**Data Loss Playbook**

**Scope**

This Playbook covers the steps to take in case of Data Loss / Data Breach.

**1. Preparation**

**Summary**

- Create and maintain a list of:

- all domains owned by Organisation.

- This can prevent you from taking actions against our own domains

- all people that can register domains

- Create email template

- to notify all employees of ongoing phishing campaign against the organization

- to contact hosting organisation for domain(s) take down

- to inform 3rd party to take actions against phishing on their infra (Microsoft, Amazon, etc.)

- Ensure that:

- Mail anti-malware/anti-spam/anti-phish solutions are in place.

- Users know how to report phish

- Detection exists for office documents spawning processes

- PowerShell

- CMD

- WMI

- MSHTA

- Etc.

- Perform dry drills to ensure all aspects of the Playbook are working

- After publication

- At least once a quarter

- Test/Validate:

- Internal Contact and Escalation Paths

- Review threat intelligence for

- threats to the organisation,

- trends for the sector,

- common patterns

- newly developing risks and vulnerabilities

- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following

- IR Playbooks to highlight information security risks faced by employees, including:

- Phishing attacks and malicious emails;

- Ransomware;

- Reporting a suspected cyber incident.

**Tool Access and Provisioning**

**Tools**

Please referrer to [DCOT Handbook]

**Assets List**

- A list of assets and owner should exist and be available for the following

- Customers Assets

- Owners

- Contacts

- Pre approved/authorized actions

- Organisation Assets

- Owners

- Contacts

- Administrators

- Pre approved/authorized actions

- Type of assets inventory needed

- Endpoints

- Servers

- Network Equipment

- Security Appliances

- Network Ranges

- Public

- Private

- VPN / Out of Band

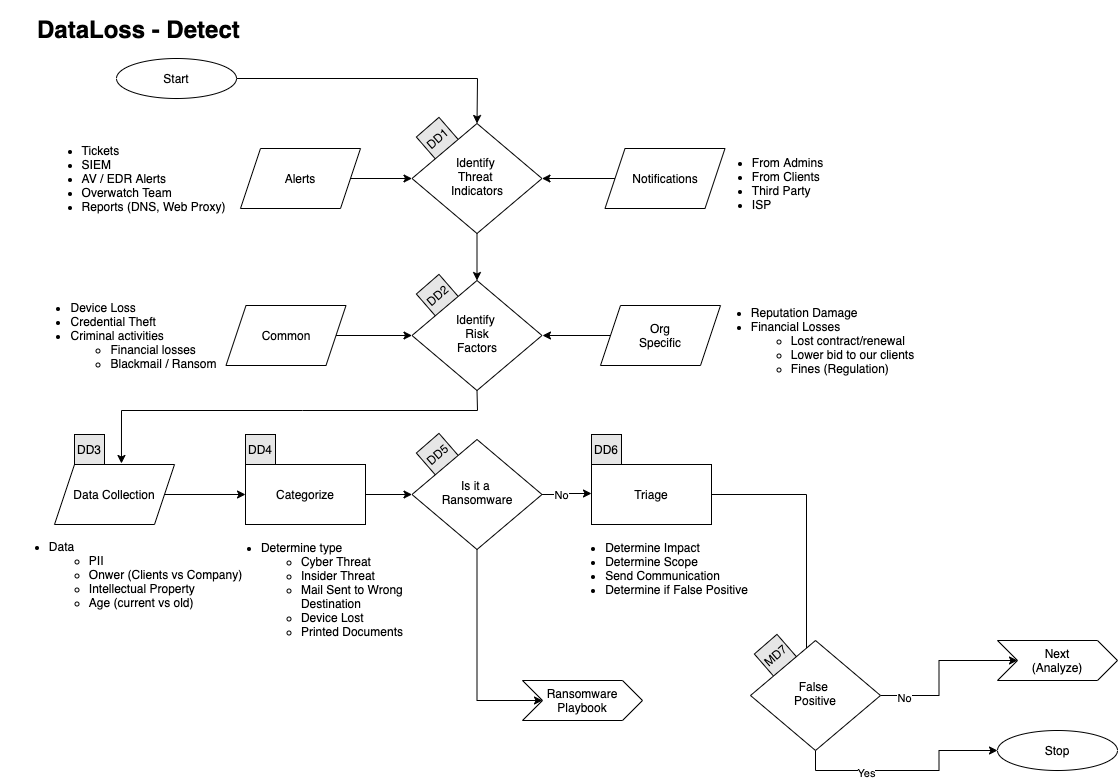
- Employees

- Partners

- Clients

**2. Detect**

**Workflow**



**Identify Threat Indicators**

**Alerts**

Alerts are be generated by different systems owned. The main sources for alerts are

