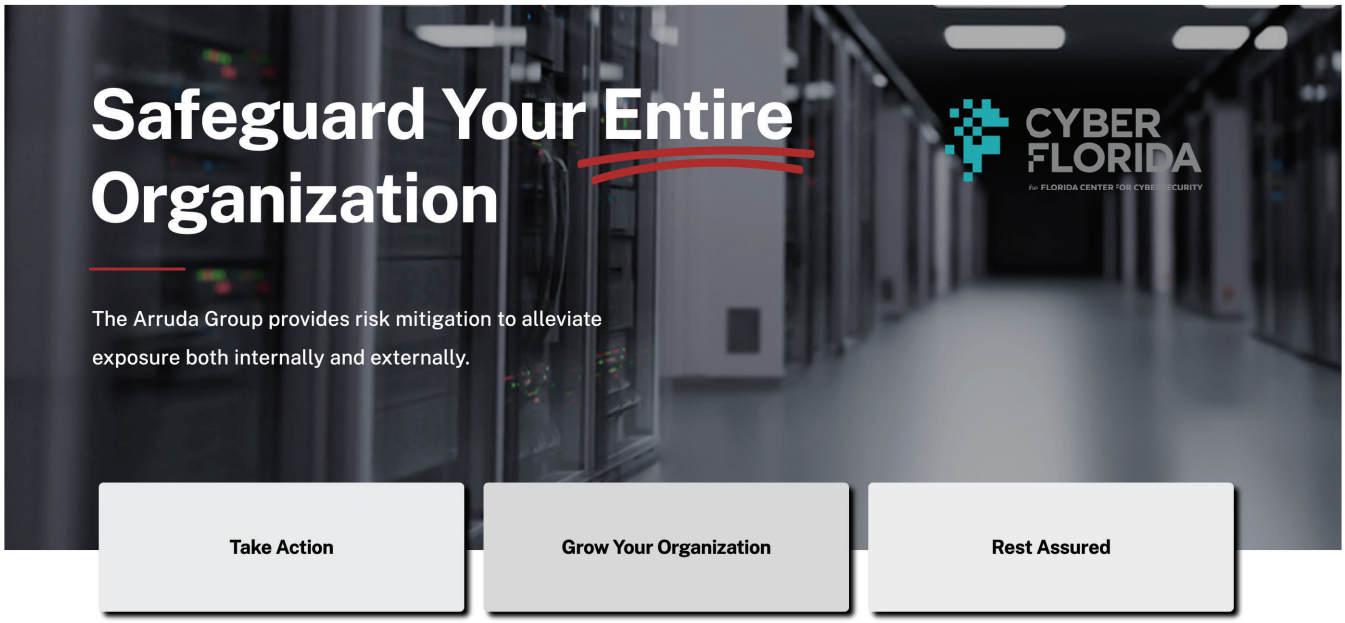


Stacy M. Arruda

Network Noise: IRP Workshop

STACY M. ARRUDA

AG | Arruda Group

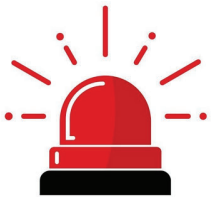
Objectives

- Build Plan
- Roles and Responsibilities
- Introduction & Guiding Principles
- Scope
- Definitions
- IRP Stages

IR Team Members

Private Sector

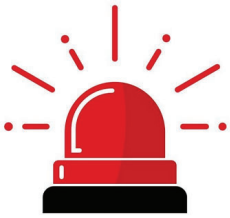
- Information Security Office (ISO)
- Information Technology Operations Center
- Information Privacy Office (IPO)
- Network Architecture
- Operating System Architecture
- Business Applications
- Online Sales
- Internal Auditing



IR Team Members

Public Sector (Maybe)

- Information Security Office (ISO)
- Chief Information Officer (CIO)
- IT Manager
- Information Assurance Office
- Internal Auditing
- Legal
- Human Resources



www.arrudagroup.com

IR Team Members

Getting Warmer???

