior, leveraging machine learning (user and entity behavioral analytics) to identify patterns and alert upon discovered anomalies.

By default, Microsoft Advanced Threat Analytics provides you with a technical severity for the suspicious activity that it reports on. These classifications should be considered an initial point for consideration of the overall issue. However, depending on the nature of the event being observed, the eventual organizational risk may vary and is purely dependent on the business impact resulting from the identified suspicious activity.

For example, ATA may report a “Golden Ticket” as a “medium” severity. However, after further investigation, your SIR team identifies that the issue is true and the severity is high as the attacker now has the ability to act as a domain controller within your environment. While ATA may set this to “medium” by default, the actual business classification is a “Critical Sev 0” with high business impact.

If ATA identifies issues, please consider the following:

1. Is the issue isolated or are there multiple related suspicious activities?
2. What is the sensitivity or value of the entities being attacked?
3. Are the accounts or computers in question administrative or used for administrative activities?

Please keep in mind that just because an account may have been targeted that was not administrative in nature does not mean that the issue is not of a high severity. While identification that a domain administrative account has been compromised is “critical”, a regular user could also be critical depending on the access that user has. Consider the severity if your Chief Financial Officers account was the target. That person may be a regular, non-administrative user but they likely have access to highly sensitive information resulting in a critical severity risk rating.

**Instructions:** During the “Event Definition and Risk Classification” workshop, you guided your customer through defining the severity of each of the ATA event definitions along with conditions that may drive that severity rating. Update the following table to reflect decisions that were made in that workshop.

The following table provides a listing of each of the suspicious activities that ATA may identify in your environment. During the response planning workshops, a business risk classification was defined for each suspicious activity along with conditions that either apply, or may alter, the defined severity. Please leverage this information as your starting point when beginning risk classification for suspicious activities that ATA may find.

|  |  |  |  |
| --- | --- | --- | --- |
| ATA Suspicious Activity | Tool Severity | Risk Classification | Why? Under what conditions? |
| Reconnaissance using DNS | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Reconnaissance using Account Enumeration | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Reconnaissance using BruteForce (LDAP, Kerberos) | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Reconnaissance using SMB Session Enumeration | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Pass-the-Ticket | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Pass-the-Hash | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Over-Pass-the-Hash | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Skeleton Key Malware | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Forged PAC | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Golden Ticket | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Remote Execution | Low | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Malicious Replication of Directory Services | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Malicious Data Protection Private Information Request | High | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Abnormal Behavior based on Authentication, Authorization and Working hours | Medium (High if Admin Account) | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Massive Object Deletion | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Sensitive Account Exposed in Plain Text Authentication | Low | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Service Exposing Accounts in Plain Text Authentication | Low | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Unusual Protocol Implementation | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Detection of MS11-013 Vulnerability | Medium | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Broken Trust | Low | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |
| Honey Token Account Use | Low | <Enter Risk Classification Here> | <Enter in Conditional Reasoning for setting, or adjusting, classification here> |

* + 1. Major Incidents

As stated in the How to Use this Plan section of this document, activities performed in these phases may occur in parallel based on the severity and priority of actions. In the case of a high severity incident, actions to communicate and contain will take precedence over activities like scheduling, RACI and even eradication.

