Playbook – Data Loss/Theft

**<Insert Corporate Logo>**

**Document Version** 1.1 **Date**

**Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Change |
| 3/12/2016 | 1.0 | Josh Geno | Complete rebuild from prior “top-down” format. Re-written into flowchart format with detailed instructions in playbook doc |
| 3/20/2019 | 1.1 | Josh Geno | Changed to generic tool/process/department references; updated resources that have changed versions or have been superseded |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Introduction 4](#_Toc5350735)

[License 4](#_Toc5350736)

[Incident Lifecycle 5](#_Toc5350737)

[Prepare 6](#_Toc5350738)

[A1 6](#_Toc5350739)

[A2 7](#_Toc5350740)

[A3 8](#_Toc5350741)

[A4 8](#_Toc5350742)

[A5 9](#_Toc5350743)

[A6 10](#_Toc5350744)

[Detect 11](#_Toc5350745)

[B1 – B10 11](#_Toc5350746)

[B11 12](#_Toc5350747)

[B12 - B14 13](#_Toc5350748)

[Triage / Prioritize 14](#_Toc5350749)

[Note Regarding Rapid Assessment Methodologies 14](#_Toc5350750)

[Checkbox Assessment 14](#_Toc5350751)

[Weighted Assessment 15](#_Toc5350752)

[C1 – C8 16](#_Toc5350753)

[C9 – C15 17](#_Toc5350754)

[C16 - C18 18](#_Toc5350755)

[C19 19](#_Toc5350756)

[Analyze 20](#_Toc5350757)

[D1 20](#_Toc5350758)

[D2 21](#_Toc5350759)

[D3 21](#_Toc5350760)

[D4 22](#_Toc5350761)

[D5 22](#_Toc5350762)

[D6 23](#_Toc5350763)

[D7 24](#_Toc5350764)

[Contain/ Eradicate/ Recover 25](#_Toc5350765)

[E1 & E2 25](#_Toc5350766)

[E3 26](#_Toc5350767)

[E4 27](#_Toc5350768)

[E5 27](#_Toc5350769)

[E6 28](#_Toc5350770)

[E7 28](#_Toc5350771)

[E8 29](#_Toc5350772)

[E9 29](#_Toc5350773)

[E10 30](#_Toc5350774)

[E11 30](#_Toc5350775)

[E12 31](#_Toc5350776)

[E13 31](#_Toc5350777)

[E14 31](#_Toc5350778)

[E15 32](#_Toc5350779)

[E16 33](#_Toc5350780)

[E17 34](#_Toc5350781)

[E18 35](#_Toc5350782)

[E19 35](#_Toc5350783)

[E20 36](#_Toc5350784)

[E21 37](#_Toc5350785)

[E22 37](#_Toc5350786)

[E23 38](#_Toc5350787)

[E24 38](#_Toc5350788)

[E25 38](#_Toc5350789)

[E26 39](#_Toc5350790)

[E27 39](#_Toc5350791)

[E28 40](#_Toc5350792)

[E29 41](#_Toc5350793)

[E30 41](#_Toc5350794)

[E31 42](#_Toc5350795)

[Post-Incident 43](#_Toc5350796)

[F1 43](#_Toc5350797)

[F2 44](#_Toc5350798)

[F3 44](#_Toc5350799)

[F4 45](#_Toc5350800)

[F5 45](#_Toc5350801)

[F6 46](#_Toc5350802)

# Introduction

This playbook is the text compendium to the Data Loss-Theft response flowchart.

It provides needed details, explanations, and external resource links for the various components called out in the flowchart. This guide and flowchart are not intended to serve as a full Security Incident Framework or response process, it contains components specific to data loss and theft response.

To maximize the value of the response flowchart and this guide, it must be modified to reflect your organization’s incident response process/framework, the roles and responsibilities of individuals in your organizational structure, security tools, and TTPs (Tactics, Techniques, and Procedures) present in your environment.

This Playbook can be automated by most incident management platforms. Incident management platforms that can also automate information collection from security tools will be of particular value during an actual incident.

For the purposes of this document, data loss is the condition where data is not available for normal use due to its erasure/deletion, or movement (as opposed to copying) to an unexpected place. Data corruption is the condition where data contents have been either unintentionally or maliciously altered. Data Theft is the condition where data has been maliciously exfiltrated outside of corporate control by one or more internal or external bad actors. Data leak is the condition where data has been exfiltrated outside of corporate control, but the bad actor does not have malicious intent.

Hackers have decades of prior art to drive innovations today. Be prepared.

The author assumes no liability for the content, quality, relevance, fitness for purpose, or accuracy of any materials used in this document and assumes no liability for any real or potential harms associated with use of the document or flowchart.

## License

This work is licensed under  [Creative Commons Attribution-ShareAlike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)

https://creativecommons.org/licenses/by-sa/4.0/

**Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

**ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

**No additional restrictions** — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Copyright 2016, 2019 Joshua C Geno

# Incident Lifecycle

This data loss-theft response guide uses a standard incident lifecycle including preparations to prevent, detect, and respond to a malware threat. Post-incident lessons learned are fed back into the lifecycle as continuous improvement measures.

Again, the flowchart and guide are not meant to capture the entire incident response function, only those components specific to detection and response for a data loss or theft incident. For a comprehensive IR framework, reference SANS Incident Handlers Handbook, Carnegie Mellon’s Handbook for Computer Security Incident Response Teams, or ENISA’s Good Practice Guide for Incident Management.

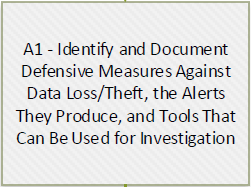


# Prepare



The prepare phase includes activities and protective measures that should be put in place prior to an incident. It also includes activities and protective measures incorporated from post-incident activities following an incident.

The more time analysts and engineers spend in prepare, the less time they’ll spend in response when an actual data loss or data theft incident happens.



A1 - In this step the organization should take a close look at their inventory of security and infrastructure tools that can detect and prevent data loss/theft or aid the investigation of an incident. Look at the threat carefully from a defenders point of view. (blue team) Document these tools and a few samples of the type of alert or notification that can be expected. Document sample investigation queries/reports/etc. that engineers can run for each tool with ‘how to’ instructions so there is a quick reference during an incident. Collect any supporting information (network diagrams, crown jewel assessments, asset inventory, etc.) that will help with decisions during an incident and regularly update them.

This information can then be called out in multiple phases:

* Later in the prepare phase to fill gaps and bolster response capabilities
* The detect phase as a feed-in for threat indicators/alerts
* The analyze phase as tools to help positively ID a data loss or theft event
* The contain/eradicate/recover phase as tools to help isolate compromised credentials or compromised systems; identify data sets that have been lost, stolen, leaked, or corrupted.

In all phases the output of one tool, such as a file hash or URI, can be used to enrich or correlate information in other tools. This will be highly dependent on the tools your organization has implemented and the level of automation between the tools.

Don’t forget to include non-technical alerts, such as user reports or external notifications from business partners or law enforcement.

