**SECURITY INCIDENT INVESTIGATION REPORT**

Table of Contents

[Incident Handler 3](#_Toc87713760)

[Incident Update 3](#_Toc87713761)

[Investigators 3](#_Toc87713762)

[Actions Taken 4](#_Toc87713763)

[Evidence found 4](#_Toc87713764)

[Parties Involved 5](#_Toc87713765)

[Incident Handler and Investigator Comments 5](#_Toc87713766)

[Findings 5](#_Toc87713767)

[MITRE Framework 6](#_Toc87713768)

[Notifications Made 6](#_Toc87713769)

[INVESTIGATION REPORT INSTRUCTIONS 7](#_Toc87713770)

# Incident Handler

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Date Report Received | | |  | Date Report Processing Began | |  |
| Name: |  | | | Report Number |  | |
| Title: |  | | | Department: |  | |
| Email Address: | |  | |  | | |
| Phone Number and, if Applicable, Extension: | | | |  | | |

# Incident Update

|  |  |  |
| --- | --- | --- |
| Incident Response Status | |  |
| Summary of Incident: |  | |

# Investigators

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Title** | **Organization** | **Phone** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Actions Taken

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Incident Handler/ Investigator** | **Action** | **Results** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Evidence found

|  |  |  |
| --- | --- | --- |
| **Date** | **Incident Handler/ Investigator** | **Evidence** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Parties Involved

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Organization** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Incident Handler and Investigator Comments

|  |  |  |
| --- | --- | --- |
| **Section 7: Incident Handler and Investigator Comments** | | |
| **Date** | **Incident Handler/ Investigator** | **Comments** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Findings

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Type of Incident (Based on MITRE) | | | | Credential Access | | Command and Control |  |
| Cause of Incident | |  | | | | | |
| Cost of Incident |  | | | | | | |
| Business Impact of Incident: | | |  | | | | |
| PHI Compromised? If yes, estimated num and actual num PHI Breach Impact: | | | | |  | | |
| Data Encrypted | | | | |  | | |
| Were the breach evaluation processes initiated? If yes, date of breach evaluation initiation: | | | | |  | | |

MITRE Framework

|  |  |  |
| --- | --- | --- |
| **Recommended By** | **Date** | **Recommended Corrective Action** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Use this report with MITRE Attack framework <https://attack.mitre.org>

# Notifications Made

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization** | **Point of Contact** | **Date of Notification** | **Summary of Information Provided** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# INVESTIGATION REPORT INSTRUCTIONS

* **Date Report Received** is the date that the Security Officer or Risk Manager first viewed the Incident Report.
* **Date Report Processing Began** is the date that the assigned Incident Handler began reviewing and investigating the Incident Report.
* **Report Number** should be assigned by the Security Officer. This Report Number should be noted on both the Security Incident Investigation Report and the Security Incident Report. If more than one Security Incident Report was filed for the same security incident, all the applicable Report Numbers should be listed on the Security Incident Investigation Report.
* **Current Status of Incident** may be an ongoing attack, one time occurrence, resolved issue, etc.
* **Summary of Incident** is the summary of all information known about the security incident/event at the beginning of the investigation process.
* **Parties Involved in Incident** should include all persons who were interviewed and all persons who were found to be involved in the incident.
* **Cause of Incident** may include misconfigured application, unpatched host, compromised user account, inappropriate user permissions, etc.
* **Cost of Incident** should include both the cost of the investigation including the time spent investigating and the cost of any actions necessary to mitigate the security breach including initial and ongoing costs.
* **Business Impact of Incident** could either be a description of the incident’s effect or an impact category based on the cost (major incident has a cost of over $250,000) as defined in the practice’s Security Incident Policy.
* **PHI Breach Impact** is based on either the estimated number of compromised PHI records or, if known, the actual number of compromised PHI records.
* **Description of Encryption** should include the encryption type. Compliance with the FIPS 140-2 standard; whether data was encrypted at rest, in transit, or both; and any other pertinent information.
* **Recommended Corrective Actions** includes ALL recommended corrective actions even if they were not acted upon. This will create a clear record of all corrective actions considered.
* **Actions Taken** should include, of course, only the recommended corrective actions that were acted upon.
* **Notifications Made** may include the CEO, the Board of Directors, Trustees, legal counsel, law enforcement, and employees. However, any breach notification as required in HIPAA regulations, including the American Recovery and Reinvestment Act’s (ARRA) Health Information Technology for Economic and Clinical Health (HITECH) Act, should be documented within the breach evaluation and notification procedure.