- Tickets

- SIEM

- Anti-Virus / EDR

- Reports

- DNS

- Web Proxy

**Notifications**

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- System Administrators

- Clients

- Third Parties

- ISP

**Identify Risks Factors**

**Common**

- Credential Theft

- Device Loss

- Laptop

- Phone

- Criminal Activities

- Blackmail / Ransom

**Company Specific**

- Reputation Damage

- Financial Losses

- Lost of contract

- Contract not renewed

- Lower bid to our clients

- Fines

- Regulation

**Data Collection**

This section describes the information that should be collected and documented about the incident.

**Type Data**

- Personally identifiable information (PII)

- Intellectual Property

- Age of the Data

- Current

- Old

- Owner of the Data

- Company

- Clients

**Categorize**

**Determine type of Data Loss**

- Cyber Threat

- Insider Threat

- Mail Sent to Wrong Destination

- Device Lost

- Laptop

- Phone

- Printed Documents

**Is it Ransomware**

If the Data Loss is caused by a Ransomware, please refer to the **Ransomware Playbook**.

**Triage**

- Determine Impact

- Determine Scope

- Number of Documents / Records

- Number of Clients

- Number of Company Entities

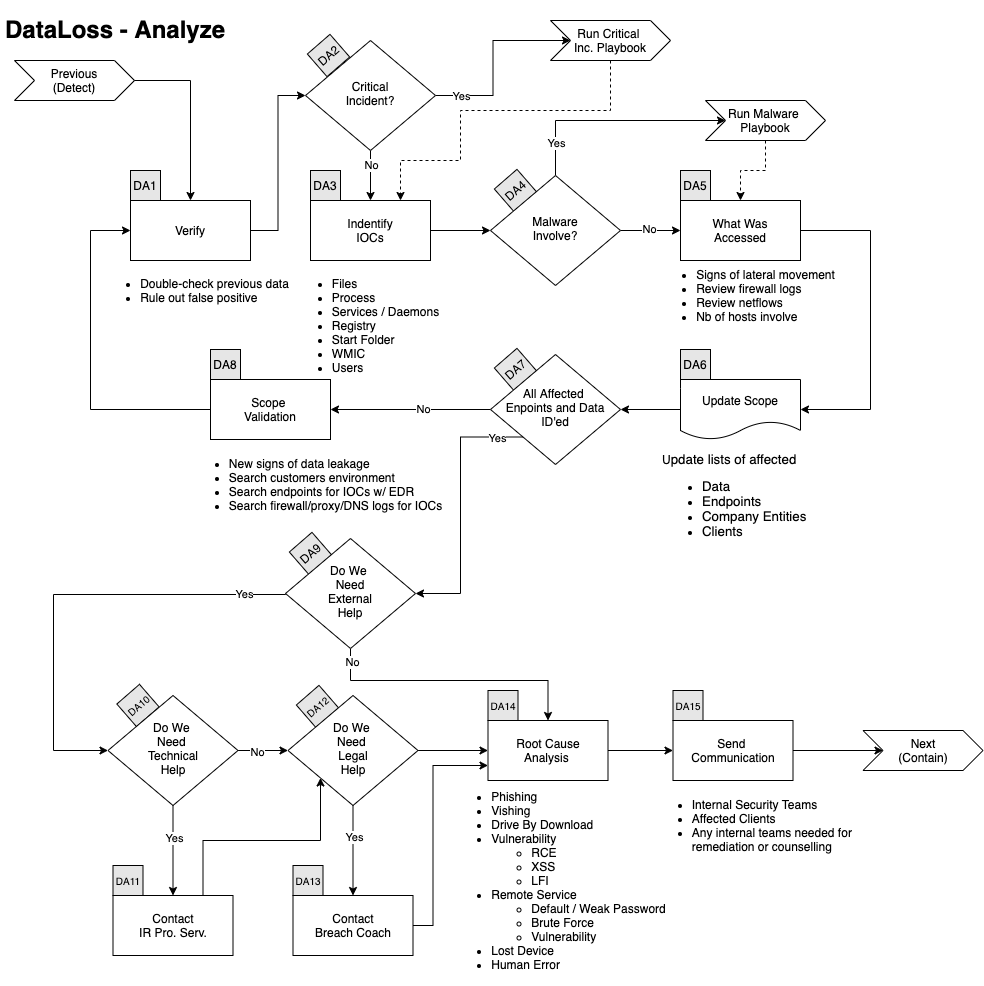
- Number of Individuals

- Send Communication

- Determine if False Positive

**3. Analyse**

**Workflow**

**Verify**

In conjunction with a senior member of the DCOT

- Double check previous data

- Rule Out False Positive

**Critical Incident**

If this incident is deemed \*\*Major or Critical\*\* by the senior analyst go to the **Critical Incident Playbook**.

