Ben Cox and Micah Leslie

CSC 321 Assignment 6

19 April 2024

“We certify that this assignment/report is our own work.”



CB Solutions

Natural Disaster Incident Plan

Ben Cox and Micah Leslie

[1. INTRODUCTION 2](#_Toc1486099195)

[1.1. General Information 2](#_Toc983699412)

[1.2. Purpose [2] 2](#_Toc1731708266)

[1.3. Scope [2] 2](#_Toc1381859512)

[1.4. Maintenance [2] 2](#_Toc1206932989)

[2. DEFINITIONS 2](#_Toc262311870)

[2.1. Event [2] 2](#_Toc705996031)

[2.2. Incident [2] 2](#_Toc578899610)

[2.3. Personally Identifiable Information [1] 3](#_Toc73471495)

[3. ROLES AND RESPONSIBILITIES 3](#_Toc1925445586)

[3.1. Incident Response Coordinator 3](#_Toc320234178)

[3.2. Incident Response Team [3] 3](#_Toc1846715717)

[3.3. Members [3] 4](#_Toc751227864)

[4. INCIDENT RESPONSE AND MANAGEMENT 5](#_Toc1470945073)

[4.1. Initial Incident Response Checklist [2] 5](#_Toc22733593)

[5. NOTIFICATION 5](#_Toc1467121868)

[5.1. Telephone Notification Process 6](#_Toc1589565006)

[5.2. Incident Response Assembly Locations 6](#_Toc1728001731)

[6. DOCUMENTATION, TRACKING AND REPORTING 6](#_Toc1209258603)

[6.1. Incident Response Checklists 6](#_Toc1986436864)

[6.1.1. Key Personnel Contact List 6](#_Toc58797930)

[6.1.2. Key Vendor Contact List 6](#_Toc1906624213)

[6.1.3. Initial Incident Response Checklist 6](#_Toc767974490)

[6.1.4. Incident Response Team Task Checklist 6](#_Toc613361557)

[6.1.5. IR Team Meeting 6](#_Toc576798244)

[6.1.6. Incident Response Coordinator Task Checklist [6] 6](#_Toc1824296916)

[6.1.7. Incident Response Recommended Actions 6](#_Toc820639548)

[6.1.8. Pre-incident Preparations [2] 6](#_Toc704990647)

[6.1.9. Post-incident Maintenance Activities [2] 6](#_Toc559269032)

[7. ESCALATION [2] 7](#_Toc494881833)

[APPENDIX 7](#_Toc878511526)

[REFERENCES 7](#_Toc1111967223)

# INTRODUCTION

## General Information

The Natural Disaster Incident Policy is meant to serve as guidance for any businesses within the scope of the document when struck by natural disasters. This document is to be given to the IR members located at any CB Solutions’ locations.

## Purpose [2]

This document is meant to stand in as the plan for CB Solutions when preparing and responding to natural disaster incidents. It defines the roles and responsibilities of participants, how incidents are defined, relationships to other CB Solutions’ policies, and the requirements for reporting incidents.

## Scope [2]

This document applies to business locations operating under CB Solutions, which involves employees and people who gain access to CB Solutions locations or data.

## Maintenance [2]

It is the responsibility of the current head of either the incident response team, or the head of information security. This document is to be updated regularly to ensure it is always in a ready state.

# DEFINITIONS

## Event [2]

An event is considered an exception to the normal operation of systems or infrastructure. Events are not to be considered the same as incidents.

## Incident [2]

An incident is an event that, after being assessed by staff, violates policies of CB Solutions related to acceptable use, information security, or physical security. An event can also be considered an incident when it threatens the code of conduct, confidentiality, or the availability of systems within CB Solutions.

Incidents can be categorized by the potential loss of data or physical hardware based on its criticality, to be rated using a tiered system of 1-3, with 3 being the highest threat to CB Solutions property.

For the purposes of this document, incidents can include:

* Fires
* Earthquakes
* Tornadoes
* Floods
* Large Storms
* Hurricanes
* Animal Infestation
* Or related natural disasters

## Personally Identifiable Information [1]

Personally identifiable information is information which pertains to a certain individual and can be used to uncover said person’s identity. There is both sensitive and non-sensitive information, for example sensitive information includes:

|  |
| --- |
| **Personally Identifiable Information** |
| SENSITIVE INFORMATION |
| Unique ID numbers, such as SSN, driver’s licenses, or other issued ID-numbers |
| Biometric data |
| Financial information |
| Medical records |
| NON-SENSITIVE INFORMATION |
| A person’s full name |
| Mother’s maiden name |
| Phone number |
| Unique ID numbers, such as SSN, driver’s licenses, or other issued ID-numbers |
| IP address |
| Place or Date of birth |
| Geographical details (ZIP, City, State, Country, etc.) |
| Employment information |
| Race or ethnicity |
| Religion |

# ROLES AND RESPONSIBILITIES

## Incident Response Coordinator

Throughout the protocol involved within this plan, the incident response coordinator is responsible for

* Managing the team in charge of collecting appropriate information
* Providing guidance in gathering necessary information and documentation of processes
* Reports efforts to the CISO (Chief Information Security Officer) and other leadership when deemed necessary.