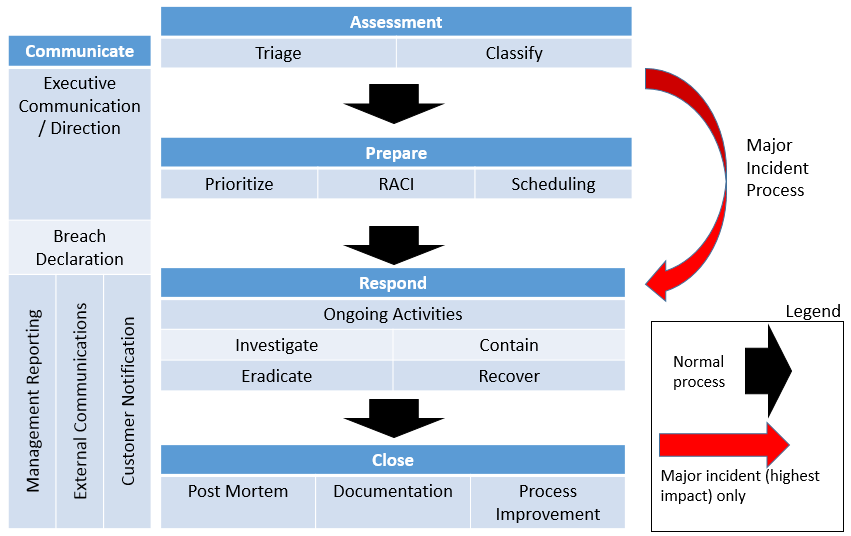


Figure - Major Incident WorkFlow

In cases such as this, a battle card is good to keep on hand. Below is an example of a high severity incident battle card that walks you thru the major incident process and provides you with direct links to standard operating procedures (SOPs). These SOPs should be readily available to all operations staff during an event.

**Note:** Consultants should work with key stakeholders to populate the table found below with document links and names of individuals accountable for each activity

|  |  |  |
| --- | --- | --- |
| ACTION | How to Do It (SOP) | Contact |
| Rapid Classification and prioritization |  |  |
| Executive Notification Process |  |  |
| Rapid Investigation and Containment |  |  |
| Rapid Notification to PR/LEGAL/ETC |  |  |
| Initiate RACI and Scheduling Review |  |  |

* 1. Prepare
     1. Prioritize

Priority speaks to order. If two Sev 0 events occur, which should get attention first? Also, goals and the activities needed to address an event need to be prioritized.

Before an appropriate response to a security incident can be defined, the team must have a comprehensive understanding of the response priorities. These may vary widely, according to a wide range organizational and incident specific factors.

Examples of prioritization scenarios:

* If an adversary is able to compromise an asset that will impact customer licensing, the top priority may be system integrity
* If the compromised system is used to store customer PII, the highest priority may be to identify the extent of any unauthorized access across the data sources depending on the context
* If the compromised system is used to delivery authentications services, restoration of reliable service may be the top priority

Priorities are normally decided by the Incident Manager with guidance from possibly all other roles. Adjudication by leadership/management may be needed, and may involve an executive sponsor from the directly impacted business unit.

A sample priority list for a security incident that involved possible exfiltration of customer data may resemble the following:

|  |  |
| --- | --- |
| Success Element | Priority (1 being High, 6 being Low ) |
| Minimize customer impact | 1 |
| Execute remedial actions | 2 |
| Restoring operations quickly | 3 |
| Address legal or regulatory risk | 4 |
| Media coverage | 5 |
| Identify actors involved in the breach | 6 |

Note: As previously stated, priorities and success elements will vary based on the severity and business impact of the security incident. Consultants should work with customers to define a list of Success Elements for most security incidents and prioritize them during the Prepare phase, and continue to revisit throughout the incident lifecycle.

* + 1. RACI

Once priorities have been established and agreed to, the next step is to identify the tasks that are involved in executing those responses, pinpoint individuals who will be owning those tasks for completion and check for any redundancy. Responsible, Accountable, Consulted and Informed (RACI) charts are useful tools for ensuring that important activities are not overlooked or duplicated. These roles may vary per, or depending upon the, incident. Completing a RACI should occur each time the process is invoked.

The following is an example of a RACI Chart. As a part of the incident response process, the RACI should be reviewed and defined as it appropriate for that specific incident. Please leverage the following table as a guide to help you further define the RACI for each incident.

Note: As is the case with a list of priorities, RACI charts are subject to change based on the severity and business impact of the incident.

Consultants should provide guidance on how to populate the table below with customer specific details.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Role** |  |  |  |  |
|  | **Incident Manager** | **IT Operations** | **Legal Representative** | **Communications Manager** | **Management** |
| Initial Assessment | Accountable | Responsible |  |  |  |
| Initial Response | Accountable | Responsible | Consulted | Informed | Consulted |
| Collects Forensic Evidence | Accountable | Responsible | Consulted |  | Informed |
| Implements Temporary Fix | Accountable | Responsible | Informed | Informed | Consulted |
| Sends Communication | Consulted | Consulted | Consulted | Responsible | Accountable |
| Check with Local Law Enforcement | Informed | Informed | Responsible | Informed | Accountable |
| Implements Permanent Fix | Accountable | Responsible | Informed | Informed | Consulted |
| Determines Financial Impact on Business | Consulted | Consulted | Consulted | Informed | Accountable  Responsible |

* + 1. Scheduling

In the event of a high security incident, the sequence of response activities may be governed by both severity and contractual obligations directed by senior leadership, legal, and SIR teams involved in the incident and regulatory compliance. SIR team, in consultation with partner teams and Incident Manager(s), will establish a schedule to execute response activities in consideration with these obligations.

The timeline below provides a high level example of possible response activities and incident milestones for a security incident.

Note: Consultants should work with customers to identify the proper platform and format for communicating status and providing checkpoints. Status updates are critical for problem management and process improvement activities. Checkpoints establish a cadence that Ops teams can use for providing updates. SIR and Executive teams use these checkpoints for managing the incident response and communications activities.

* 1. Communicate

The SIR team will provide periodic updates to the key stakeholders regarding the incident until the incident has been closed. Communication frequency and level of detail should be agreed upon in advance.

* + 1. Executive communications and reporting

During Assessment, notification to executive leadership is often appropriate and necessary. Executive(s) can aid in determining the total impact (both financial and otherwise) of a security incident to the business or the entire organization. Leadership provides guidance on the response (e.g., who notifies customer(s), public relations actions, early legal involvement, etc.). Finally, leadership provides legitimate-power coverage for expedited authority chains (e.g., quick decision making for major incidents).

* + 1. Breach declaration

Breach declaration involves communicating out both internally and externally the nature, impact and response to the breach. Breach declaration will often be governed by notification laws established by local and national governments. These laws require an entity that has been subject to a data breach to notify their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach. It is critical to be aware of the requirements and exceptions to these laws before declaring a breach (e.g., laws may permit delayed notification for certain circumstances such as when a law enforcement agency determines that notification would impede a criminal investigation).

Additional Information:

National Conference of State Legislatures

<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

US-CERT  
<https://www.us-cert.gov/incident-notification-guidelines#Incident_Notification>

U.S. Department of Health and Human Services

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

Office of the Australian Information Commissioner

<http://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>

* + 1. External communications

The Security team and Executive leadership shall be responsible for providing guidance regarding all communication with third parties and what information is being disseminated internally among organizations. Given the sensitivities surrounding these types of events, no entity should engage internal or external third parties without the approval of leadership and SIR teams.

However, you should be mindful of the information you are sharing as sharing inaccurate data, or information that is too subjective, may lead to reputational damage to your organization. As you consider your communication strategy, consider seeking outside council to assist you. Preferably a reputable firm that is experienced in communicating breach declarations especially when communications are intended for an external audience. While there may be a need to move quickly, you must remember going out with information too early can hurt an organization in a data breach. Here are a few items to consider:

* Resist communicating numbers early in the investigation
* Be careful of claiming the issue is fully resolved
* Focus initial messages on steps being taken to investigate the issue

Remember, “facts” are fluid so rushing public statements can result in several bad outcomes for a company including:

* Inaccurate dissemination of information
* Compromising more data
* Damaging company reputation further by breaking trust again

Please consider the following items as you begin to establish your messaging:

* **Customers must be your primary focus**. Communicate with them clearly and effectively through traditional and digital channels
* However, don’t neglect the wide variety of stakeholders interested in breaches including policymakers, regulators (state and federal) and industry stakeholders (e.g. payment brands)
* Be lean, but integrate legal, IT, PR and business group into communications planning
* Think through what you push out via social media
* Media train executives
* Set up the appropriate media/social monitoring and listening posts
* Develop a long-term reputation recovery strategy, versus treating it as an isolated incident
  + 1. Internal communications

While emphasis is often placed on external communications, internal communications must not be neglected. You must spend time determining when to tell employees and what to tell them. While it may be uncomfortable to consider, leaking information does occur and could negatively impact, or dramatically alter, your external communications plan. While you may be inclined to tell employees quickly, you need to expect that whatever you share internally, will be made available externally.

This may lead you to believe that sharing information internally is not a good idea. However, you may have employees who work directly with customers and if you have shared information externally, customers may be asking these employees questions or vetting their concerns. Regardless of the situation, if you have employees who may be in a situation where a customer will be asking them questions, you need to consider what their response needs to be and how you will educate them on how to respond to customers. For example, if you are a bank and you have recently disclosed a security breach, what should a teller do at branch bank when a customer asks questions or is observably upset about the potential impact to their own personal information? Do you direct them to the branch manager? Do you have cards with information on it that the customer can follow? Regardless of the correct process for you, you must define the process and train your employees accordingly.