**Identify IOCs**

- Data

- All Files Lost

- Records Stolen

- MFA Token

- Credentials

- PII

- Validate hashes

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- Validate links

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [URLScan](Tools)

- ID other addresses, domains, IPs

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [Intelligence](Tools)

- Search Threat Intel sources

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [Intelligence](Tools)

- Disk forensics on recipient's endpoint

**Malware**

If Malware was involved in the incident refer to the **Malware Playbook**.

**What Was Accessed**

**Did the attack touch other systems**

Look for:

- Signs of Lateral Movement

- Review Firewall Logs

- Review Netflows

- Assess the Number of Hosts Involved

- Number of Clients Affected

- Perform the same research for all affected clients

**Update Scope**

- Update lists of affected

- Data

- Endpoints

- Company Entities

- Clients

**Scope Validation**

Have all the machines and data been identified

If you find further traces of phishing or new IOCs go back to **Verify Step**.

When you are done identifying all:

- Data that was Lost

- Affected Endpoints

- Affected Company Entities

- Affected Customers

And if applicable investigated all:

- URLs

- Domains

- IP

- Ports

- Files

- Hash

You can proceed with the next steps.

**Root Cause Analysis**

Identify how this incident happened.

- Phishing Emails

- Voice Phishing

- Drive-by Download

- Vulnerability

- Remote Code Execution

- Cross-Site Scripting

- Remote Services

- Default / Weak Password

- Brute Force

- Vulnerability

- Lost Device

- Human Error

**Send Communication**

Contact any relevant of the parties

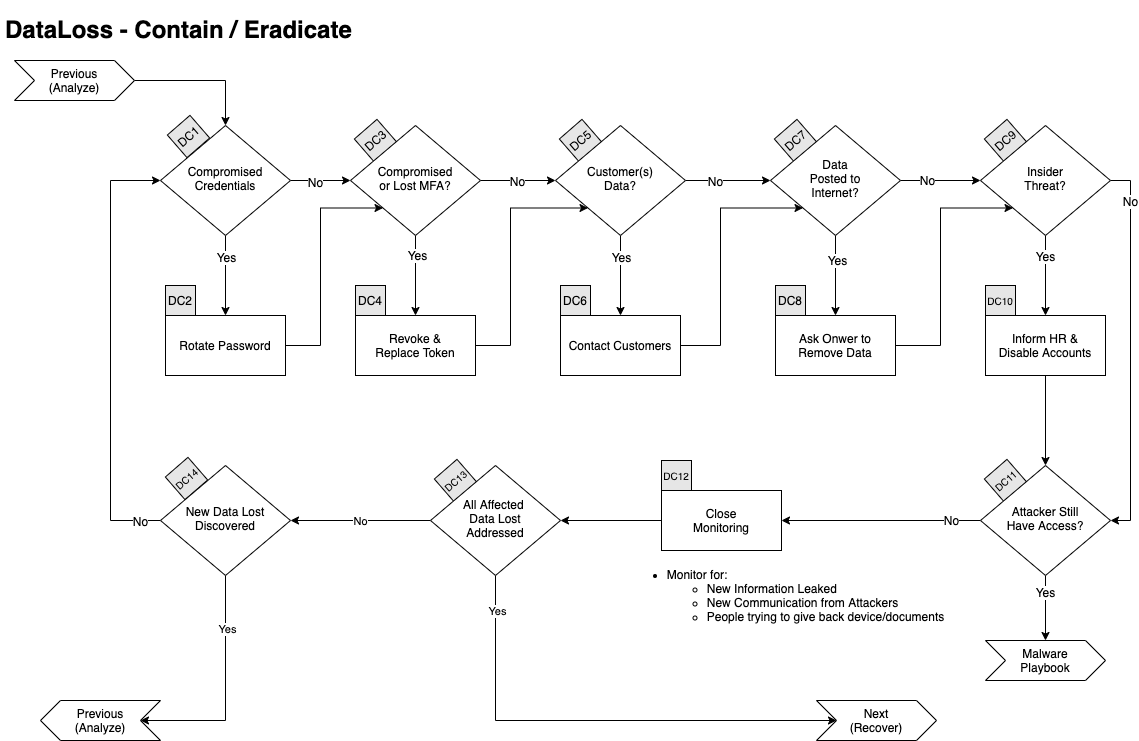
- 138 SIG SQN

- DCOT

Go to the next phase **Contain/Eradicate**