## Incident Response Team [3]

A team comprised of company staff, advisors, and service providers shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). Our team consists of both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an incident that warrants IRT involvement, according to the incident’s severity. The entire IRT would be informed and involved in the most severe incidents.

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants, or other resources, (often referred to as Subject Matter Experts – SME’s) as needed, for the analysis, remediation, and recovery processes of an incident.

The Information Technology (IT) function plays a significant role in the technical details that may be involved in incident detection and response. There shall be a member of the IRT designated as the Incident Response Manager (IRM), who will take on organizational and coordination roles of the IRT during an incident where the IRT is activated for response to the incident.

## Members [3]

Primary Team Members

* CISO (Chief Information Security Officer)
  + Maintain strict guidelines of established policies and procedures
* Incident Response Coordinator
  + Coordinate and manage communications when a IRT is activated
* CFO (Chief Financial Officer)
  + Coordinate financial aspects of an incident
    - Financial impact and financial data security
* CHRO (Chief Human Resources Officer)
  + Communication to employees
  + Employee data protection
* CEO (Chief Executive Officer)
  + Operational impact of an attack and recovery
  + Public relations
    - Media and news management
* CSO (Chief Security Officer) \*Physical\*
  + Building access and controls

Secondary Team Members

* Legal Representative
  + Legal Advisor
  + Contractual matters

While CB Solutions does employ legal services among our staff, during an Incident Response we have external vendors for legal matters. We do this because specialized help with issues involving data leakage and mitigation is heavily important. We have to work to protect ourselves from audits and breaking contractual expectations.

* Public Relations Vendor
  + Public relations advisor
    - Works with CEO to issue a statement.

# INCIDENT RESPONSE AND MANAGEMENT

## Initial Incident Response Checklist [4]

|  |  |
| --- | --- |
| **Detection and Analysis** | |
| 1. | Determine when the incident occurred |
| 1.2 | As soon as the handler believes an incident has finished, begin documenting the investigation and gathering evidence |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |
| 3. | Report the incident to the appropriate internal personnel and external organizations |
| **Containment, Eradication, and Recovery** | |
| 4. | Acquire, preserve, secure, and document evidence |
| 5. | Contain the incident if applicable (fire, animal infestation) |
| 6. | Eradicate the incident if applicable (fire, animal infestation) |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited if possible |
| 6.2 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them |
| 7. | Recover from the incident |
| 7.1 | Return affected systems to an operationally ready state |
| 7.2 | Confirm that the affected systems are functioning normally |
| 7.3 | If necessary, implement additional monitoring to look for future related activity |

# NOTIFICATION

## Telephone Notification Process

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident. The IRT contains contact information for key leaders and executives within CB Solutions.

For notification of any possible incidents, please contact your local head of the IR team at ###-###-####. Possible incidents are defined above, early notification of them is necessary to prevent incident escalation. Be sure to have a list of:

* The location and time of incident
* Current losses to property
* The type of incident (fire, flood, storm, etc.)
* Anyone already responding or preparing for the incident

## Incident Response Assembly Locations

Incident response teams are meant to meet at the designated office for each CB Solutions location. These locations are designated by the regional manager and are to be always kept available during an incident. When incidents are escalated or deemed to be level 3, these teams are expected to report to, or meet at, the main CB Solutions location.

# DOCUMENTATION, TRACKING AND REPORTING

## Incident Response Checklists

### Key Personnel Contact List

|  |  |
| --- | --- |
| **Personnel Title** | **Phone Number** |
| Chief Information Security Officer | ###-###-#### |
| Head Incident Response Coordinator | ###-###-#### |
| Local Incident Response Coordinator |  |
| Chief Financial Officer | ###-###-#### |
| Chief Human Resources Officer | ###-###-#### |
| Chief Executive Officer | ###-###-#### |
| Chief Security Officer | ###-###-#### |

### Key Vendor Contact List

|  |  |
| --- | --- |
| **Vendor** | **Contact Number – If blank to be filled by local IR manager** |
| Legal Representative | ###-###-#### |
| Local Internet Service Provider |  |
| Electricity Provider |  |
| Public Relations Vendor | ###-###-#### |