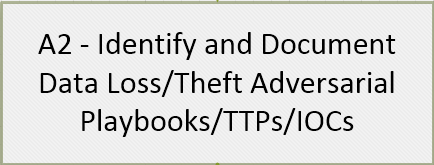
Resources:

<https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure>

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 36)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 44)

<https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM_English_Pack.zip> (IRM 11)



A2 - This step is about looking at the threat from the attacker’s point of view. (red team)

The more responders understand how the organization can be attacked the better they can fill gaps, tune security tools and procedures, and the better they can respond to an attack. Collect and share adversarial playbooks from actual attacks. Research TTPs related to malware. Collect IOCs (Indicators of Compromise) and search for them in the environment.

Verizon releases an annual data breach report that contains details of actual attacks. It is an excellent source of adversarial playbooks, which they call attack patterns. Search for their case studies (registration required) for an in-depth look at how a particular breach unfolded. There are many other security researchers that release similar reports.

There are also many public sources of IOCs such as “IOCs”, FireEye’s publicly shared IOC repository. Free/Open source tools to scan the environment include Redline and Loki.

Resources:

<https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

<https://github.com/fireeye/iocs>

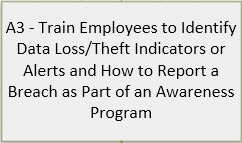
<https://www.fireeye.com/services/freeware/redline.html>

<https://github.com/Neo23x0/Loki>

<https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure>

<http://www.ten-inc.com/presentations/invincea1.pdf>

<https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM_English_Pack.zip> (IRM 11)



A3 - If your organization has not already done so, implement an awareness program that includes safe data handling, transmission, and destruction training as part of that awareness program. At minimum, every person in the company should be aware of basic indicators of data loss or theft and know how to report it to IT security. The program should also stress the importance of disk encryption.

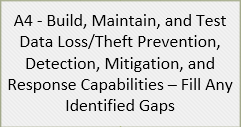
Resources:

<https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf>

<https://insights.sei.cmu.edu/insider-threat/2017/06/security-awareness-and-training-part-9-of-20-cert-best-practices-to-mitigate-insider-threats-series.html>

<https://www.csoonline.com/article/2133408/data-protection/network-security-the-7-elements-of-a-successful-security-awareness-program.html>

<https://www.wombatsecurity.com/blog/security-awareness-training-best-practices-to-consider>



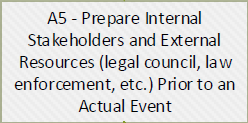
A4 - In this stage, run tests against the previously identified security tools and TTPs to gauge detection and response capability. Make sure analysts and responders are getting expected detections and alerts. To test response capabilities, run tabletop exercises. Identify gaps in detection, alerting, and response and make plans to fill them.

Resources:

<https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure>

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 61)

<https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf>



A5 - The first time incident responders contact internal teams or external resources shouldn’t be during an actual incident. Stakeholders, such as management, other corporate teams, internal privacy/compliance, internal or external legal resources, SecaaS/incident response vendors, etc. should be regularly engaged to discuss the role they play in incident response, and regularly briefed about the Security Operations Center activities. Ideally, they should also be included in response tests or tabletop exercises.

External resources, such as local, state, or federal law enforcement are likely not able to be part of your internal response testing, but should still be considered as part of the process and called out in appropriate steps. It is beneficial to reach out to them every couple of years to maintain general awareness. They can help you understand who can help with various problems and what resources are available.

Sometimes law enforcement shows up to local security conferences or have their own security events. Make use of these opportunities.

Document stakeholders and what role they may be called to play. Communicate incident response expectations and find out what expectations they have of the SOC when requesting resources during an incident. Keep stakeholders informed as to the activities and capabilities of the SOC. See page 11 of the agoria.be document below for an example of a Skills / Responsibilities / Roles chart.

Resources:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 18)

<https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-3/preventiand-response-twopronged-approach-cyber-security-and-incident-response-planning.html>

<https://www.sans.org/reading-room/whitepapers/legal/legal-considerations-creating-incident-response-plan-37487>

<https://www.agoria.be/upload/agoriav3/Cyber-Security-Incident-Management-Guide-2015.pdf> (pages 11 and 13)

<https://www.halkynconsulting.co.uk/a/2015/12/incident-response-key-stakeholders/>



A6 – The ability to repel or recover from a data loss or theft attack hinges on your organization’s ability to maintain superior security practices.

An excellent reference for comprehensive data loss/theft prevention techniques is NIST’s Special Publication 800-53. There is a specific listing of relevant controls in SP80-122, in section 4.3 (page 29 of the PDF). The PDF is available here:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>

At a high level, organizations need to be able to:

* Enforce Access Control and Least-Privilege
* Audit actions taken by users.
* Have the ability to restore deleted or corrupted data.
* Continuously reduce your organization’s attack surface. (patching, penetration testing, etc.)

Many security compliance frameworks will have these security hygiene measures documented, keep this information available and updated. If your organization does not have this documentation available, document it here for future reference.

Resources:

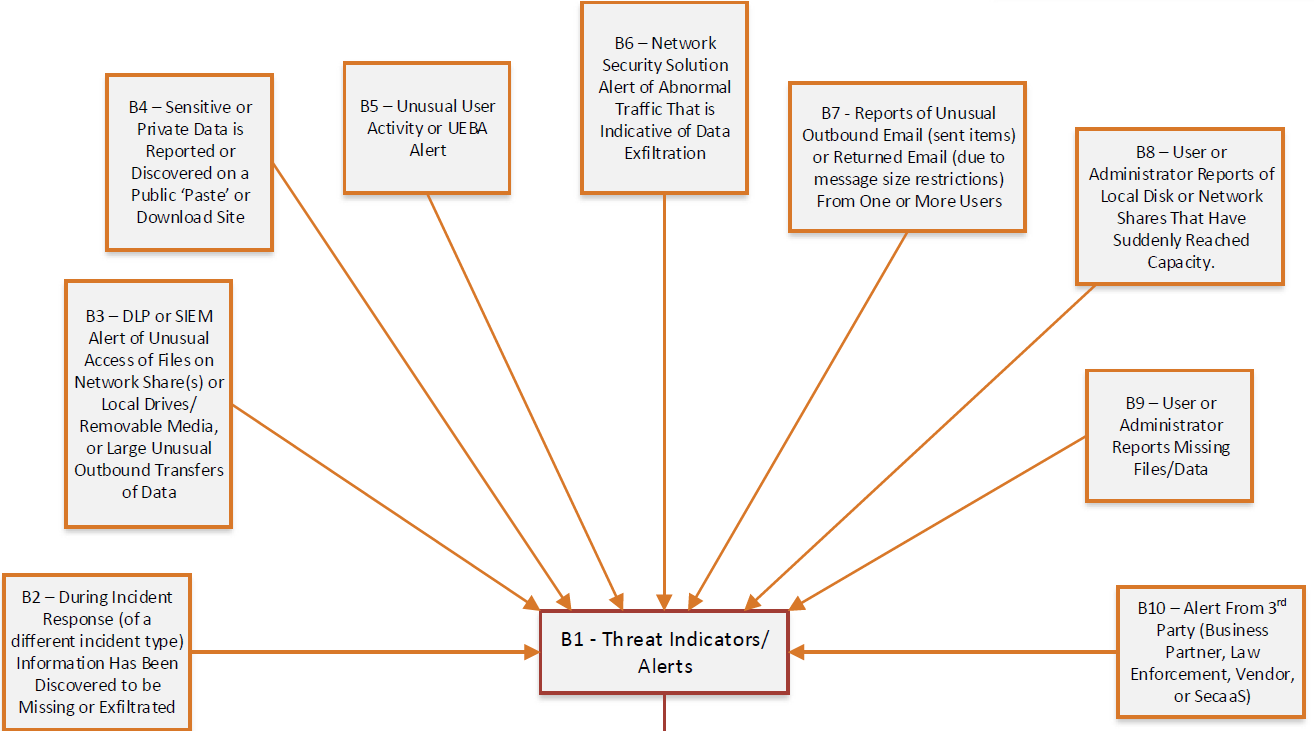
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<https://americansecuritytoday.com/employees-leave-best-practices-preventing-data-theft/>