**4. Contain / Eradicate**

**Workflow**



**Compromised Credentials**

If any credentials are suspected to have been accessed, stolen or used they will all need to be changed.

This applies to:

- Local Passwords

- Network Passwords

- Remote Passwords

- Etc.

**Compromised or Lost MFA**

If any Multi Factor Authentication token/code were accessed, stolen or used they will all need to be

- Revoke

- Replace.

**Customer Data**

If any if customer data was accessed or leaked, we will need to send communication to all affected clients using the approved **Customer Communication Template.**

**Data Posted to the Internet**

**Insider Threat**

If the information was intentionally leaked/sold by an employee, we need to:

- Contact HR

- Disable User Account

- Disable any MFA token

We will potentially need to send physical security to the employee's desk to seize his/her laptop and other devices.

**Attacker Still Have Access**

If there is any sign of the attacker still being in the network, go to the **Malware Playbook**.

**Close Monitoring**

- Monitor for

- New information leaked

- New communication from Attackers

- People trying to give back device(s)/document(s)

**All Affected Data Lost Addressed**

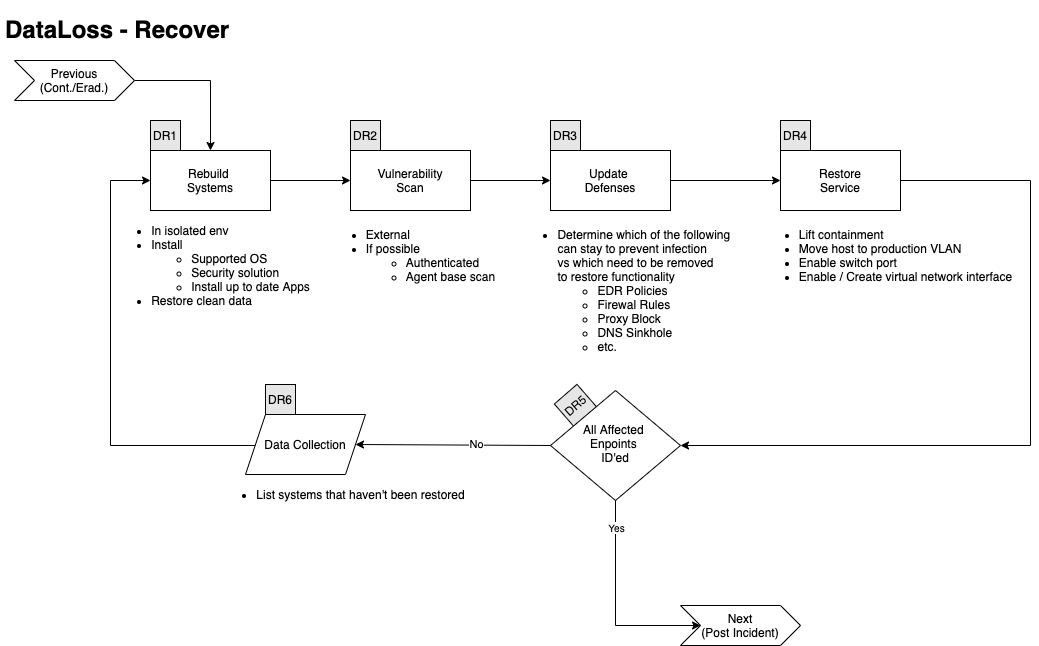
If all affected data have been addressed, you can go to the **Recover phase**, otherwise continue below.

**New Data Lost Discovered**

If there was new leaked data/devices discovered, go back to the **Analyse Phase**.

**5. Recover**

**Workflow**



**Rebuilt Systems**

In an isolated environment:

- Install

- Supported OS

- Security solutions

- Up to date applications

- Restore data (from a clean backup)

**Vulnerability Scan**

Perform:

- External VA

- If possible

- Authenticated scan

- Agent base scan

**Update Defences**

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Firewall Rules

- EDR

- Ban hashes

- Ban domains

- Containment

- Proxy Block

- DNS Sinkhole

- Etc.