### Initial Incident Response Checklist [4]

|  |  |
| --- | --- |
| **Detection and Analysis** | |
| 1. | Determine when the incident occurred |
| 1.2 | As soon as the handler believes an incident has finished, begin documenting the investigation and gathering evidence |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |
| 3. | Report the incident to the appropriate internal personnel and external organizations |
| **Containment, Eradication, and Recovery** | |
| 4. | Acquire, preserve, secure, and document evidence |
| 5. | Contain the incident if applicable (fire, animal infestation) |
| 6. | Eradicate the incident if applicable (fire, animal infestation) |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited if possible |
| 6.2 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them |
| 7. | Recover from the incident |
| 7.1 | Return affected systems to an operationally ready state |
| 7.2 | Confirm that the affected systems are functioning normally |
| 7.3 | If necessary, implement additional monitoring to look for future related activity |

### Incident Response Team Task Checklist

The members of the incident response team are expected to follow the following checklist to ensure they have properly covered all aspects of incident response for any given incident.

* Prior to expected incidents, make sure all members’ contact information is up to date and available during an incident
* During the start of an incident, be sure to classify it based on severity, impact, and the possible damages
* Setup a communication plan during the pre-incident planning process
* Define roles and responsibilities among the incident response team, this can involve who contacts outside aid, or who is responsible for updating the IR Coordinator
* Make sure the recommended actions are adhered to for the given incident
* Report and document the time, location, actions taking, outcomes, damages, and any other details pertaining to the incident
* Follow up the incident by reviewing the incident reports to find what could be updated in the response and recommended actions of the policy
* After the report is finalized, prepare and present information learned from incident

### IR Team Meeting

Based on factors discussed including severity, and confidentiality. An IR Team Meeting could be planned to address an ongoing incident or learn from post-incident reports.

Additionally, the IR Team meets once a quarter to go over and update policies and procedures. Then a member will submit changes and revisions to be approved by the team. These updates are expected to be based on performance of prior incident documentation as required per the IR team task-list.

### Incident Response Coordinator Task Checklist [6]

In an incident, the incident response coordinator is expected to keep the incidence response process going, as such there is a checklist for them to follow while responding to an incident:

* Track the progress of the incident response during the incident
* Coordinate the actions of other IR members, spreading information out as necessary, and preventing any IR members from interfering with other IR members in the process
* Provide status updates to relevant parties, such as any companies whose data might be in danger
* Provide expertise to the IR team by offering guidance and experience, or by distributing information from a subject matter expert.

The IR response coordinator should also be formally trained in responding to incidents and have prior experience with the IR process.

### Incident Response Recommended Actions

This section will be split into parts to denote recommendations for the more common natural disasters that may interfere with CB Solutions operations.

**Fires:**

* Locate the nearest exit plan, these can be found on the walls around elevators and stairways
* If the fire has not spread, quickly grab any documents as you calmy exit the building
* For communication, direct all information to the local IR head

**Floods:**

* Assuming the flood is not life threatening, locate and move all CB Solutions documents and, if possible, computers to higher ground.
* Contact the local IR head, and depending on escalation the regional IR head, and have them track the damages caused by flooding
* If flooding is localized to the building, invest in pumps to prevent future flooding from damaging more documents or servers.

**Storms:**

* In the event of larger thunderstorms, ensure all electronics are unplugged and all windows are kept shut
* If winds are strong ensure to also prep for tornadoes if expected in the region

**Tornados:**

* In the event of an early notification or alert, please secure all doors and windows
* After an alert of a confirmed tornado, immediately move to lower levels of the building or ask your buildings Safety Officer where the designated storm location is

**Hurricanes:**

* Similarly to tornadoes, secure all doors and windows
* Make sure all property is safe from getting damaged by water
* In the event of large hurricanes, boarding windows is appropriate in the effort of securing them

**Animal Infestation:**

* Factors in the type of infestation will determine immediate action
* Our custodial staff will be a point of contact in determining if an external vendor is necessary to be called or if it can be mitigated internally
* Our main priority in this event is employee safety and health, we will do everything in our power to ensure a clean and safe working environment

**Earthquake:**

* In the case of an earthquake follow recommended CDC steps
  + Incudes: staying away from outer walls, windows, and take cover under anything to protect from falling debris

### Pre-incident Preparations [2]

All Incidence Response team members must engage in tests on their responses to natural disasters. As part of pre-incident preparation, any CB Solutions location is required to adhere to safety standards. As such any CB Solutions location should always have the required detectors, anti-flooding equipment, sheltered rooms, and any other necessary preventative measures for the expected disasters of the region. There are a few requirements for all CB Solutions locations that can be considered pre-incident preparations, they are:

* Have visible escape plans on the wall in a visible location near any staircases or elevators
* Along with escape plans, floor layout plans should also be easily visible in the hallways of CB Solutions buildings.
* All buildings must maintain proper locations for the storage of documents, such as fireproof safes or rooms to protect CB Solutions, and customers, data and property.
* Fire extinguishers must be up to date, with at least one on each floor
* For flooding, any basements must have the proper drainage system assuming the region has flooding
* Every CB Solutions building must be kept to code to prevent other more regional disasters.