<https://i-sight.com/resources/top-20-tips-for-preventing-data-theft/>

# Detect

The detect phase covers receipt of an alert or notification and the initial data gathering to validate that an actual data loss/theft incident has occurred.



B1 – B10 – The threat indicators, technical alerts, and manual notifications identified in A1 are inputs to B1. Many of these are common among organizations and should appear in every Data Loss/Theft playbook. Some are specific to the tools, 3rd parties, and organizational structure of a single organization. Take time to periodically review these inputs to prune or add entries as your available tools and TTPs change and make sure they all work as expected.

If the source or content of one or more of the inputs (B2 – B10) is not crystal clear to everyone on the security team, use the information identified in A1 to individually document the source and alert in this part of this document to aid responders.

Once an indicator is observed, alert is triggered, or notification is received, incident response is initiated.

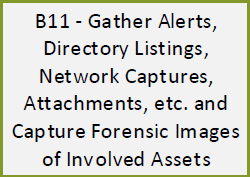
Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 34)

<https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM_English_Pack.zip> (IRM 11)

<https://www.incidentresponse.com/workflows/download/Data_Theft.pdf>

<https://www.incidentresponse.com/workflows/download/UnauthAccess.pdf>



B11 – Utilize the information and context available in the indicator/alert/notification to guide the initial data gathering activities. For instance, if you received an alert from your DLP suite that there is traffic on the firewall that indicates a server is uploading files to a Dropbox account, use the source information to identify the affected endpoint. From there, use available tools and network logs to evaluate whether an internal user was logged into the server, or if the upload command originated from an external source. If remote tools are not available in your environment, send someone (or acquire the endpoint) with appropriate skills to put hands on the keyboard to gather suspect files/hashes, email attachments, web history entries, packet captures, descriptions of unusual behavior, etc.

If the cause of the indicator/alert/notification is not immediately obvious, utilize automated scripts to rapidly collect indicators, such as Bambiraptor.

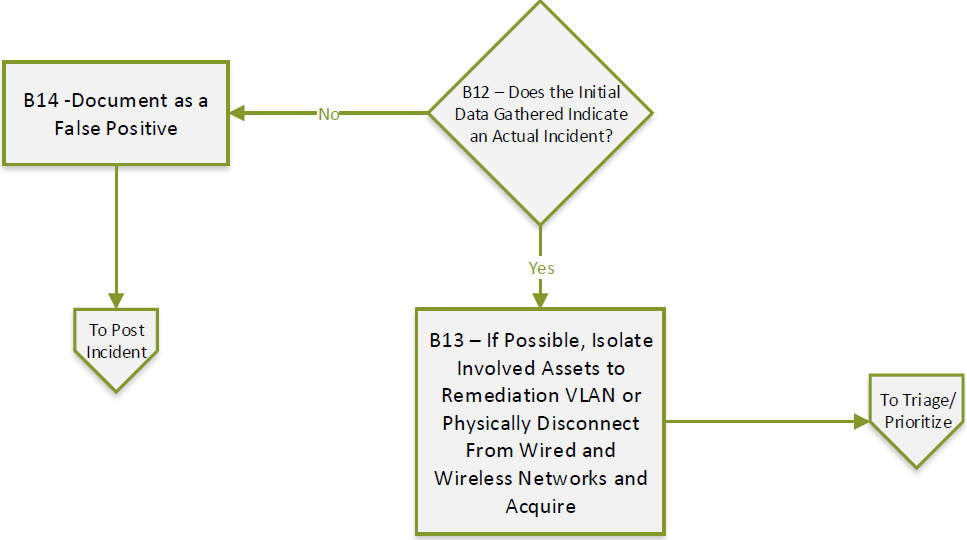
<https://www.brimorlabsblog.com/2016/12/live-response-collection-bambiraptor.html>

Gather as much information as is necessary to make a determination as to whether the indicator/alert/notification is a false-positive or an actual incident. Being familiar with data loss/theft mechanisms (A2 above) will help responders zero in on relevant facts quickly.

Your organization may have tools and TTPs related to gathering initial data. If so, document them here.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 34)



B12 - B14 – If there is no evidence of a data loss or theft event after the initial data gathering and the indicator/alert/notification can be attributed to a false-positive (user observed strange behavior and called ‘just in case’, new rule from a DLP or network tool vendor, etc.), document the incident as a false positive and move to F4 in Post-Incident.

Post-Incident is still required for false-positives as documentation may need to be updated, tools may need to be tuned or rules adjusted, and stakeholders (system owners, end users) will certainly need to be told that there is no security problem.

If enough evidence has been gathered to make a determination that one or more systems may have been involved in a data loss/theft event, consider isolating suspect systems, credentials, devices, etc. to stop more information from being lost or leaked. If you have remote tools isolate systems via remediation VLAN, or disconnect the system from all wireless and wired networks and remove/unplug directly attached storage devices. (USB storage, IoT, PLC, printers, mobile devices, etc.)

For cloud services, most come with a built-in firewall that can be configured to cut off public access. Be sure you don’t accidentally cut off your own access while locking network traffic down.

Any external storage device that was attached should also be considered to part of the loss or leak until enough additional evidence and forensics is collected to rule it out.

Ideally the devices physically removed from the network should be pulled and acquired by responders to prevent ‘proactive’ users from plugging them back in. A good stakeholder communication plan as part of your incident response function and a sticky note on the device or monitor (where possible) will go a long way toward keeping data sources out of the production network until the device can be acquired or remediated.

Your organization may have tools and TTPs available to remotely help with isolation to a remediation VLAN, if so document them here.

If your organization has a specific procedure for disconnecting wireless and wired network connections and physically acquiring devices, document them here.