**Restore Service**

Depending on the containment applied to the host, perform all the following that applies:

- Lift containment in EDR console

- Move host to production VLAN

- Enable switch port

- Enable/Create virtual network interface

- etc.

**All Affected Endpoints Restored**

If all affected endpoints have been restored, you can go to the **Post Incident** phase, otherwise continue below.

- List systems that haven't been restored

**Validate Countermeasures**

Determine if legitimate elements are blocked by:

- Proxy

- Firewall

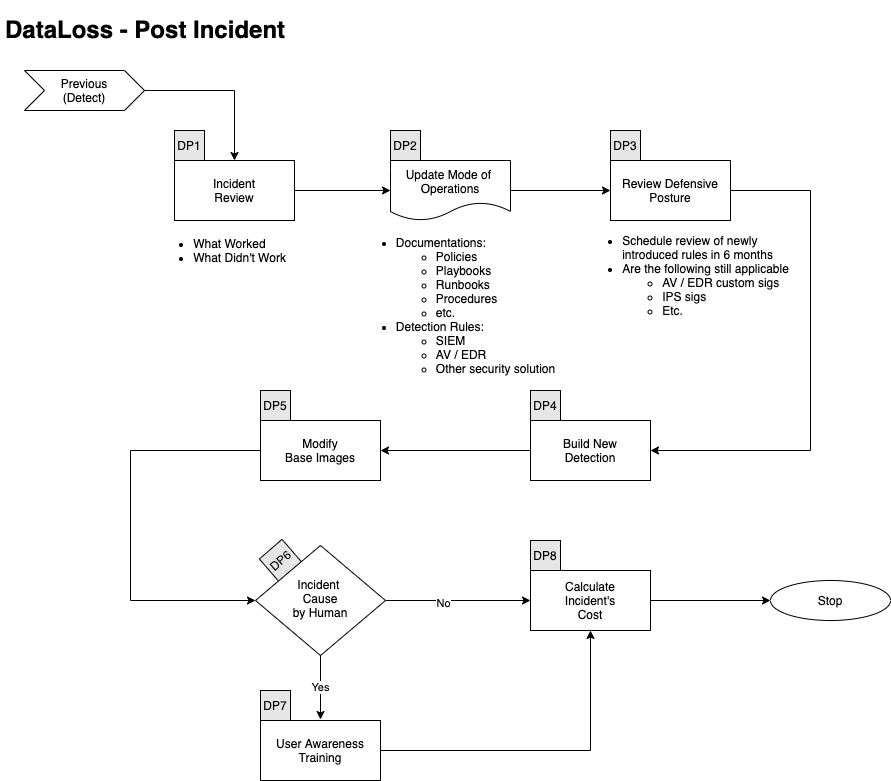
- EDR

If so, go back to **Update Defences.**

Otherwise go to the next phase **Post Incident.**

**6. Post Incident**

**Workflow**

**Incident Review**

- What worked

- What didn't work

**Update Mode of Operations**

Update the following documents as required:

- Policies

- Processes

- Procedures

- Playbooks

- Runbooks

Update Detection Rules in:

- SIEM

- Anti-Spam

- Malware Gateway

- EDR

- Other security solution

Review Defensive Posture

- Schedule review of newly introduced rules in 6 months

- Are the following still applicable

- Firewall Rules

- Proxy Rules for C2

- AV / EDR custom Signatures

- IPS Signatures

**Build New Detection**

If the Data Loss was not caused by a lost device, we need to build new detections

- Mail Service

- Anti-Spam / Anti-Phish

- ATT&CK Techniques

- etc.

Modify Base Images

If the Data Loss was caused by a lack of hardening or sufficient patch level:

- Review hardening processes

- Include critical patches in base Images

- etc.

**User Awareness Training**

If the incident was caused by a human error

- Create / Select new mandatory training

- Cyber Education Vendor

- From YouTube videos

- Built by internal teams

**Calculate Incident's Cost**

Calculate the incident's Cost

- Time Spent

- Ransom paid

- Downtime

- Fines / Penalties

- etc.

# References

This Playbook was built using the following references:

https://www.dfir.training/index.php?option=com\_jreviews&format=ajax&url=media/download&m=14tt1&1600804844570

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf