

IT205   
IT Security Incident Response Plan

|  |  |
| --- | --- |
| Status | Final |
| Version | 2.13 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc26134101)

[Introduction 4](#_Toc26134102)

[Purpose 4](#_Toc26134103)

[Audience 5](#_Toc26134104)

[Scope 5](#_Toc26134105)

[Policy Statement 6](#_Toc26134106)

[Document Control 7](#_Toc26134107)

[Exceptions 8](#_Toc26134108)

[Enforcement 10](#_Toc26134109)

[Revision History 10](#_Toc26134110)

Testing and Updates…...…………………………………………………………………………………………………………………………12

Incident Response Process Overview 6 Phases…….…………………………………………………………….…………………13

Phase I – Preparation Details…………………………………………………………………………………………………………………15

Phase II - Identification and Assessment…………………………………………………………………………………………….…15

Phase III – Containment………………………………………………………………………………………………………………….…….19

Phase IV – Eradication………………………………………………………………………………………………………………………..…24

Phase V – Recovery………………………………………………………………………………….……………………………………………25

## Phase VI - Lessons Learned……………………………………………………………………………………………………………………26

## Forensic Analysis & Data Retention……………………………………………………………………………………………………….27

Incident Response Checklist….....………………………………………………………………………………………………………..…29

Responsibilities At-a-Glance………………………………………………………………………………………………………………….34

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc. (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | February 17th, 2022 |
| Shamira Jaffer | CEO | December 20th, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | December 19th, 2019 |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Computer information systems and networks are an integral part of business at Signifi and its affiliates. These systems and infrastructure provide access to financial, administrative and confidential information. Security is critical to the physical and logical network, systems, applications and databases with each area offering its own set of security issues and risks. The protection of information systems is essential to manage business risk at Signifi. The nature of our business requires that we ensure the confidentiality, integrity and availability of Signifi information systems to provide high quality products and services to our members.

Purpose

To maintain the trust of Signifi’s employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential attack, the faster we can eradicate any threat and reduce the impact on the business.

This document describes the plan for responding to information security incidents at Signifi. It will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT team, technical support, operations/QA, development, legal, human resources, and corporate communications. It is important that the roles are well understood, as well as the ways of coordination with others.

This plan will be updated annually to reflect organizational changes, new technologies and new compliance requirements that concern our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

Roles, Responsibilities, Contact Information

This Incident Response Plan must be followed by all personnel, including all associates, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of Signifi. All personnel are referred to as ‘staff’ within this plan.

Below are details about the roles and responsibilities of each member of Signifi to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Incident Response Team Responsibilities

The **Incident Response Lead** is responsible for:

• Making sure that the IT Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.

• Making sure that the Incident Response Plan is current, reviewed and tested at least once each year.

• Making sure that staff with Incident Response Plan responsibilities are properly trained at least once each year.

• Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan when needed.

• Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.

• Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

**Security Incident Response Team (SIRT)** members are responsible for:

• Making sure that all staff understand how to identify and report a suspected or actual security incident.

• Advising the Incident Response Lead of an incident when they receive a security incident report from staff.

• Investigating and documenting each reported incident.

• Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.

• Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.

• Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.

• Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.

• Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

• Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All **staff members** are responsible for:

• Making sure they understand how to identify and report a suspected or actual security incident.

• Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).

• Reporting any security related issues or concerns to line management, or to a member of the SIRT.

• Complying with the security policies and procedures of Signifi.

Roles and Contacts

|  |  |  |
| --- | --- | --- |
| ROLE | RESPONSIBILITY | CONTACT DETAILS |
| **INFORMATION SECURITY** | | |
| **CISO** | Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan.  Authorizes when and how incident details are reported.  Main point of contact for executive team and Board of Directors. | Name: John Martin, VP, Technology  Phone: +1-416-432-2506  Email: jmartin@signifi.com  Name: Razvan Anghelidi, Director of IT  Phone: +1-647-708-3941  Email: ranghelidi@signifi.com |
| **Incident Response Team Lead and Team Members** | Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident.  Maintains incident response plan, documentation, and catalog of incidents.  Responsible for identifying, confirming, and evaluating extent of incidents.  Conducts random security checks to ensure readiness to respond to a cyberattack. | Name: Britt Swann, VP Customer Success  Phone: +1-480-662-8825  Email: bswann@signifi.com  Name: Stefano Tomio, Senior Service Delivery Manager  Phone: +1-647-381-9276  Email: stomio@signifi.com  Name: Dave Smith, Director, Support Services  Phone: +1-905-601-5522  Email: dsmith@signifi.com  Name: Joey Fleming, VP, Product Development  Phone: +1-416-993-1029  Email: jfleming@signifi.com  Name: Vahidin Sehic, Director, Quality Assurance  Phone: +1-647-833-7973  Email: vsehic@signifi.com |
| **Identity and Access Team Lead and Team Members** | Responsible for privilege management, enterprise password protection and role-based access control.  Discovers, audits, and reports on all privilege usage.  Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.  Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior.  Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.  Takes action to prevent the spread of a breach by updating privileges. | Name: John Sutton, IT Administrator  Phone: +1-416-606-6241  Email: jsutton@signifi.com  Name: Albi Dhamo, IT Administrator  Phone: +355-676-059-664  Email: adhamo@signifi.com  Name: Saimir Sako, IT Administrator  Phone: +355-676-034-534  Email: ssako@signifi.com |
| **IT Operations and Support** (internal) | Manages access to systems and applications for internal staff and partners.  Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack. | Name: John Sutton, IT Administrator  Phone: see above  Email: jsutton@signifi.com  Name: Albi Dhamo, IT Administrator  Phone: see above  Email: adhamo@signifi.com  Name: Saimir Sako, IT Administrator  Phone: see above  Email: ssako@signifi.com  Name: Hadeel AlZuhairi, IT Administrator  Phone: +1-647-677-0009  Email: halzuhairi@signifi.com |
| **Technical Partners**  (ISP, MSP, Hosting, Testing Partners, etc.)  **Third Party External Incident Response Teams** | Manages security controls to limit the progression of a cyberattack across third-party systems and organizations.  Coordinates with Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can be available in an emergency IR situation and provide any requested information prior to an emergency to help them become familiar with your environment. | Name: Razvan Anghelidi, Director of IT  Phone: 905-602-7707  Email: ranghelidi@signifi.com  Name: Oppos Inc. (consulting)  Phone: +1-416-953-0802 (Darace Rose)  Email: darace.rose@getoppos.com |
| **COMPLIANCE** | | |
| **Legal Counsel** | Confirms requirements for informing employees, customers, and the public about cyber breaches.  Responsible for checking in with local law enforcement.  Ensures IT team has legal authority for privilege account monitoring. | Name: Kevin Andrade, Legal Advisor  Phone:  Email: kevin@inhauslegal.com |
| **Audit & Compliance** | Communicates with regulatory bodies, following mandated reporting requirements. | Name: Razvan Anghelidi, Director of IT  Phone: +1-647-708-3941  Email: ranghelidi@signifi.com |
| **Human Resources** | Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees. | Name: Caroline Martin, VP, Talent Acquisition  Phone: +1-416-406-0001  Email: cmartin@signifi.com |
| **Regulatory Contacts** | Receives information about a breach according to timeline and format mandated by regulatory requirements. | Name: Kevin Andrade, Legal Advisor  Phone:  Email: kevin@inhauslegal.com |
| **COMMUNICATIONS** | | |
| **Marketing & Public Relations Lead** | Communicates externally with customers, partners, and the media.  Coordinates all communications and request for interviews with internal subject matter experts and security team.  Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach. | Name: Jamie McDowell, VP, Marketing  Phone: +1-416-707-1396  Email: jmcdowell@signifi.com |
| **Web & Social Media Lead** | Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users.  Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media. | Name: Melissa Dsouza, Digital Marketing Manager  Phone: +1-437-983-6212  Email: mdsouza@signifi.com |
| **Technical Support Lead** (Internal) | Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes. | Name: Razvan Anghelidi, Director of IT  Phone: see above  Email: ranghelidi@signifi.com |
| **Technical Support Lead** (External) | Provides security bulletins and technical guidance to external users in case of a breach. | Name: Dave Smith, Director, Support Services  Phone: see above  Email: dsmith@signifi.com |

Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.