Document your remote tools and TTPs here.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 44)

# Triage / Prioritize

The Triage/Prioritize phase covers the assessments that need to be quickly performed in order to prioritize the new/current incident in relation to other incidents already in the security incident queue.

This is also the phase where it is determined whether or not internal or external teams need to be notified of an incident. This playbook doesn’t cover the specifics of who should be contacted and what information to share with them; that is for your larger Incident Response Program to decide. This is the place we call out as appropriate to make the determination as to whether the notification portions of the Incident Response Program require action.

### Note Regarding Rapid Assessment Methodologies

The two rapid assessments below, C1 and C9, can be effectively performed two ways. Which way your organization uses will be determined by organizational needs for the level of granularity required and rate of incidents your organization handles at a time.

### Checkbox Assessment

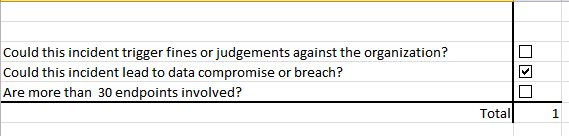
For organizations that handle few incidents at a time, an express assessment method can be used as a ‘tie-breaker’ for those few occasions where there is more than one incident in process, but there aren’t enough resources to service all of them. Each of the inputs is turned into a question and given a checkbox where it is checked if the condition is true. At the end you simply add up all the checked boxes for a score. The higher the score, the higher the priority.

Estimated number of endpoints isn’t easy to capture in a checkbox, so you have to reframe the question to “Are more than X endpoints involved?” Obviously this isn’t a one size fits all situation; you will have to come up with a number for your organization where more than that number signifies a critical situation.

The others are easy to turn into questions, such as:

* Could this incident trigger fines or judgements against the organization?
* Could this incident lead to data compromise or breach?
* Is sensitive data potentially involved?

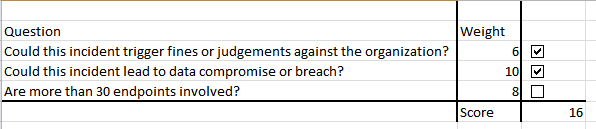
A simple spreadsheet is enough to capture responses and final score. Alternately, many case management systems allow you to setup data capture steps as part of an IR workflow.



### Weighted Assessment

For larger organizations that handle many incidents at a time and are able to run multiple responses at a time, weighted assessment provides a better level of granularity for assigning priority and the order in which incidents will be taken from the queue.

This methodology can also spark holy wars as to what weight should be given to each input. To get started stakeholders have to come together and agree on the weight of each question posed by each input. I recommend a weight of 1 -10. Invariably, one stakeholder will feel that one of the inputs, say Loss of Productivity, should be a 1 whereas a different stakeholder feels it should be a 10. However your organization gains consensus for these situations, the end goal is the same; weight each of the inputs so that when it’s question is checked, that weight is added to the total. Incidents can then be listed highest to lowest score where highest score is highest priority and will be taken by the next available responders from the queue.





C1 – C8 – The first rapid assessment concerns the organization’s expectation of potential loss due to the incident. In case the meanings of each input are not clear, here is a brief explanation of each:

* Reputation Damage – Potential for loss to repair the organization’s reputation (PR firm, advertising, etc.) May include indirect losses of lost business due to reputation damage.
* Fines/Judgements – Potential losses incurred by violating contractual agreements where there is a financial penalty, or regulatory fines.
* Loss to Replace or Repair – Potential losses incurred when systems are not available while being replaced, remediated, etc.
* Loss of Productivity – Potential loss of man-hour productivity while systems or hardware are not available for use.
* Loss Due to Legal Response – Potential loss incurred to hire lawyers, pay court fees, or potential punitive judgements.
* Loss of Competitive Advantage – Potential losses due to intellectual property or corporate secrets being leaked.

Tally the loss expectation score using the chosen assessment method above, it will be needed in C16.

Resource:

<https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model>



C9 – C15 – The second rapid assessment covers a severity assessment that will later be added to the loss assessment to determine priority. The severity assessment covers attributes of the incident itself rather than the business impact of the incident.

Additionally, it is time for responders to decide if external notifications are required or external/3rd party resources should be engaged since questions are already being asked about data compromise/breach and whether or not sensitive data is involved.

In case the meanings of each input are not clear, here is a brief explanation of each:

* Possibility of Data Compromise / Breach – Possibility that corporate data could be stolen, tampered with, or deleted. The systems involved and what function they serve should be taken into account.
* Estimated Number of Endpoints Involved – An order of magnitude assessment that is relative to the size of your business. 1 infected workstation in an organization of 10 total workstations is a much larger percent of infected hosts than 1 in a 50,000 workstation organization.
* Customer Impact – The possibility that the incident will impact your customers in some way. This could be direct financial impact or indirect impacts, such as a service being unavailable.
* Sensitive Data Involved – The possibility that protected classes of data (health, education, govt ID) or sensitive internal data (corporate secrets, intellectual property) could be affected by the incident.
* Recoverability – The relative possibility that damage caused by the incident can be reversed, rebuilt, or halted. Check the box on the checklist if recoverability is difficult, time consuming, resource consuming, or impossible.

Tally the severity assessment score using the chosen assessment method above, it will be needed in the next step. If the decision has been made that notifications are required or additional resources need to be pulled in, follow the procedures in your organization’s larger Incident Response Program to engage them.



C16 - C18 – Add the two scores calculated in C1 and C9. This is the incident’s priority score. Document this score and the two component spreadsheets from C1 and C9 in the incident documentation (Your Incident Response Program should have procedures and templates for this) and in your ticketing / case management system.

If this incident rates higher than the other items already in the queue then it takes precedence over other incidents and progresses to the Analyze phase. If it rates lower than other incidents in the queue, is added to the queue for later investigation and remediation. Any incident artifacts (data gathered, alerts, etc.) should be documented for later retrieval per your Incident Response Program’s requirements.

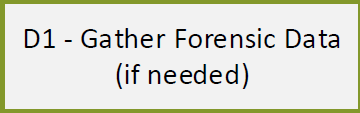


C19 – For incidents in the queue where responder resources have become newly available to investigate the next incident, this is the place in the playbook where the queue feeds in for data loss and theft events. Any data loss and theft event in the queue will have already been through the playbook up to this point.

Responders take the incident with the highest priority score in the queue and advance it to Analyze.

# Analyze

In the Analyze phase responders will utilize internal and external resources to identify the source of the breach. We want to find out if malicious code was used to execute the loss or theft, and call that playbook to clean up the malware before continuing the loss/theft playbook. It is exceedingly difficult to contain data loss or theft if there is underlying malware tearing through your infrastructure. The information collected in this phase will be used in the next phase to regain positive control over systems or credentials involved in the incident and recover information.