### Post-incident Maintenance Activities [2]

The head of the incident response team, contactable from HeadIR@CBSolutions.com, is responsible for documenting and communicating post-incident activities.

Post-incident maintenance and activities occur after the detection, containment, and recovery of any disaster incidents. This phase of IR is important as it involves reflection, compilation, and analysis of the activities that led to, or the possible prevention of, the incident. Important points to review and document are:

* Exactly what happened and when
* What information or property has been lost
* Are there any casualties to the disaster
* How well did the staff perform in dealing with the disaster
* With the above, are there any IR members who need to use better communication to prevent accidentally inhibiting the IR process
* Would earlier information or warning of disaster have helped
* Would further preparation, assuming the disaster was warned, have prevented more damages or were the damages caused unavoidable
* Are there steps that inhibited recovery
* What could be done differently utilizing the documentation and experience from the event
* What information should be shared to other companies
* What actions could prevent or mitigate this type of disaster in the future

Post-incident activities should be incorporated into training for all parties involved in the incident, such as victims, system administration, and especially the incident responders. Depending on the incident type, victims are not required to perform in training, these would be any victims that may be scarred by the incident and should not be required in extra training. Aside from training and the above steps, the post-incident activities should involve a gradual return to normal operations.

# ESCALATION [2]

The escalation process is intended to be used as a way of involving other appropriate resources as the details of the disaster increase in impact. Incidents should initially be handled at the lowest reasonable level that they can be responded to with as few resources required as to reduce total impact. This will help mitigate the cost involved with the incident. In more extreme disasters, responding with lower levels may be devastating to property and thus use caution when first selecting a severity. The table below defines the tiers of escalation and the associated members involved.

|  |  |  |
| --- | --- | --- |
| **Severity Level** | **Response Team Involvement** | **Description** |
| 0 (No incident) | * Local IR members | No current disaster, time is dedicated for planning and preparation |
| 1 (Low) | * Local staff and IR members | Low amounts of flooding or thunderstorms |
| 2 (Medium) | * Local staff * Regional IR members * Notify directors | The operations in the area are being hit by a severe storm or flooding |
| 3 (High) | * Local staff * Regional IR members * Notify directors * Request disaster aid | A severe natural disaster is hitting the location and local disaster aid will be necessary |

At any time during the incident response process, the Incident Response Coordinator, Director of Information Security, and the Chief Information Security Officer may be called upon to escalate any issue regarding the process or incident.

The Incident Response Coordinator and Chief Information Security Officer in consultation with OGC will determine if an incident should be escalated to external authorities. [5]

# APPENDIX

Incident Response Team:

|  |  |  |
| --- | --- | --- |
| Role | Leaders/Members | Contact Information |
| CISO | Steven L | ###-###-####  StevenL@CBSolutions.com |
| Incidence Response Coordinator | Bill J | ###-###-####  BillJ@CBSolutions.com |
| Local IR Branch Manager | [To be filled by each location] | [To be filled by each location] |
| Local response services | Police  Firefighters  Other Disaster Response Teams | 911, or the appropriate local phone numbers |

**Other Numbers / Contacts:**

* Intended to be filled by regional IR leaders
* -
* -
* -

# REFERENCES

Using IEEE since that was shown in the table of contents example

[1] “What is personally identifiable information (PII)?,” IBM, <https://www.ibm.com/topics/pii> (accessed Apr. 19, 2024).

[2] Example incident response plan, <https://www.michigan.gov/-/media/Project/Websites/msp/cjic/pdfs6/Example_Incident_Response_Policy.pdf?rev=4bf335b6d1344226a92a0947bc8688ec> (accessed Apr. 19, 2024).

[3] SANS Institute, “Cyber Security Incident Response Plan Cyber and Data Security Incident Response Plan Template.” Available: <https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf>

[4] “Incident Handling Checklist.” Available: https://www.hhs.gov/sites/default/files/incident-handling-checklist.pdf

‌

[5] Carnegie Mellon University, “Incident Response Plan - Information Security Office - Computing Services - Carnegie Mellon University,” *Cmu.edu*, 2014. https://www.cmu.edu/iso/governance/procedures/IRPlan.html (accessed Apr. 19, 2024).

[6] L. Zeltser, “The critical role of the Security Incident Response Coordinator,” Lenny Zeltser Content, <https://zeltser.com/information-security-incident-response-coordinator/> (accessed Apr. 19, 2024).

‌

‌