2. The Incident Response Plan Testing will test Signifi’s response to potential incident scenarios to identify process gaps and improvement areas.

3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.

4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

Incident Response Process Overview

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their Incident Handler’s Handbook. The six steps outlined are:

### Phase I – Preparation

review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Cyber Security Incident Response Team (CSIRT). It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools

### Phase II – Identification and Assessment

monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything. Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements. (See Phase II - Identification and Assessment)

Phase III – Containment

perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems. Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

### Phase IV – Eradication

remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

### Phase V – Recovery

bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

### Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. No later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Chart, diagram, funnel chart

Description automatically generated

## Phase I – Preparation Details

The Preparation phase is easily the most important and often overlooked phase. Without proper preparation incident response activities may be disorganized, expensive, and could cause irreparable harm to Signifi.com. Tasks included in the Preparation phase include but are not limited to the following.

* Establish Cyber Security Incident Response Team (CSIRT).
* Ensure appropriate parties are aware of incident reporting processes.
* Document and share cyber insurance details with appropriate parties.
* Validate Logging, Alerting, and Monitoring policy compliance.
* Ensure CSIRT receives appropriate training based on skill gap analysis, career development efforts, and skill retention needs.
* Define and document standard operating procedures and workflows for CSIRT.
* Improve documentation, checklists, references, etc.
* Maintain and validate Network Diagrams and Asset Inventories.
* Review Penetration Test reports and validate remediations to findings.
* Review Vulnerability Management reports and validate remediation efforts.
* Establish disposable and disabled administrative credentials to be enabled and used for investigations.

Finally, it should be noted that the Phase I is continuous or at least cyclical as incidents are brought to conclusion.

### Reporting Incidents

Effective ways for both internal and outside parties to report incidents is equally critical as sometimes users of Signifi.com systems and information may be the first to observe a problem. Review the different types of incidents addressed in Phase II under *Incident Categorization* and list or establish reporting methods for a variety of incident types.

## Phase II - Identification and Assessment

## Identification

When a Signifi.com employee or external party notices a suspicious anomaly in data, a system, or the network, or a system alert generates an event, Security Operations, Help Desk, or CSIRT must perform an initial investigation and verification of the event.

#### *Events versus Incidents*

As defined above, Events are observed changes in normal behavior of the system, environment, process, workflow, or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with Signifi.com policy that negatively impacts (or may negatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all the following:

1. Email or phone notification from an intrusion detection tool.
2. Suspicious entries in system or network accounting, or logs.
3. Discrepancies between logs.
4. Repetitive unsuccessful logon attempts within a short time interval.
5. Unexplained new user accounts.
6. Unexplained new files or unfamiliar file names.
7. Unexplained modifications to file lengths and/or dates, especially in system files.
8. Unexplained attempts to write to system files or changes in system files.
9. Unexplained modification or deletion of data.
10. Denial/disruption of service or inability of one or more users to login to an account.
11. System crashes.
12. Poor system performance of dedicated servers.
13. Operation of a program or sniffer device used to capture network traffic.
14. Unusual time of usage (e.g. users login during unusual times)
15. Unusual system resource consumption. (High CPU usage)
16. Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
17. Unusual usage patterns (e.g. a user account associated with a user in Finance is being used to login to an HR database).
18. Unauthorized changes to user permission or access.