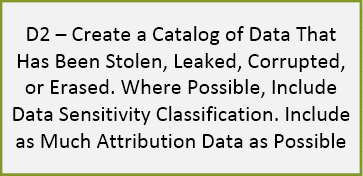
D1 – To identify additional assets involved in the incident in the next step, forensic data must be collected from known involved systems and checked for signs of lateral movement, credential use/misuse, and signs of unusual data movement, exfiltration, or erasure. Collect forensic images for any systems that weren’t taken in the Detect phase and for newly found systems.

Be sure to gather forensic data related to the Operating System/Software Environment (browser history, persistence mechanisms, etc.), Network (packet captures, security tool alerts/logs, involved credentials, etc.), and file system. (hashes of suspect executables, leaked/stolen files, etc.)

Document your organization’s tools and TTPs related to gathering and analyzing forensic data here. Include supporting tools and TTPs that help you follow an attacker or malicious code as it pivots throughout your environment.

Resource:

<https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps>

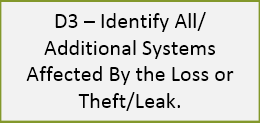


D2 – Create a catalog of stolen, leaked, corrupted or erased data. Be as specific as possible and include details such as device/network path, URI/URL, file hash if possible, sensitivity classification, and whether it contained protected data. (health, state/federal ID, financial, etc.)

This catalog will likely grow as you work through the Analyze, Contain, Eradicate, and Recover Phases. The primary use of this catalog is to feed the activities in D6, but the information will also be needed later if data needs to be restored or tracked on its journey through multiple internal and external systems. It may also be required if a 3rd party is engaged to monitor leaked/stolen data where take-down notices were not effective.

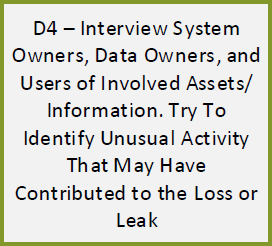
Be sure to include as much attribution information as possible (logs of the data moving or changing, tools used to move, corrupt, or delete data, etc.) to help create a suspect list.

Document the catalog as part of your incident artifacts per your Incident Response Program requirements.



D3 – Utilize the information collected in the Detect phase, D1, and D2 to widen your investigation and find additional systems, credentials, data, etc. involved in the incident. Gather the low-hanging fruit here and then move on. There will be additional widening of the scope of the investigation later.

Document your organization’s tools and TTPs related to following an attacker or malicious code as it pivots throughout your environment here. Add any newly discovered systems, credential, and data involved in the leak/loss as part of your incident artifacts per your Incident Response Program requirements.

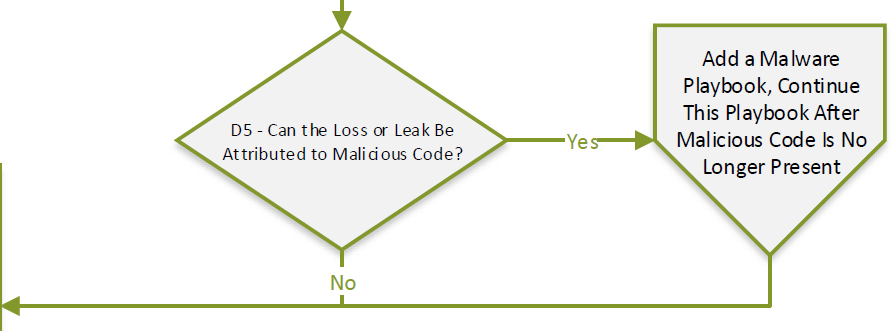


D4 – In this step the incident response team widens the investigation to include people involved in the incident. The idea is to collect observations about how the loss/leak entered and moved throughout your environment.

While logs and packet captures provide definitive clues as to what happened and when, human observation is still important to help find breakdowns in policy or procedure, human-centered security gaps, and opportunities to enhance your security awareness program.

Keep in mind that, in the case of insider threat, the information given to the incident response team may be false or misleading.

As in other steps and phases, document everything users and system administrators tell you as part of your incident artifacts per your Incident Response Program requirements.

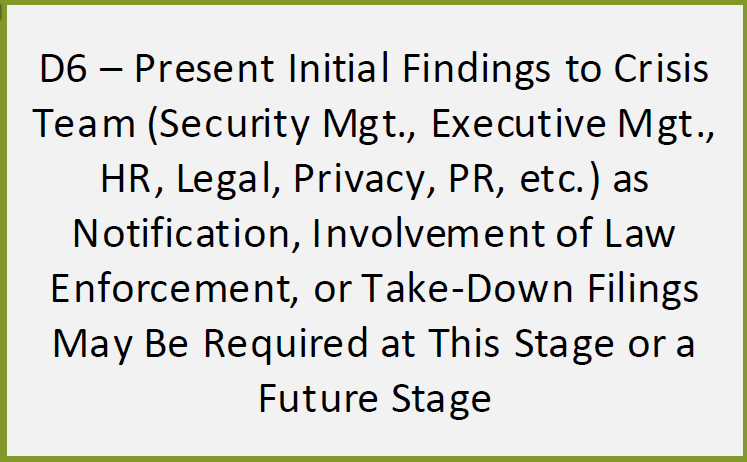


D5 – If the collected information and evidence points to malicious code being a vector of the data loss or leak, now is the time to add a malware playbook. This (Data Loss – Theft) playbook will pause until the malware infection is eradicated as it is not possible to contain eradicate and recover form a data leak incident if the malware causing the leak is still running rampant.

Once the malware is eradicated, move on to D6.

If malware does not appear to be involved, move on to D6.

Any findings from malware detection tools or investigation should be formatted as a write-up and be documented as part of your incident artifacts.

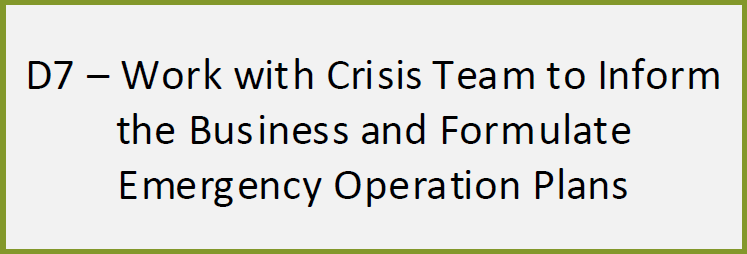


D6 – By now the investigation team should have enough information about the scope of the incident and what data was leaked or lost to meet with the corporate Crisis Team to present the initial investigation findings. The exact makeup and function of this team should already have been codified and solidified in your larger incident response program. The Crisis Team is generally made up of critical business management functions such as Information Security Management, Executive Management, Human Resources, Legal, Privacy, Compliance, Public Relations, and leaders from critical customer-facing business units.

Use the information collected so far and work with the Crisis Team to identify worst-case scenarios and implications of the incident. The scenarios and implications should address (at minimum) customer impact, business operations, technical operations, public data leak, and compliance/regulatory implications. Additionally, products and services affected should be identified that are or will be affected.

The Crisis Team may be required to take actions at this point to involve or inform law enforcement, customers, government agencies, service providers, etc. The job of the incident responders at this step is to support their actions and keep communication flowing to the Crisis Team as incident resolution progresses.