- Information Security Office (ISO)
- Chief Information Officer (CIO)
- IT Manager
- Internal Auditing
- Legal
- Human Resources

Info Sec//IT Manager

Roles and Responsibilities

- Determine Nature & Scope of Incident
- Contact Qualified Resources
- Contact Members of the IRT
- Determines Necessary IRT Members
- Training and Incident Handling
- POC to Executive Management
- Engages Departments as Necessary
- Responsible for Chain of Custody
- Prepares Post-Mortem Report

Introduction

The **Incident Response Plan** is an **approved** organizational procedure that directs coordinated response to cyberattacks. The incident response plan provides specific guidance for each role and action of the Incident Response Team, with the goal of identification, containment, eradication, recovery, and lessons learned from the cyber attack. The Incident Response Team is responsible for putting the plan into action.

Introduction

The **Incident Response Team** is established to provide a quick, effective and methodical response to computer related incidents.

Their **mission** is to prevent loss of data, loss of the public's confidence or information assets by providing an immediate, effective, and appropriate response to any unexpected event involving computer information systems, networks or databases.

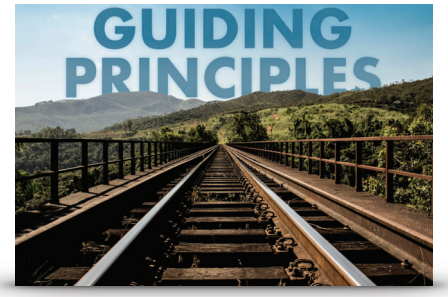
Introduction

The Incident Response Team is authorized to take the steps necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Information Security Officer/ Chief Information Officer will coordinate these investigations.

Introduction

- All suspected **Incidents** must be reported directly to Information Security via phone (as noted in **Section 5 – Contacts**) and/or email at: **xxxxx@gov.net**

- All communications regarding an incident are on a need-to-know only basis, meaning that no internal and/or external announcement will be made outside the IR process.



www.arrudagroup.com

Roles/Responsibilities

- In the management of incidents, Information Security acts as an independent third-party.

- The xxxxxxx in association with the Legal Department, xxxxxxxx, and Information Security/xxxxxxDepartment will draft, review, and finalize all external and internal communications.

Roles/Responsibilities

- Information Security will ensure every possible "root cause" scenario is appropriately investigated until evidence is identified that confirms or denies one or more scenarios.

- Information Security//Managed Service Provider will provide the Incident Board with the risks associated to each possible "root cause" scenario to enable the area involved to select the proper course(s) of action at any stage of the IR process.

www.arrudagroup.com

Roles/Responsibilities

- Computer forensics may require the engagement of an external party. The Finance Department will determine when this is necessary and work with Information Security to engage the vendor. (May want to have a vendor on contract)

- The Legal Department will determine when it is appropriate to contact the appropriate law enforcement agencies (FDLE, FBI, contact name and phone number) as well as notification to appropriate customer entities as required by contractual obligation.

Roles/Responsibilities

- The Human Resources (HR) Department, in association with the Legal Department will initiate and authorize all technology employee-related investigations as needed.

- All events, action items, and resolutions will be logged, saved, and stored by Information Security to be retrieved as required by law, regulators, or auditors.

www.arrudagroup.com

Roles/Responsibilities

- It is very important the Incident Response Team members receive all authorizations and permissions as well as resources to perform all investigative work throughout the incident. (elaborate further based on your organization's policies)

Scope

- Standard Protocol/Framework
  - Classification
  - Notification
  - Investigation
  - Remediation

Scope

When addressing reported incidents, it is the responsibility of key team members throughout the XXXX and the MSP (if you use one), to participate at a heightened state of awareness and diligence to provide senior level support when needed to gather critical information and facilitate administrative tasks as required. This can mitigate an incident to an acceptable level. It is also important to outline the process and requirements for incident response so that all team members can recognize an incident and know how to react when and if the opportunity arises to be called into action.