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

***NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.***

### Assessment

Once a potential incident has been identified, part or all the CSIRT will be activated by the IR (Incident Response) Commander to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The CSIRT should work quickly to analyze and validate each incident, following the process outlined below, and documenting each step taken.

The Incident Response Manager will assign a team member to be “Recorder” to begin formal documentation of the incident. The below determined categorization, scope, and impact must be included with documentation of the incident.

Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

#### *Incident Categorization*

The [MITRE ATT&CK Framework](https://attack.mitre.org/) is a globally-accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents. While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

|  |  |
| --- | --- |
| * Phishing * Unsecured Credentials * Network Sniffing * Man-in-the-Middle * Data Destruction * OS Credential Dumping * Event Triggered Execution | * Account Creation * Disk Wipe * Network Denial of Service * Resource Hijacking * Defacement * File and Directory Permissions Modification |

It should be noted that the MITRE ATT&CK Framework may not address some situations, specifically those without malicious intent, that trigger the Incident Response Management Plan. The following exceptions may require categories of their own as dictated by the organization’s Risk Management entities or policies:

|  |  |
| --- | --- |
| * Data Loss * Administrative Errors * Unsecured Credentials * Data Destruction * Lax File and Directory Permissions | * Account Creation * Disk Wipe * Network Denial of Service * Resource Misuse (non-malicious) * ADD OTHERS AS APPLICABLE TO THE ORGANIZATION/INDUSTRY |

#### *Incident Scope*

Determining the scope will help the CSIRT understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

* How many systems are affected by this incident?
* Is Confidential or Protected information involved?
* What is/was the entry point for the incident (e.g. Internet, network, physical)?
* What is the potential damage caused by the incident?
* What is the estimated time to recover from the incident?
* What resources are required to manage the situation?
* How could the assessment be performed most effectively?

#### *Incident Impact*

Once the categorization and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken in order to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander.

## Phase III – Containment and Intelligence

The objective of the containment phase of the incident response is to regain control of the situation and limit the extent of the damage. To achieve this objective, Signifi.com has defined a number of containment strategies relevant to a variety of incident types. Reference the procedures related to one or more of the Containment Strategies listed below.

### Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for the situation. If none of these strategies match the current situation, refer to ***Common Containment Steps*** listed below.

* Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
* Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed.
* If DOS/DDOS - control WAN/ISP.
* Virus outbreak – contain LAN/system.
* Data loss – review user activity, implement data breach response procedures.
* Website defacement – repair site, harden from future attacks.
* Compromised API – review changes made, repair API, harden from future attacks.

### Common Containment Steps

Containment requires critical decision making related to the nature of the incident. The Incident Response Manager, in coordination with the Incident Response Commander and other members of Executive Management, should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimize the impact to the business operations. Third party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

* Enable disposable administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while in being used.
* Will the ability to provide critical services be impacted? How? For how long?
* When should the Cyber insurance carrier be notified? (See Contact Information)
* Is a legal investigation or other action likely? Does evidence need to be preserved?
* How likely is the containment step to succeed? What is the end result, full containment or partial?
* What resources are required to support the containment activity?
* What is the potential damage to equipment and other resources?
* What is the expected duration of the solution? (Temporary, short-term, long-term, or permanent)
* Should IR team members act discretely to attempt to hide their activities from the attacker?
* Is the assistance of a third party required? What is the expected response time?
* Do interested parties (customers, partners, investors) need to be notified? If so, when?
* Does the impact to Signifi.com equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?
* Does the data impacted include protected data such as cardholder data? If yes, refer to Notification Requirements.

#### Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by Signifi.com and legal considerations.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **In-house investigation** | **Law enforcement** | **Private forensic specialist** |
| **Time Response** | Quick response | Varies by area and agency | Quick response |
| **Competency** | Skills vary | Depends on local law enforcement | Highly skilled, often with law enforcement background |
| **Preservation of evidence** | Does not ensure evidence integrity | Preserve evidence integrity and present evidence in court | Preserve evidence integrity and present evidence in court |
| **Reputation impact** | Minimal effect | Potential loss of reputation if certain incidents reach public | Potential loss of reputation if certain incidents reach public |

#### Preserve Evidence

***NOTE: If there is strong reason to believe that a criminal or civil proceeding is likely, the Signifi.com Chain of Custody form (location) must be used any time evidence has been taken into custody, or custody is transferred for the purpose of investigation.*** *For incidents involving cardholder data, Visa has defined specific requirements to be followed to preserve evidence and facilitate the investigation. Refer to Notification Requirements for more information.*

Consult legal counsel regarding applicable laws and regulations related to evidence collection and preservation. Create a detailed log for all evidence collected, including:

* Identification information (e.g. serial number, model, hostname, MAC address, IP address, or other identifier).
* Name and contact information for all individuals who have handled the evidence during the investigation.
* Date and time of each transfer or handling of the evidence.
* List of all locations where the evidence was stored.
* Deviations from SOP and associated justifications.

#### Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact to affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

* Stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.).
* Isolate compromised systems from the network.
* Avoid changing volatile state data or system state data early on.
* Identify critical external systems that must remain operational (e.g. email, client application, DNS) and deny all other activity.
* Maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence or giving them an opportunity to learn the CSIRT’s tactics, techniques, or procedures.
* To the extent possible, consider preservation of system state for further investigation or use as evidence.

#### Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

* Enable full packet capture.
* Collect and review system, network, and other relevant logs.
* Create a memory image of impacted systems.
* Take a forensic image of affected systems.
* Monitor possible attacker communication channels.

#### Conduct Research

Performing an Internet search, consulting third party resources, and/or consulting IT Insurance carrier using the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack. For example, if the insurance carrier has received multiple reports of similar incidents, or if a mailing list message contains the same IP or text of the message you received.

#### Notify Interested Parties

Once an incident has been identified, determine if there are others who need to be notified, both internal (e.g. human resources, legal, finance, communications, business owners, etc.) and external (e.g. service providers, government, public affairs, media relations, customers, general public, etc.). Always follow the “need to know” principle in all communications. Most importantly, remain factual and avoid speculation. See Notify Interested Parties for more detail.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs or issue gag orders to employees who need to be involved.

### Key Decisions for Exiting Containment Phase

* The attacker’s ability to affect the network has been effectively controlled/stopped.
* The affected system(s) are identified.
* Compromised systems volatile data collected, memory image collected, and disks are imaged for analysis.

### Investigation

As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, additional it may be necessary to revisit earlier phases. The Containment, Eradication, and Recovery phases are frequently cyclical.

The investigation attempts to fully identify all systems, services, and data impacted by the incident, including root cause analysis, which helps to determine the entry point of an attacker or weakness in the system that allowed the event to escalate into an incident.

A third-party may need to be contracted if investigation is beyond the skills of the CSIRT, impacted systems are owned by a Cloud Service Provider, or forensic analysis is required.

### Initial Cause (“Root Cause”) Investigation

Investigation should be conducted with consideration given to the ongoing impact to critical business operations. Ideally, the Initial Cause Investigation should be concluded before leaving the Eradication phase. At times, however, it may be necessary or appropriate to continue investigation during or after eradication and recovery. Delaying the Investigation should only be considered when the CSIRT is confident that the incident has been fully contained and the full scope of the impact is known. Delays or modifications to the scope of investigation activities must be approved by the Incident Response Commander.

The investigation techniques utilized will vary by the type of incident. The investigation may rely on some (or all) of the following:

* Interviews with witnesses and/or affected persons.
* Capturing images, snapshots, or memory dumps of affected systems.
* Obtaining relevant documents.
* Conducting observations.
* Taking photographs of physical locations.
* Reviewing security camera footage.
* Analyzing the logs of the various devices, technologies and hosts involved (e.g. firewall, router, anti-virus, intrusion detection, host).
* Reviewing email rules (compromised email account).
* Compare the compromised system to a known good copy.
* Anomaly detection/behavior monitoring (compare to preestablished baseline).

## Phase IV – Eradication Details

The Eradication consists of full elimination of all components of the incident.

Eradication

***NOTE: The specific administrative tools on a compromised host could be altered versions of the originals. Use a separate set of administrative tools (e.g. boot disk) than those on a compromised host for investigation whenever possible.***

Steps to eradicate components of the incident may include:

* Disable breached user accounts.
* Reset any active sessions for breached accounts.
* Identify and mitigate vulnerabilities leveraged by the attacker.
* Close unnecessary open ports.
* Increase authentication security measures (implement MFA, add geolocation restrictions).
* Increase security logging, alerting, and monitoring.
* Clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according to Signifi.com system build standards, including but not limited to:

1. Applying all the latest security patches.
2. Disabling all unnecessary services.
3. Installing anti-virus software.
4. Applying Signifi.com hardened system configuration baselines.
5. Changing all account passwords (including domain, user, and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full clean installation. IT personnel, at the direction of the CSIRT, will make this determination.

### Key Decisions for Exiting Eradication Phase

* Has the root cause been identified and identified vulnerabilities been remediated?
* Have all impacted accounts, including CSIRT burner credentials been reset?
* CSIRT is confident that the network and systems are configured to eliminate a repeat occurrence.
* There is no evidence of repeat events or incidents.
* Sign-off from IR Manager for limited-severity incidents or CIO for moderate and critical-severity incidents

## Phase V – Recovery Details

Prior to restoring systems to normal operation, it is critical that the CSIRT validate the system(s) to determine that eradication was successful, and the network is secure. Once the organization has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access to the compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to re-introduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorized access attempts.

Recovery steps may include:

* Restoring systems from a clean backup.
* Replacing corrupted data from a clean backup.
* Restoring network connections and access rules.
* Communicating with interested parties about changes related to increased security.
* Increasing network and system monitoring activities (short or long-term).
* Increasing internal communication/reporting related to monitoring.
* Engaging a third party for support in detecting or preventing future attacks.

### Key Decisions for Exiting Recovery Phase

* Have business operations been restored?

## Phase VI - Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

### Documentation

All details related to the incident response process must be formally documented and filed for easy reference. The following items must be maintained, whenever possible:

1. All system events (audit records, logs).
2. All actions taken (including the date and time that an action is performed).
3. All external conversations.
4. Investigator Notes compiled.

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

1. A description of the exact sequence of events.
2. The method of discovery.
3. Preventative measures put in place.
4. Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learned, to improve on the identified areas and used as reference for future incidents.

### Lessons Learned and Remediation

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents. Based on understanding of the root cause, steps will be taken to strengthen and improve Signifi.com information systems, policies, procedures, safeguards, and/or training as necessary. Where mitigations or proposed changes are rejected, a Risk Acceptance Process must be followed. Incidents should be analyzed to look for trends and corrective action should be considered where appropriate.

Lessons Learned discussion should cover:

* Review of discovery and handling of incident(s).
* How well staff and management performed and whether documented procedures were followed.
* Review of actions that slowed or hindered recovery efforts.
* Proposed improvements to future response and communication efforts.
* Recommendations to increase the speed of future detection and response efforts.
* Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur, either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added into the overall treatment plan.

Updates to the incident response procedures should also be considered and incorporated where areas of improvement are found.

Voluntary information sharing should occur whenever possible with external stakeholders to achieve broader cybersecurity situational awareness (InfraGard, ISAC, etc.). Legal and Management must be consulted before doing so if a formal Information Sharing policy and process do not exist.

### Forensic Analysis & Data Retention

In the event of possible legal action, forensic analysis will ensue in such manner as to preserve digital evidence consistent with legislative and legal requirements. Outside legal counsel and forensic experts may be required.