Document Crisis Team actions, law enforcement involvement, worst-case scenarios, incident implications, services affected as incident artifacts per your Incident Response Program requirements.



D7 – In this step the Crisis Team initiates communicate with the larger business to explain the scope and the effects of the data loss or leak. Who initiates these communications and what they say should already have been decided long ago as part of the larger Incident Response plan. If not, these communications will have to be crafted on-the-fly

Incident Responders will move on the next phase while the Crisis Team does its job but will still be available in a supporting role. Two-way communication becomes crucial between the two teams.

The Crisis Team will also work with the business, system owners, data owners, and management to identify and document operations that are affected by the loss or leak. Any products or services affected should be explicitly called out and documented.

The Crisis Team will work with system owners and data owners to Identify disaster recovery plans, work-arounds, or alternate courses of action, if these plans have not been pre-created as part of the larger Incident Response/Disaster Recovery plans. It is important to include plans to address worst-case interruptions or disruptions in case the incident is not quickly correctable.

These plans should not yet be activated at this step since containment has not yet been achieved. However, the business, Crisis Team, and Incident Responders may choose to activate them now for critical business functions and implement additional technical and procedural controls to prevent reoccurrence until the incident is resolved, or at least contained. If these plans are needed, they will be implemented in E11.

Document communications between the Crisis Team and various groups of stakeholders and add them as incident artifacts per your Incident Response Program requirements.

Document affected business operations, products, and services as incident artifacts per your Incident Response Program requirements.

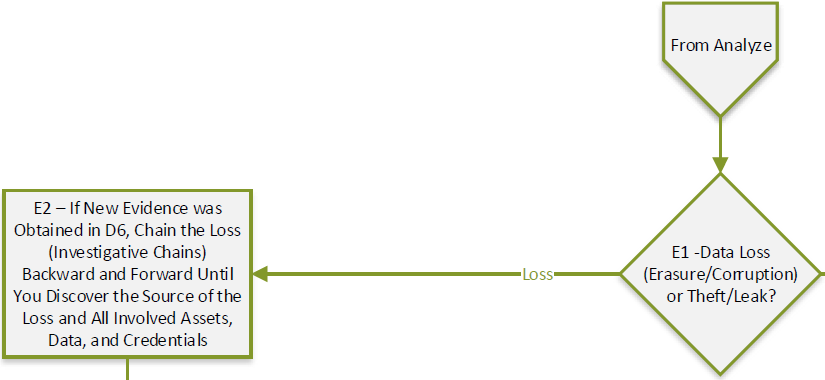
Document related disaster recovery plans, work-arounds, and alternate course of action plans as incident artifacts per your Incident Response Program requirements.

Resource:

<https://medium.com/@sroberts/crisis-communication-for-incident-response-4f3712485f15>

# Contain/ Eradicate/ Recover

The Contain/Eradicate/Recover phase puts all the work and information from the previous phases into action. In this phase the responders will track the loss or leak back to its initial infection vector and forward through the entire incident chain until all affected systems, credentials, and data are identified and remediated.



E1 & E2 – By now the responders have enough information to determine whether this incident is a loss (data erasure or corruption) event or a theft/leak event. A theft/leak event will move to E16, documented below. A loss/corruption event will move to E2.

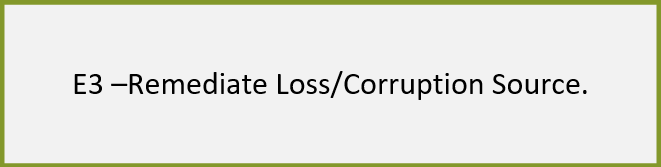
If any additional evidence was uncovered during or since D6, perform one final widening of the investigation. Chain it forward and backward to uncover the trail of loss/corruption of data.

Utilize artifacts related to the Operating System/Software Environment (browser history, persistence mechanisms, etc.), Network (packet captures, security tool alerts/logs, involved credentials, etc.), file system (hashes of suspect executables, leaked/stolen files, etc.), and security tool alerts or queries. Additionally, utilize information collected from user/system administrator interviews (from D4) to track the loss or corruption back to its source.

Continue until you discover the root cause of the data erasure or corruption and identify all affected assets, data, and credentials.

Document your organization’s tools and TTPs related to gathering and analyzing forensic data here. Include supporting tools and TTPs that help you follow an attacker or malicious code as it pivots throughout your environment.

Document the findings as part of your incident artifacts per your Incident Response Program requirements.



E3 – The goal of this step is to remediate the source of the loss or corruption identified in E2 to prevent more/new damage. The implementation of this step will be variable based on the nature of the source of the loss or corruption.

By this point in the process several potential sources of loss or corruption have been weeded out. The remaining eventualities will generally fall into four major categories:

**Hostile** (Irrational, Thief, Disgruntled, Activist, Terrorist, Organized Crime, Competitor Spy, Nation State)

**Non-hostile** (Reckless, Untrained/Distracted, Sympathizer)

**Unknown** (Supplier, Partner)

(Source: Intel Insider Threat Field Guide, link below)

**Software/Hardware** (Bug/Vulnerability, Defect, Failure)

Specific remedies for the various sources differ and will depend upon your tools available, but may include (among others):

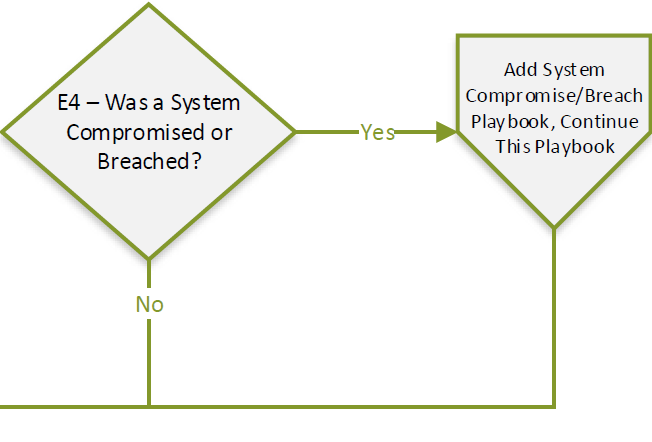
* Data Loss Prevention (DLP) rules/policies
* Patching and/or firmware updates
* Hardware replacements
* Additional filesystem access controls
* Suspend credentials
* Access Control lists on network firewalls or other network infrastructure
* Network Access Control (NAC) technologies
* Host-based firewalls
* Intrusion Prevention Systems (Network and host based)
* Network black-hole routes
* Proxy (Internal and remote)
* Email filtering
* Endpoint security suite
* Blocks at network infrastructure via port-level (bring the interface down) or MAC address blocks.

Document your remediation tools and TTPs here.

Record remediation activities and add them to your findings as part of your incident artifacts per your Incident Response Program requirements.

Resources:

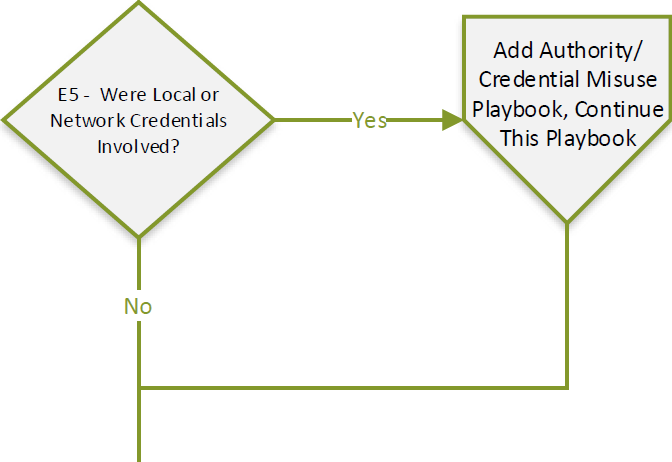
<https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf>



E4 – If the investigation and subsequent source remediation/containment point to system(s) being compromised or breached, add a System Compromise/Breach playbook and continue working this playbook in parallel.

If not, continue to E5.

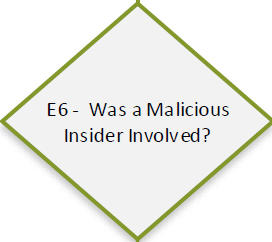
Any findings from system(s) that were compromised or breached should be formatted as a write-up and documented as part of your incident artifacts.



E5 – If the investigation and subsequent source remediation/containment point to credentials being misused or breached, add an Authority/Credential Misuse playbook and continue working this playbook in parallel.

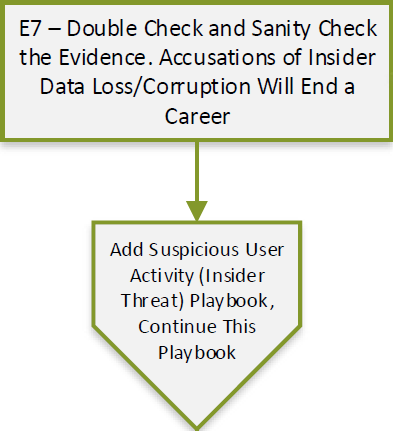
If not, continue to E6.

Any findings from credentials that were misused or breached should be formatted as a write-up and documented as part of your incident artifacts.



E6 – If the investigation and subsequent source remediation/containment point to a malicious insider being involved, move to E7.

If not, continue to E9.



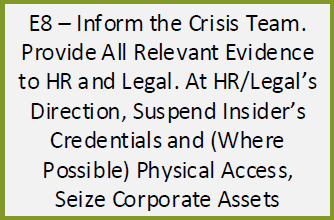
E7 – Before initiating an insider threat playbook, pause a moment and double-check your work. Sanity check the data. Make sure there is no other explanation other than malicious insider. Accusing someone of being a malicious insider can affect their career.

Make efforts to make sure you are not getting a false positive from an external entity. Logs should line up with the suspected insider’s physical presence. If not, dig deeper.

After all other avenues for investigation are exhausted, if the incident still points to a malicious insider being the source of the data loss or corruption, add a Suspicious User Activity (Insider Threat) playbook and continue this playbook in parallel.

Document the evidence and activities of your double-check as part of your incident artifacts.

Additionally, any findings from your Suspicious User Activity investigation should be formatted as a write-up and documented as part of your incident artifacts.



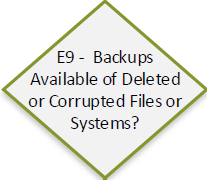
E8 – Present the insider threat information collected in prior steps to the Crisis Team. If your Crisis Team does not have HR and/or Legal representatives, work with the Crisis Team to get it to the appropriate decision makers and policy enforcers.

Given the severity of the accusations, provide as much supporting documentation as possible and expect questions.

At the direction of HR and/or Legal, suspend the insider’s credentials, cut off their physical access to company locations and assets, and seize any company assets in their possession.

Document tools and procedures used to automatically or manually suspend credentials, cut-off physical access, and seize corporate assets here.

Document your communication to the various stakeholder groups and any actions taken at their direction to suspend credentials, cut-off physical access, and seize corporate assets as part of your incident artifacts per your Incident Response Program requirements.

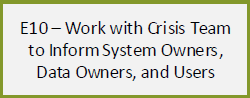


E9 – Containment and Eradication should have been achieved by step, either through actions taken as part of this playbook or one of the other playbooks called out. It is also possible, depending upon which other playbook(s) have been initiated, that recovery is under way or complete. If this is the case, skip appropriate steps below.

If there are backups available to recover from data loss or corruption, move to E12. If there are no backups available to address data loss or corruption, continue to E10.

Depending upon the scope of the incident, your organization may have backups for some data and not others. Follow the appropriate path for each data set or system if this is the case.

Document the availability (or unavailability) of backups as part of your incident artifacts per your Incident Response Program requirements.



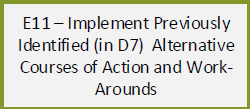
E10 – If the incident response lands here, the news isn’t good for users and customers.

Backups could be unavailable for a variety of reasons:

* Affected systems may not have been deemed important enough to be backed up
* Systems may have been mirrored or a snapshot may have been taken, but the mirrored/snapshot systems may be affected as well
* Backups may have been taken, but are not restorable due to hardware failures

Whatever the reason, the bad news has to be communicated properly. Work with the Crisis Team to inform stakeholders who do not know the system cannot be restored. Include System owners/administrators (these groups usually know already, but its best to be inclusive in case there are questions), data owners, users, and management chains above each of the mentioned groups.

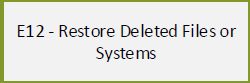
Document your communication activities as part of your incident artifacts per your Incident Response Program requirements.



E11 – Work with the Crisis Team and appropriate system owners, administrators, data owners, and users to implement any alternative courses of action and work-arounds identified in D7. These are generally temporary measures, but users should be made ready to continue these activities for extended periods of time while system owners and administrators rebuild affected systems.

Perform system testing and user acceptance testing after the measures are implemented and make sure everyone who has been operationally affected by the data loss or corruption is trained on new procedures.

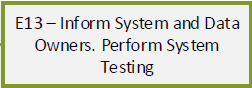
Document implemented work-arounds and alternate courses of action as part of your incident artifacts per your Incident Response Program requirements.



E12 – This step may have been completed while running one of the other playbooks. If not, now is the time to restore deleted or corrupted data, or entire systems.

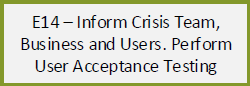
Where restoration activities are part of the incident responder’s responsibilities, document your tools and procedures here.

Document restoration activities as part of your incident artifacts per your Incident Response Program requirements.



E13 –Once restoration activities are complete, if restoration activities are part of the incident responder’s responsibilities, inform system and data owners. They should perform initial system checks at this time.