* 1. Respond
     1. Investigate

The critical next step in response to a security incident is investigation. While investigating a security incident, the SIR and Operations teams will focus on deeper analysis of the event, gathering forensic evidence, determining the root cause and if necessary revising the original scope and impact of the incident.

To properly investigate a security incident, you should:

1. Acquire, organize and preserve evidence in a manner that is forensically sound (from an investigative versus a law enforcement perspective), given circumstances of the incident
2. Iteratively reassess and revise the scope, impact and severity of the incident as more facts are uncovered
3. Periodically check regulatory requirements regarding compliance and privacy
4. Identify possible root cause for the incident
5. Assess containment, eradication and remediation options with the operations team to reduce the impact of the incident
   1. SIR team will conduct the investigation in conjunction with the IT incident management process to leverage existing communication channels, resources and operating rhythm of each team
   2. Each of the five stages of the Investigate phase are iterative in nature and can be optional depending on multiple factors such as: nature of the incident, availability/integrity of evidence, environmental access, external dependencies, core customer data impact etc.

#### Evidence Gathering

It is extremely important to identify, gather and preserve evidence pertaining to a security incident in a manner which does not compromise your forensics process whether that is an internal process or one that is required by law or regulation. When collecting evidence, consider the following.

* Where is the evidence? List what systems were involved in the incident and from which evidence will be collected.
* Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
* For each system, obtain the relevant order of volatility.
* Remove external avenues for change.
* Following the order of volatility, collect the evidence with tools as discussed in Section 5.
* Record the extent of the system's clock drift.
* Question what else may be evidence as you work through the collection steps.
* Document each step.
* Don't forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted.
* Where feasible you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence.

More information for evidence collection and archiving can be found here

<http://www.ietf.org/rfc/rfc3227.txt>

#### Forensics

#### Root Cause Analysis (As Appropriate)

Depending on the nature of the incident, efforts should be focused on identification of incident root cause to the extent possible and validate it with the key stakeholders in the services. The primary goal of conducting root-cause analysis is to begin to determine the overall scope of the issue and identify a preliminary remediation plan to mitigate the overall impact. In many cases, identifying the root cause may not be possible within the timeframe of the incident response, making the priority on ruling out possible attack vectors and focus on immediate steps to contain the attack and its impacts.

#### Scope Revision

Identifying the initial scope and being able to revise the scope as more facts are uncovered in the phases of evidence gathering, forensics and root-cause analysis is essential in order to accurately respond to security incidents. Scope revision is focused on continually assessing scope, impact and severity. This should be an iterative process throughout the investigation and should rule out possibilities of cross-functional, cross-service and cross-organizational impact of the security incident, which significantly impacts the response posture, remediation efforts and notification requirements.

#### Investigation Synthesis

As the investigation matures from the initial triage to an evidence-oriented quest, it is important for the incident response team to synthesize the known facts, timelines and impact discovered so far to be able to classify the incident (section 4.1.2). The following checklist provides a guide for incident team to make an informed decision in classifying the incident:

Note: Consultants are encouraged to walk thru the checklist with the customer and add/update/remove any artefacts and/or guidance that doesn’t apply.

|  |  |  |
| --- | --- | --- |
| Artifact | Impact (NA/Low/Medium/High) | Guidance |
| Nature of Compromise |  | Type of Compromise and the value of The Asset involved in compromise |
| Root Cause |  | Method of Compromise |
| Method of Persistence |  | Mechanism that can facilitate reentry in to the environment or to regain access to assets after cleanup |
| Duration of Compromise |  | A timeline suggesting the initial indicator of compromise and subsequent activities |
| Relevant malicious activity |  | Any surrounding factors suggesting a possible link to the identified compromise vector |
| Data or credential loss |  | Actual data or credentials that are believed to be compromised |
| Asset Owner |  | IT Dept or business unit actually impacted by the compromise |
| Source of Attack |  | Attack vector that was used to initiate the compromise |
| Lateral Movement |  | Additional assets accessed by malicious actors after the initial compromise |
| Actual Loss |  | Indication of actual misuse of data or credentials believed to be stolen |
| Victims Involved |  | Compromised systems used for movement or traversal |
| Actor Attribution |  | Attribution of intrusion, control or activity to a specific group or individual |
| Actor Timeline |  | Timestamps and actions that could be attributed to the actor |

Table 1: Investigation Checklist

* + 1. Containment

The Containment phase is centered on protecting systems from further risk associated with the Incident through system isolation. In this phase, the memory of the systems of interest are sampled, disks are forensically copied, and the network is monitored.

* Containment & Remediation: In case of a security incident, the SIR team in consultation with the IT Operations teams and SMEs will develop an appropriate remediation and containment plan to reduce the impact of the incident in a timely fashion

Other Considerations

* Try to avoid letting attackers know that you are aware of their activities. This can be difficult, because some essential responses might alert attackers. For example, if there is an emergency meeting of Security Incident Response team, or you require an immediate change of all passwords, any internal attackers might know that you are aware of an incident.
* Compare the cost of taking the compromised and related systems offline against the risk of continuing operations. In the vast majority of cases, you should immediately take the system off the network. However, you might have service agreements in place that require keeping systems available even with the possibility of further damage occurring. Under these circumstances, you can choose to keep a system online with limited connectivity in order to gather additional evidence during an ongoing attack.

In some cases, the damage and scope of an incident might be so extensive that you might have to take action that invokes the penalty clauses specified in your service level agreements. In any case, it is very important that the actions that you will take in the event of an incident are discussed in advance and outlined in your response plan so that immediate action can be taken when an attack occurs.

* Determine the access point(s) used by the attacker and implement measures to prevent future access. Measures might include disabling a modem, adding access control entries to a router or firewall, or increasing physical security measures.
* Consider rebuilding a fresh system with new hard disks (the existing hard disks should be removed and put in storage as these can be used as evidence if you decide to prosecute attackers). Ensure that you change any local passwords. You should also change administrative and service account passwords elsewhere in your environment.
  + 1. Eradication

A key part of recovering from an intrusion is regaining control or “capturing” systems that an attacker has had administrative control of. The most effective way to accomplish this is to completely rebuild the affected system from trusted media so as to remove any attacker code.

NOTE: Prior to rebuilding a host, your organization should first perform analysis to ascertain

1. Whether this is part of a larger adversary operation or if this was an isolated incident.

2. Whether legal action may be planned and what forensic information must be captured as evidence for those efforts.

While rebuilding the operating system of the affected system from known good media will remove any attacker code that exists within the operating system, attackers can also persist in other ways. This can include in application binaries, data, and user state such as profiles as well as through credentials stolen from the computer. In rare cases, this can also include persistence through firmware and other components of hardware, but this is not commonly seen at this time. A system rebuild after a security compromise is different than a normal disaster recovery because attackers are motivated to persist access and great care must be taken not to allow the attacker’s presence to be reintroduced from any of those layers.

This section represents practical guidance on the type of activity required to perform a host rebuild after compromise. This guidance is not intended to be prescriptive step-by-step guide that guarantees a successful remediation forever as attackers are motivated to adapt and persist.

Rebuilding a system is just one facet of recovery from a persistent adversary. A recovery operation must include a planned approach, operational security (OpSec), hardening, monitoring, and other related activities to be complete.

The following are generic “Do’s and Don’ts” for securely rebuilding any individual system.

DO:

* Disconnect the system from the network at the start of the remediation event and do not reconnect it until it has been wiped.
* Inventory the machine for all installed software and data. Ensure you have a trusted copy of all software have saved off any application configuration and data.
* Wipe the machine’s hard disk so that the data is removed and will not boot under the old, vulnerable configuration.
* While not absolutely required it is also recommended that you flash any updatable ROMs/BIOS with the latest versions from the manufacturer.
* If possible, use a new host name so that the old name can be monitored for re-compromise attempts.
* Use new passwords for any accounts on the system. This includes local accounts, services, batch jobs, and accounts stored within applications on the system. You should also review accounts that were recently used on the system as their credentials may also have been compromised.
* Install the operating system (OS), using “known good media” from a trusted source. See Appendix C for details.
* Configure the local firewall or network profile to block all inbound connections until the system is fully updated.
* Apply patches and upgrades to correct known vulnerabilities with the OS.
* Install specific applications so that it can perform its prior business function. Ensure you are getting the latest patch version to eliminate any vulnerabilities.
* Inspect any restored application configuration and data for scripts, procedures, or other customizations that an attacker could have left to regain remote access.
* Where possible, do not restore any user profiles on the system and in particular pay attention to data in auto start execution points that can be used to start applications when the user logs on (e.g. registry “run” keys and start menu “startup”) items.
* Inspect data to be restored for malicious content that can be used to execute code.
* Where possible delete any .exe and .dll files to be restored.
* Virus scan all other content especially commonly exploited formats like Microsoft Office, Adobe PDF, HTML, images, and videos.
* Connect to the network and validate that any group policy settings have been applied.

DON’T:

* Use software to rebuild the system that was on the network and could have been tampered with by an attacker.
* Restore a full backup on to the new OS build because you might restore attacker tools installed on the machine.
* Restore data from backups that use compromised credentials. If necessary, change them before allowing the system on the network.
* Partially configure and/or patch the system.
  + 1. Recovery

The return of systems to a safe running state with technical operations reporting as normal, does not mean that services to stakeholders have been fully recovered. Steps need to be taken to ensure that services are at full, normal capacity and available for stakeholders. These steps may include

* Communications to stakeholders indicating they may proceed with normal system(s) use, or in some cases, engage systems per refined security protocols (e.g., password requirement changes or admin workstation isolation)
* Verification steps to ensure services have been fully restored for stakeholders (e.g., Do any new permissions implemented for protection prevent access and consumption of services).
* Escalation and de-confliction process have been established in the case when recovered services cannot be accessed as expected or needed.
  1. Close
     1. Post mortem

The best way to understand how a security incident happened is to perform a post mortem. The SIR team will conduct a postmortem of the incident with the service team and will document the findings and improvements needed to mitigate future threats.

A Post Mortem Report may include the following

* Problem - A description of what the problem was, and when the incident began and ended.
* Participants - Who actively participated in addressing this issue. This can be drawn from the RACI matrix
* Detailed Timeline of the incident (See Scheduling section above)
  + Date/time stamps of the update and/or action performed
  + Actions performed including results
  + Key milestones in the IR Plan (e.g. Executive Notification, Eradication Complete)
* Cause - What actions, or failures resulted in this incident coming to pass?
* Handling
  + What steps were taken during the handling of this incident?
  + What did each of the participants do?
    - Call out anything notable that an individual did / discovered (positive or negative).
  + Note: how the source of the problem was ultimately discovered.
* Solution - How was the problem ultimately resolved?
* Prevention - What can we do to prevent this incident from happening again, or to minimize the possibility of its reoccurrence?
* Lessons Learned
  + What could we have done better in the handling of this incident?
  + What mistakes were made in the management of this incident?
  + What steps can be taken to address the shortcomings of the handling of this incident?
  + What steps can be taken to prevent the mistakes that were made, or minimize the possibility of their reoccurrence?
    1. Documentation

During a Security Incident, all open tasks for the operations teams should be tracked within the [Customer]’s ticketing systems. The Incident handler shall choose the appropriate ticketing system based on the particulars of the Incident and the organizational teams involved. At the close of the incident, the SIR team will ensure all tickets related to the incident have been properly closed. All details captured during each phase of the indent response should be captured and included in a post incident review with appropriate properties.

* + 1. Process improvement

Once the threat has been contained, eradicated and services recovered, the Security Incident Response team will conduct process improvement activities that seek to close process and/or system performance gaps. Below are some starter questions that can help initiate the process improvement activities.

* Could the problem have been identified faster?
* Could you have realized it was a security incident sooner?
* Could you have stopped the problem earlier?
* What would have helped speed up any of these processes?
* Are you lacking a run book? A process? A tool? The right skill set? The right people on-call?
* Do you have sufficient resources to handle these attacks? Do you have enough people to look at the system logs, the firewall logs, and Intrusion Detection System (IDS) reports?
* Are you using software to analyze these logs and pull out relevant data to minimize the mind-crushing boredom of going through each by hand?

1. Appendix B: Further Reading

Responding to IT Security Incidents

<https://technet.microsoft.com/en-us/library/cc700825.aspx>

The Day After: Your First Response To A Security Breach

<https://technet.microsoft.com/en-us/magazine/2005.01.incidentresponse.aspx>

Computer Security Incident Handling Guide

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>