Consider the following when deciding whether and for how long to retain evidence related to the incident:

* Prosecution – is it likely that the attacker will be prosecuted? If so, evidence may need to be retained for multiple years.
* Reoccurrence – consider whether the evidence collected may be useful in case the attacker or a similar attack should occur in the future.
* Data Retention Policies – Consider the contents of evidence held (such as a system image capture) and retention policies related to this data (e.g. email retention policy).
* General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years.
* Cost – Depending on the type and amount of data or equipment preserved as evidence, cost may be a limiting factor.

### Key Decisions for Exiting Lessons Learned Phase

* Management is satisfied that the incident is closed.
  + IR Manager makes the decision for limited-severity incidents. CIO makes the decision for moderate and critical-severity incidents.

There is an action plan to respond to operational issues which arose from this incident. At this point, it is time to return to the Preparation Phase

### **General Investigation – Approach**

Digital forensic investigations should only be conducted by DFS(s) to ensure admissibility of the evidence obtained in subsequent legal proceedings – a DFS may be required to testify as an expert witness during court proceedings.

At the start of the digital forensic investigation, the DFS must:

* document and take photographs of all digital media which shall be subject to the forensic investigation, as well as the physical surroundings and layout;
* Date/Time/Location/By Whom must be recorded;
* make an inventory of the digital media acquired during the seizure. The inventory must be documented in the “Digital Forensic Report”, and the relevant photographs attached as evidential reference material.

In general terms, the DFS should conduct a full digital forensic acquisition of the devices referred to above.

If possible and whilst onsite, the DFS should preview those devices to determine whether they may contain data potentially relevant for the investigation and whether a partial forensic acquisition would be appropriate. Pending the initial preview, the DFS may conduct a partial forensic acquisition of the data.

The assurance and right to privacy does not and shall not prevent the DFS from conducting a thorough digital forensic acquisition of the targets of evaluation/examination.

The DFS will create a security backup copy of the acquired data on site, time permitting, storing it on a separate digital medium, and verify that it functions properly prior to leaving the site.

In order to protect the chain of evidence, the DFS will make an inventory of the digital media acquired during the seizure. This includes not accepting digital devices from any person at any time during the digital forensic investigation. Only the authorised DFS shall accept digital devices, and inventory where appropriate, to conduct a digital forensic acquisition.

At the site of acquisition (seizure), the DFS shall draw up a “Forensic Acquisition Register” recording all activities relating to access, acquisition, collection, compilation and storage of the data for forensic investigation. All digital forensic copies created and their respective hash values must be recorded against the forensic acquisition inventory (as described above).

Any error, damage or other incident and any remedial steps taken shall be specified and documented and validated by the DFS and witnessed.  Where the digital medium was not acquired forensically, this shall be recorded and noted on the forensic acquisition inventory.

Objections made during the digital forensic investigation by the offender being investigated shall be recorded in the notes of the “Forensic Acquisition Register”. The DFS will forward any recorded objection which relates to personal data or procedural guarantees for legal advice where necessary.

The “Forensic Acquisition Register” will record and identify all persons actively involved in the digital forensic investigation. The “Forensic Acquisition Register” shall be signed by the DFS who carried out the forensic acquisition and if applicable witnessed by any additional on-site technical staff who assisted in the execution of their duties. The DFS shall retain a copy of the “Forensic Acquisition Register” and shall register this immediately upon return to the office/laboratory as part of the case file.

All devices containing information gathered during the digital forensic acquisition must be transported in a secure manner, for example (but not limited to):

* on hard-ware encrypted hard disks,
* anti-static bags sealed with security seals,
* protective/padded carry bags to avoid damaging the device(s)

When being transported from the seizure site to the laboratory, the items will remain under the physical control of DFS staff (e.g. by hand) at all times. This maintains the integrity of the chain of evidence.

Where a digital forensic image and a security copy have been made, they should be carried by different members of staff, if possible, but adhere to the same principles as defined above.

