Preparation 1

Objective: Establish contacts, define procedures, and gather information to save time during the incident handling.

Contacts

- Identify internal technical contacts (security team, incident response team …)
- Make sure to have contact points in your public relation team, human resources team and legal department
- Identify external contacts who might be needed, mainly for investigation purposes (like Law Enforcement for example).

Security policy

- Make sure that the corporate information value is explained in the rules of the procedure, the IT chart, awareness and training session
- Make sure all valuable assets are identified as it should be
- Make sure that security incident escalation process is defined and the actors are clearly defined and identified.

Identification 2

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Data leak can occur from anywhere. Remember that the cause of the leakage can be an individual employee willingly or unwillingly bypassing security issues, or a compromised computer.

Step 1: DETECT THE ISSUE

- **Incident notification process:**

Internal information can be a good source of detection: employee confidence, security team identifying a problem, etc.

- **Public monitoring tool:**

A watch on Internet search engines and public database can be very valuable to detect information leakage.

- **DLP (Data Loss Prevention) tool:**

If there is a DLP tool in the company, it can provide valuable information to incident handlers working on information leakage.

Step 2: CONFIRM THE ISSUE

Don't do anything, without a written request from the concerned CISO/person in charge. Based on your legal team advisory, a written permission from the concerned user might also be handy.

- **E-Mail:**

The disclosure source could have sent data using his corporate e-mail address.

On the messaging system, look for e-mails sent to or received from a suspect account or with a special subject.
On the e-mail client on the desktop of the suspect (if available), use a tool which allows you to search by filtering out the "PRIVATE" flagged e-mails. If you really need to do so, ask the user for a written agreement or ask him to be with you.
When applicable, look through related log files.

Use forensic tools to check for deleted browsing history. Also check all the offline content left from all browsing.

Identification 2

- **Browsing:**

Data might have been sent on webmail/forums/dedicated websites.
On the proxy server, check the logs relating to the suspect account connections on the suspected URL used to disclose data.
On the desktop (if available), check the history of the installed browsers. Remember some people might have different browsers on the same desktop computer; be sure to check every browser history. If the moment of the data leak can be time-stamped, some log files can provide useful information.

- **External storage devices:**

A various number of devices can be used to store data: USB keys, CD-ROM, DVD, external hard disks, smartphones, memory cards…
Little information will be found concerning data transfer using these devices. The USB key used to transfer data can be referenced by the operating system. A forensic analysis can confirm the use of hardware but not the data transmitted.

- **Local files:**

If nothing has been found yet, there are still chances to find traces in the local file system of the suspect. Just like for e-mail researches, use a parsing tool which forbids any access to the PRIVATE zone of the user. If you really need to do so, act accordingly to local employment law.

- **Network transfer:**

Multiple ways might be used to transfer data out of the company: FTP, instant messenger, etc. Try to dig into log files showing such activity.
Data might also have been sent using a VPN tunnel or on an SSH server. In this case, one can prove the connection by watching log files but can't see the content transmitted.

- **Printer:**

Data can be sent to printers connected to the network. In this case, check for traces on the spooler or directly on the printer, since some constructors directly store printed documents on a local hard drive.

- **Malware:**

If nothing has been found, think of a possible malware compromission and act accordingly with the "Malware Detection" IRM.

Note: Even when enough evidence has been found, always look for more. It is not because you proved that data got fraudulently from A to B with one method that it wasn't also sent to C with another method. Also don't forget that someone else could have accessed the computer. Was the suspected employee actually in front of his computer when the leak occured?

Containment 3

Objective: Mitigate the attack's effects on the targeted environment.

Notify the management, legal and PR team to make sure they are prepared to deal with a massive or targeted disclosure.

Depending on the leakage vector, block the access to the disclosure URI, the disclosure server, the disclosure source or the disclosure recipients. This action must be done on all infrastructure points.

Suspend the logical and physical credentials of the insider if the leakage has been confirmed. Involve HR and legal team before any action.

Isolate the computing system (desktop, printer) used to disclose data in order to perform a forensic analysis later. This manipulation should be done the hard way: remove the electric plug (and the battery in case of a laptop).

Remediation 4

Objective: Take actions to remove the threat and avoid future incidents.

If data has been sent to public servers, ask the owner (or webmaster) to remove the disclosed data. Be sure to adjust your request to the recipients (hacktivism webmaster won't behave as a press webmaster)
If it's not possible to remove the disclosed data, provide a complete analysis to the PR team and the management. Monitor leaked documents spread on websites and social networks (FB, Twitter, etc) and Internet user's comments or reactions.

Provide the elements to HR team to eventually file a complaint against the insider.

Recovery 5

Objective: Restore the system to normal operations.

If a system has been compromised, restore it completely.

Eventually warn your employees or some local teams about the issue to raise awareness and increase security rules.

When situation comes back to normal, eventually remove the official communication.

Aftermath 6

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform hierarchy, subsidiaries and partners to share the best practices applied on this incident to enforce similar rules on other locations.

Report

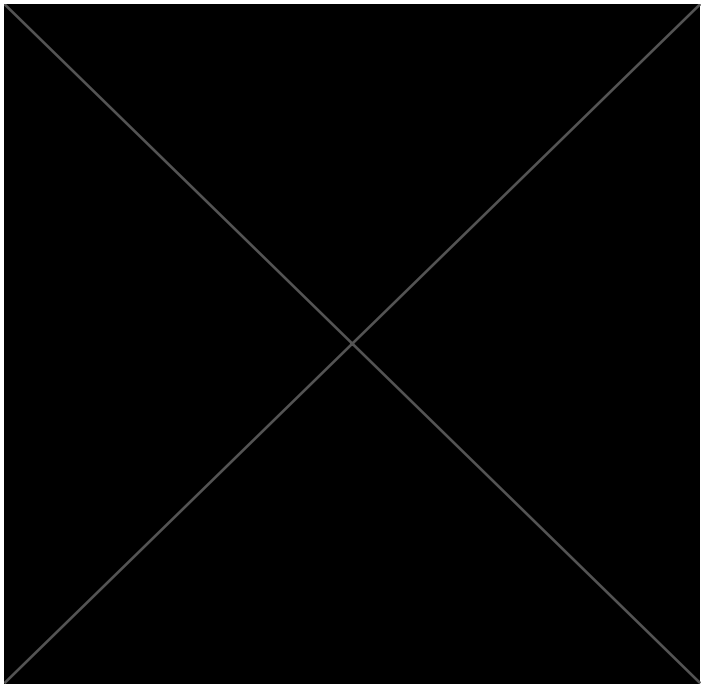
An incident report should be written and made available to all of the actors of the incident.

The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident impact

Capitalize

Actions to improve the information leakage handling processes should be defined to capitalize on this experience.



Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.
Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERT (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed:

Incident handling steps

6 steps are defined to handle security Incidents

- **Preparation: get ready to handle the incident**
- **Identification: detect the incident**
- **Containment: limit the impact of the incident**
- **Remediation: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.