Definitions

EVENT: Observable occurrence in your infrastructure

INCIDENT: An event that specifically affects an organization's security // triggers Incident Response Plan

Definitions

INCIDENT Classification

Non-Technical

- Loss of backup media
- Discovered poor password control
- Equipment vandalism or theft
- Office break-in
- Unauthorized use of resources
- Fraudulent use of resources
- Violation of security policy
- Copyright infringement

Definitions

INCIDENT Classification

Technical

- Distributed Denial of Service (DDoS)
- Information Gathering (port scans, social engineering, phishing, etc.)
- Malicious code outbreak (Ransomware)
- Suspected intentional, subversive actions that preempt or degrade performance of a system
- Unauthorized alteration of a file or other uncontrolled system changes
- Unauthorized access to a system
- Repeated failed attempts to gain access to a system
- Unauthorized interception/monitoring of network

www.arrudagroup.com

Definitions

Incident Board – Initial communications are sent to the Incident Board (IB); the IB members allocate resources in their respective departments and provide leadership during the investigation stages; the IB is the executive component of incident management. Composition of the Board may vary, but will generally include the Attorney, Information Security Chief, Investigator Liaison, Incident Response Team Lead, and MSP liaison if you have one. Please add or delete as your agency dictates.

Definitions

Managed Service Provider (MSP) - Contracted vendor providing network administration, help desk support, firewall management, etc.

Incident Receiver – Person who initially recognizes the incident.

Incident Handler – Person (usually a manager or supervisor) responsible for logging the event and initializing the communication stage.

www.arrudagroup.com

Definitions

Incident Response Team - Resources allocated by the Incident Board for investigation, reporting, and Mitigating Action implementation; the Incident Response Team performs all work as determined necessary by the IB.

Investigator Liaison – Person (usually a business or IT lead) from the Incident Response Team responsible for coordinating investigative action items directly related to the area impacted by the incident.

Definitions

Non-Public Personal Information/Personally Identifiable Information (NPPI or PII) - Data that compromises the security, confidentiality, or integrity of personal information, which may include: a person's name in combination with any of the following data elements: (1) social security number; (2) driver's license or State identification card number account number, credit card number, in combination with any required security code, access code, or password that would permit access to a person's personal information or financial account.

www.arrudagroup.com

Definitions

Hot Fixer – Person (usually a technical resource) from the Incident Response Team responsible for identifying and applying Mitigating Actions.

Post-Mortem – The final stage and report of an investigation, lessons learned.

Special Counsel – Legal counsel assigned or engaged to assist with Incident Resolution.

Definitions

Mitigating Action – Temporary fix to the system that halts or minimizes the impact or further exploitation of a system.

Incident Report – The findings of an investigation along with Mitigating Actions applied and further remediation steps.

www.arrudagroup.com

IR Stages

Stage 1 - Incident Trigger

4.1

Security Incident

-Manual

-Infected e-mail
-Intelligence Reporting
-Internal Reporting

-Automatic

-MSP
-Firewall
-AV
-Security Incident Manager

Stage 1 - Incident Trigger

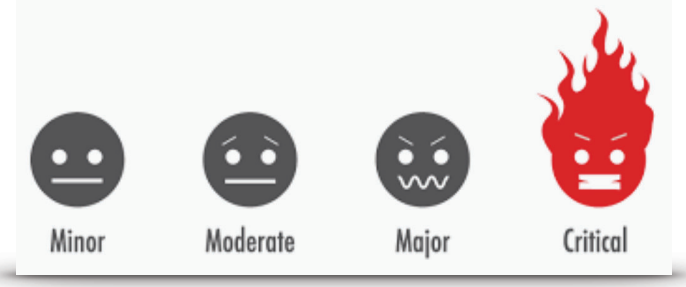
4.1

The event is classified by the severity of the incident which dictates the flow of and subsequent steps in the IR Process. The type and state of data compromised, and the scope of the breach are main factors when classifying severity.

Severity Levels

4.1.1

- Criticality of Asset
- Sensitivity of Date
- Impact to Agency/Organization
- Impact to Customer Experience



High Severity Incident

4.1.1

- Compromised NPPI//PII
- Malicious Code (Ransomware) Attack
- System Authentication Information
- Source Code or IP leak
- Sensitive//Confidential Comms Compromised
- B2B, B2C Website Defacement
- Unauthorized Access
- Sustained DDoS
- Insider Threat

Medium Severity Incident

4.1.1

- Unauthorized Access of Semi-Private Data
- Modification of Non-PII/NPPI Data
- Internal Website Defacement
- Encrypted NPPI/PII Compromised
- DDoS

Low Severity Incident

4.1.1

- Unintentional Leak of Public Data

RISK

Potential Incident Triggers

4.1.1

- MSP Alerts
- Firewall Notification
- IDS Alerts
- AV Software
- E-mail Threats
- SIM Alerts
- Intelligence Reporting
- Internal Reporting
  - Users
  - Admins

Note: At no time should any individual remove power, perform changes, or modify the system or any of its connections until a member of the Information Security team has been notified and has authorized such action. The only permissible action is to remove the network cable from the computer, or block/ disable access via firewall policies (MSP).

Stage 2 - Communication

4.2

Not Subject to Disclosure Under S. 119.071(3)(a), FL Statute

Stage 2 - Communication

4.2

The objective of the communication stage is to involve the appropriate parties at periodic status meetings. If the severity of the incident is classified as high, a secure method of communication must be established.

All internal communication will be stamped with "NOT SUBJECT TO DISCLOSURE UNDER S. 119.071 (3) (a), FLA. STAT." In addition, all internal communication must be directed to the Legal Department using the same notice.

Follow Incident Trigger

4.2.1

After informing the Legal Department and/or Information Security, the Incident Handler is responsible for drafting an IR notice email (refer to **Appendix A**):

- The recipients of the email are the Incident Board and the MSP.
- The purpose of the email is to bring the legal representatives and Information Security up to date on the situation and to log all known facts gathered thus far (time, date, systems, and scope of the incident).

Arruda Group

4.2.1

Incident Response (IR)

Security Incident Response and Notification
Please provide information related to the incident by answering the questions below. Take the time to be as complete, clear, and concise as possible. It is imperative that all information related to the incident is kept confidential and, on a need-to-know basis. Please, label all communication "NOT SUBJECT TO DISCLOSURE UNDER S. 119.071 (3) (a), FLA. STAT"

Severity of incident: [Enter: High/Medium/Low]

High:
- Non-Public Personal Information/Personally Identifiable Information (NPPI/PII) in clear text compromised or suspected of being compromised
- Malicious Code (Ransomware) attack
- System Authentication Information (usernames/passwords, e.g.)
- Source code or intellectual property (IP) information leaked
- Sensitive or confidential communications exposed
- B2B and B2C website defacement
- Unauthorized access to, or dissemination of, sensitive data
- DDoS (Severe-Halt of operations)

Medium:
- Semi-private data (data that is readily available to the public, but has been aggregated) accessed by unauthorized persons
- Modification to Non-PII/NPPI data
- Internal website defacement
- Encrypted NPPI/PII compromised or suspected of being compromised
- DDoS (Disruption of operations)

Low:
- Unintentional leak of public data

WHEN? Date/Time of incident:

WHAT/HOW? Impacted System Description
The affected systems are/is [list the systems impacted by the incident].
- Describe the business function of the system.
- If sensitive data is involved, describe the nature of the data.
- How many records are contained in the system?
- Describe the architecture of the system (Database location, Application server location, Components that make up the system) if known.