Incident Response Checklist

To demonstrate and improve the effectiveness of Signifi’s incident response team and security tools, the process requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

Also use the ‘Signifi – Incident Report (Security).xlsx’ template to record information.

|  |  |  |  |
| --- | --- | --- | --- |
| PHASE OF CYBER INCIDENT | ACTION | TEAM MEMBER/ SYSTEM | DAY/TIME  ACTION TAKEN |
| **Incident Discovery and Confirmation** | Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.). |  |  |
|  | Note the system or systems affected (internal or production server) |  |  |
| Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred. Check the alerts and the SIEM systems. |  |  |
| Describe potential attacker, including known or expected capabilities, behaviors, and motivations. |  |  |
| Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party. |  |  |
| Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response. |  |  |
| Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. |  |  |
| Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification). |  |  |
| Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification). |  |  |
| Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network. |  |  |
| Collect meeting notes in a central repository to use in preparing communications with stakeholders. |  |  |
| Inform employees regarding discovery. |  |  |
| Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools. |  |  |
| Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements. |  |  |
| **Containment and Continuity** | Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems. |  |  |
| Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media. Perform a Veeam or XCP-ng backup of the affected server. |  |  |
| Force multi-factor authentication or peer review to ensure privileges are being used appropriately. |  |  |
| Change passwords for all users, service, application, and network accounts. |  |  |
| Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker. |  |  |
|  | Remove systems from production or take systems offline if needed. |  |  |
| Inform employees regarding breach containment. |  |  |
| Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network. |  |  |
| Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Eradication** | Close firewall ports and network connections. |  |  |
| Test devices and applications to be sure any malicious code is removed. |  |  |
| Compare data before and after the incident to ensure systems are reset properly. |  |  |
| Inform employees regarding eradication. |  |  |
| Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Recovery** | Download and apply security patches. |  |  |
| Close network access and reset passwords. |  |  |
| Conduct vulnerability analysis. |  |  |
| Return any systems that were taken offline to production. |  |  |
| Inform employees regarding recovery. |  |  |
| Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Lessons Learned** | Review forensic evidence collected. |  |  |
| Assess incident cost. |  |  |
| Write an Executive Summary of the incident. |  |  |
| Report to executive team and auditors if necessary. |  |  |
| Implement additional training for everyone involved in incident response and all employees. |  |  |
| Update incident response plan. |  |  |
| Inform employees regarding lessons learned, additional training, etc. |  |  |
|  | Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |

Responsibilities At-a-Glance

| **Activity** | **Role** |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **CSIRT Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Officer** | **Management** |
| Initial Assessment | Owner | Advises | None | None | None |
| Initial Response | Owner | Implements | Updates | Updates | Updates |
| Collects Forensic Evidence | Implements | Advises | Owner | None | None |
| Implements Temporary Fix | Owner | Implements | Updates | Updates | Advises |
| Sends Communication | Advises | Advises | Advises | Implements | Owner |
| Check with Local Law Enforcement | Updates | Updates | Implements | Updates | Owner |
| Implements Permanent Fix | Owner | Implements | Updates | Updates | Updates |
| Determines Financial Impact on Business | Updates | Updates | Advises | Updates | Owner |

Update

This document and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE (YYYY-MM-DD) | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2013-06-11 | First version | Razvan Anghelidi |
| 1.1 | 2016-05-06 | Contact updates | Razvan Anghelidi |
| 1.2 | 2019-05-06 | Updated version, contact updates | Darace Rose |
| 2.0 | 2019-12-09 | Template change, contact updates | Razvan Anghelidi |
| 2.1 | 2020-12-02 | Annual review, contact updates | Razvan Anghelidi |
| 2.11 | 2021-12-16 | Annual review, contact updates | Razvan Anghelidi |
| 2.12 | 2022-02-15 | Added details on the IT internal process | Saimir Sako |
| 2.12 | 2022-02-16 | Updated version, annual review, contact updates | Razvan Anghelidi |