WHO/WHERE? Incident Description
Briefly describe the situation.
- Describe the timeline of the incident to date.
- How did the incident come to light?
- Who was involved in discovering the incident?
- How many people have been affected by the incident?
- How many people are aware that the incident has taken place?

Actions Taken
- List the steps taken to contain the incident to date.

CYBER FLORIDA the FLORIDA CENTER FOR CYBERSECURITY

Arruda Group

Follow Incident Trigger

4.2.1

- Notice to be provided to the City/County and insurer.

The Attorney or Special Counsel and Information Security will review the IR notice email and determine if the Incident Board needs to be convened based on the initial classification of the incident by the Incident Handler.

www.arrudagroup.com

CYBER FLORIDA the FLORIDA CENTER FOR CYBERSECURITY

The Initial Meeting

4.2.2

The initial meeting will determine the frequency of the IB meetings, as well as the need to set up the Incident Response Team. When NPPI/PII data is breached, compliance requirements must be followed by the appropriate parties.

The IB will prepare an initial assessment to the City/ County Commission individually, and possibly prepare an emergency public meeting notice of a Commission Meeting to be held as soon as practicable.

Throughout the Investigation

4.2.3

The Incident Board will hold meetings as needed to ensure progress is being made on the investigation of the incident and that all required communication and notification action items are being completed.

Business Operations Communication and Notification – Early in the investigation stage, the Incident Board needs to determine how the resource impacted will handle additional requests related to the incident.

Throughout the Investigation

4.2.3

Communication to Commission - Continuous updates should be provided to the Mayor/County Administrator and City/County Commission, where appropriate.

Throughout the Investigation

4.2.3

Communication and Notification – As the investigation provides facts and evidence about the incident, the Incident Board will be able to determine the type of communication required internally to manage the incident as well as the type of notification required externally. With this step, applicable "security breach" and "privacy" laws must be adhered to, to meet specific notification requirements.

www.arrudagroup.com

Throughout the Investigation

4.2.3

Notification to Consumers – The Legal Department is responsible for drafting the notification letters to the affected consumers and, if applicable, providing notification to the three major credit bureaus. The Legal Department will also notify the state's regulatory authorities, if required by the applicable state statute along with any required notification to consumers.

Throughout the Investigation

4.2.3

Activity Log – Throughout the investigation all activities related to the incident must be kept in a centralized log, including minutes from meetings, issues, resources, etc. This log will be used to draft the Post-Mortem Report.

www.arrudagroup.com

Stage 3 - Escalation

4.3

As a result of the initial Incident Board meeting, the Incident Response Team is assembled and an Incident Response Lead designated. The objective of the Incident Response Team is to provide the technical resources to investigate and remediate the incident.

Responsibilities

4.3

- The Incident Response Team Lead is responsible for the coordination of the investigation efforts and setting up the periodic team status meetings. The IRTL will be a single point of contact to the Incident Board in status meetings and will be responsible for preparing the final report from the investigation.

Responsibilities

4.3

- ☑ The Incident Response Team will designate a Hot Fixer and an Investigator to ensure all action items and remediation actions are deployed appropriately toward the resolution of the incident.

- ☑ For high severity incidents, the Incident Board determines if outside involvement is required (i.e., law enforcement, subject matter experts, forensic examiners, or outside counsel). Also, secure communications must be established for members of the Incident Response Team.

Stage 4 - Investigation

4.4

The investigation is executed by the Incident Response Team under the leadership of the Incident Response Team Lead, through a three step process:

- Preparation
- Discovery
- Investigation

Stage 4 - Investigation

4.4

Preparation

This step in the investigation is used to identify where any exfiltrated data resides, how to retrieve it, and obtain authorizations required by the Incident Response Team to access it.

In order to assist the impacted area, it is recommended the Hot Fixer, and Investigator be two separate people. Where resources are tight, the Incident Response Team's role is to identify back-up staff from another area to act as the investigator – if possible

Stage 4 - Investigation

4.4

Discovery

A dataflow analysis containing data classification, a physical and logical network diagram of the affected systems are created. All third-party interfaces are verified.

Stage 4 - Investigation

4.4

Investigation

The investigation step is used to understand the scope of the breach, parties involved, and identify the attack vector(s). A chronology of events will be produced from a thorough investigation.

As facts and evidence are discovered during the investigation, Mitigating Actions may be available. These actions are passed to the Incident Response Team Lead (IRTL) who determines an appropriate time to implement. The IRTL coordinates the implementation with the Hot Fixer. Mitigating Actions may include disabling user accounts, blacklisting IPs, or adding server-side validation routines to thwart the attack.

If it becomes apparent the scope of the breach or type of data affected warrants a change in severity, the IRTL sends the process back to the communication stage for reclassification.

Stage 5 - The 3 R's

4.5

Response

Near-term action to stabilize the system. Mitigating Actions fall into the Response category. This step is usually conducted during the investigation stage.

Stage 5 - The 3 R's

4.5

Recovery

Action taken to resume normal operation of the system. Once the affected systems are restored, they are tested to ensure the threat has been completely eradicated and that they are no longer vulnerable to the attack(s) that caused the incident. They are also tested to make sure they will function correctly when placed back into production.

Stage 5 - The 3 R's

4.5

Remediation

Long-term action to create a more secure system. The remediation items are usually more resource intensive.

www.arrudagroup.com

Stage 5 - The 3 R's

4.5

Each area representative may have action items that are assigned in the Post-Mortem Report. It is up to the area representative on the Incident Board to estimate, agree to, and plan for their action items. As each action item is implemented, the Post-Mortem Report is updated with the date of completion. The incident is closed only when **all** action items have been completed. Alternatively, a project plan can be established to ensure timely completion of long-term action items.

Stage 6 - Post Mortem

4.6

The Post-Mortem Report will include a summary of all **main** activities related to the incident. In this step, the entire incident and response is reviewed to determine which criteria of the IR plan worked correctly and any needed improvements. The areas in which improvements are needed are then corrected, and the IRP documentation is updated accordingly. Other areas requiring modification (policies, system configurations, etc.) may also be identified during this phase.

Stage 6 - Post Mortem

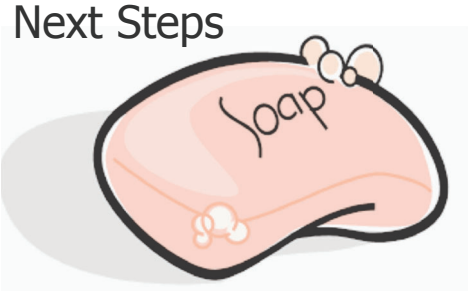
4.6 Post-Mortem Report Sections

- Overview of the IR Process
- Overview of the Post-Mortem Stage
- Who — The Players
- What — Nature of Incident
- Where — Physical Locations
- How — Attack Vectors

Stage 6 - Post Mortem

4.6 Post-Mortem Report Sections

- Remediation Steps
  - Mitigation Actions
  - Long-Term
- Conclusion
  - Estimated Costs (direct and indirect)
  - Lessons Learned
  - Next Steps



www.arrudagroup.com

Stage 6 - Post Mortem

4.6

The Post-Mortem Report is prepared by the Incident Response Team Lead and is presented to the Incident Board upon completion of the investigation. Artifacts such as the Activity Log developed in the investigation are included in the report as appendices.

Approval Page

Appendix C - Revisions and Management Approval Page

The following table contains detailed information about the revisions made to this document:

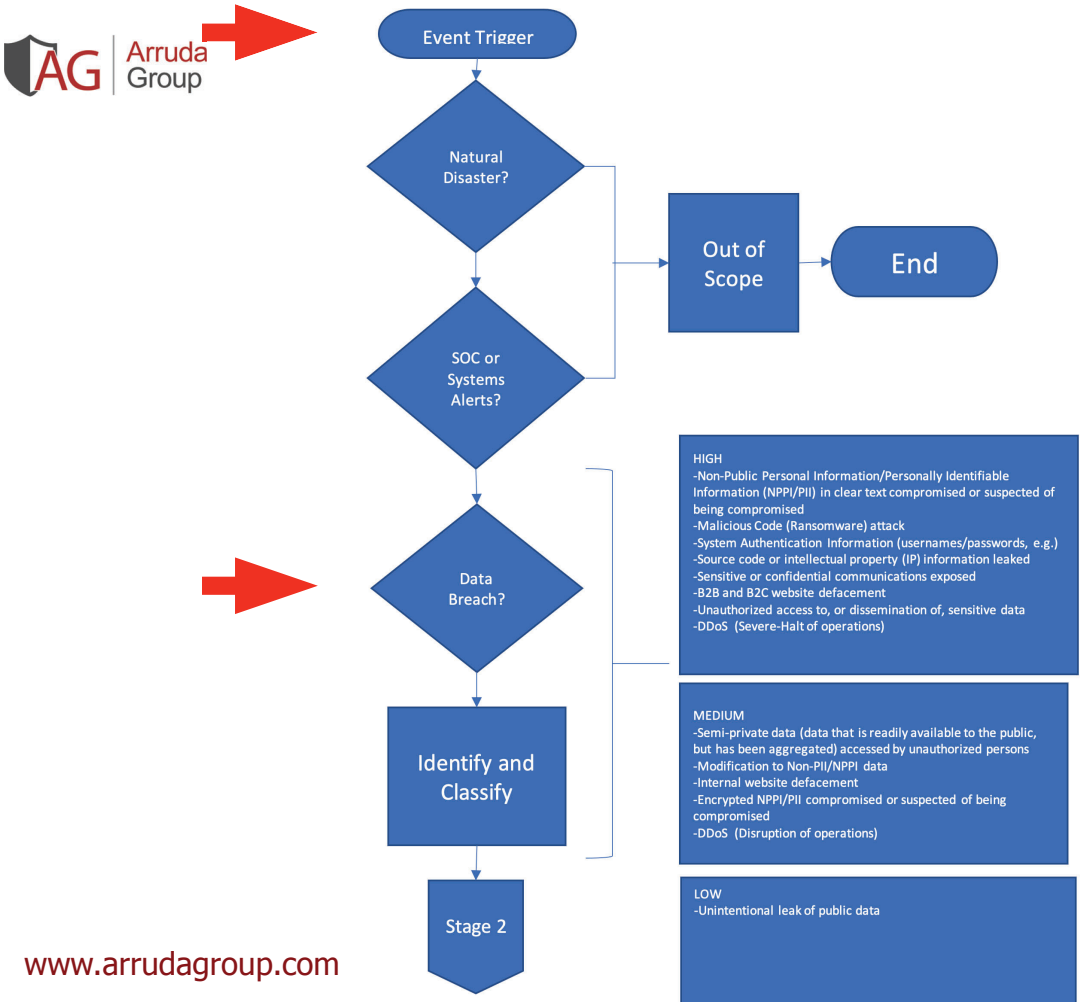
Version	Author Initials	Date (mm/dd/yyyy)	Comments

This document was reviewed and agreed upon by the ISO as evidenced below.

Signature:		Title:		Date:	

This document was reviewed and agreed upon by Legal as evidenced below.

Signature:		Title:		Date:	



www.arrudagroup.com

- Insider Threat
- Social Media: Cyber Crime Incubator
- Building a Security-Conscious Org
- Annual Cybersecurity Awareness
- Social Media Vulnerability Assessment
- Cyber Tabletop Exercises
- Incident Response Planning

813.382.0859
info@arrudagroup.com

www.arrudagroup.com