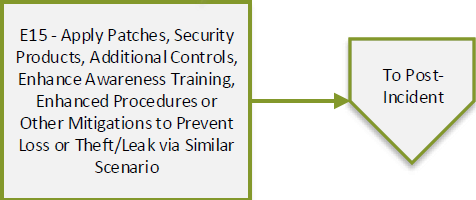
Document communications as part of your incident artifacts per your Incident Response Program requirements.



E14 – Work with the Crisis Team, system owners, and data owners to inform users of the restoration activities. Coordinate user acceptance testing with the various stakeholders to assure expected system functionality and data availability.

Work with appropriate support resources to correct problems until the system passes user testing.

Document communications, user acceptance testing activities and results as part of your incident artifacts per your Incident Response Program requirements.



E15 – The goal of this final step is to take any remaining actions required to prevent future data loss or leak scenarios. These actions will depend upon the root cause of the loss or leak and the tools you have available in your environment.

Some examples of actions the responders may need to initiate include (non-exhaustive):

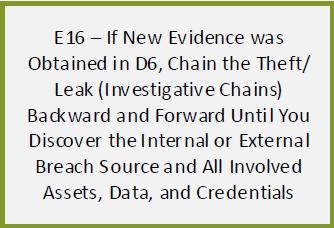
* Apply patches to software or firmware upgrades to hardware
* Implement additional technical or procedural security controls/mitigations
* Increase monitoring and/or auditing of security controls
* Enhance awareness training
* Enhance endpoint/server/cloud/service build procedures
* Implement new or custom rules in your security tools to detect or prevent the encountered threat in the future. What tools are modified will highly depend on your organization’s environment.

Return and/or reconnect any remaining remediated isolated endpoints to the production network.

Document any actions taken to prevent future similar loss/theft scenarios as part of your incident artifacts per your Incident Response Program requirements.

Document returned/reconnected endpoints as part of your incident artifacts per your Incident Response Program requirements.

Proceed to the Post-Incident Phase



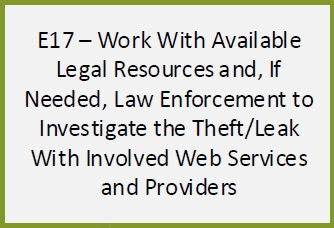
E16 - If any additional evidence was uncovered during or since D6, perform one final widening of the investigation. Chain it forward and backward to uncover the trail of the theft/leak of data.

Utilize artifacts related to the Operating System/Software Environment (browser history, persistence mechanisms, etc.), Network (packet captures, security tool alerts/logs, involved credentials, etc.), file system (hashes of suspect executables, leaked/stolen files, etc.), and security tool alerts or queries. Additionally, utilize information collected from user/system administrator interviews (from D4) to track the loss or corruption back to its source.

Continue until you discover the root cause of the data erasure or corruption and identify all affected assets, data, and credentials.

Document your organization’s tools and TTPs related to gathering and analyzing forensic data here. Include supporting tools and TTPs that help you follow an attacker or malicious code as it pivots throughout your environment.

Document the findings as part of your incident artifacts per your Incident Response Program requirements.



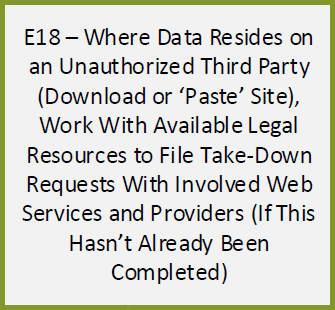
E17 – The goal of this step is to contain the data theft or leak as much as possible and engage additional resources to investigate the theft or leak.

Depending upon the nature and scope of the theft or leak, external legal and/or law enforcement may need to be involved to move the investigation forward. Doing so, however, will force the incident responders to relinquish control over certain aspects of the investigation, containment, and eradication. The incident responders and Crisis Team should carefully consider the pros and cons of involving 3rd parties.

Additionally, depending upon the nature of the theft or leak, you may need to investigate with 3rd parties (cloud storage, file transfer, cloud email, etc.) with which your business has no contract or contractual right to investigate. Prepare to be disappointed by the lack of cooperation.

If you do manage to get access to external data or systems, request the same investigative artifacts that you would for any internal system. (Artifacts related to the Operating System/Software environment, browser history, persistence mechanisms, packet captures, security tool alerts/logs, network device alerts/logs, involved credentials, file system hashes of suspect executables, leaked/stolen files, security tool queries for IoCs, user/system administrator interviews, etc.

Document any actions taken by responders or legal/law enforcement resources and their findings as part of your incident artifacts per your Incident Response Program requirements.

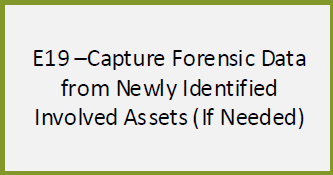


E18 – The goal of this step is to (as much as possible with a third party) further contain and eradicate the theft/leak. Some third parties have take-down request procedures that the incident responders can file, but most likely you are going to need legal resources and/or law enforcement involved.

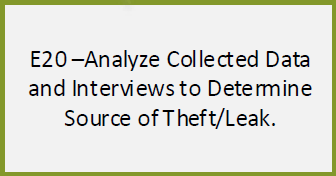
There will certainly be cases, especially when dealing with foreign service providers, where no legal avenues exist to remove your data. Again, do not expect cooperation.

If it’s not possible to remove the disclosed data, consider engaging a data monitoring/brand protection service. They can monitor for additional movement of the data and alert your PR and legal resources if the data spreads. Your legal team may be able to file take-down notices with newly involved services.

Document any actions taken by responders or legal/law enforcement resources and their findings as part of your incident artifacts per your Incident Response Program requirements.



E19 – In the unlikely event you have been granted access to investigate 3rd party assets identified in E16-E18, use the opportunity take a forensic image.



E20 – Collect all of the previous alerts, logs, interviews, and forensics to determine the source of the theft or leak. What needs to be determined will depend upon the nature and scope of the incident.

Points to determine include (non-comprehensive):

* What systems were involved
* What credentials were involved
* What 3rd party services or systems were involved
* Who was involved (people, as opposed to credentials)
* Method used to harvest and stage data
* Method used exfiltrate data
* Lateral movement methods
* Tools used

By this point in the process several potential sources of theft or leak have been weeded out. The remaining eventualities will generally fall into four major categories:

**Hostile** (Irrational, Thief, Disgruntled, Activist, Terrorist, Organized Crime, Competitor Spy, Nation State)

**Non-hostile** (Reckless, Untrained/Distracted, Sympathizer)

**Unknown** (Supplier, Partner)

(Source: Intel Insider Threat Field Guide, link below)

**Software/Hardware** (Bug/Vulnerability, Defect, Failure)

Add findings to the incident artifacts per your Incident Response Program requirements.

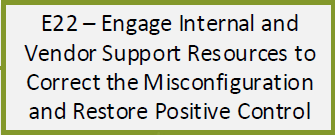
Resources:

<https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf>



E21– If the theft or leak can be attributed to non-malicious intentions, such as a storage bucket accidentally left at default permissions or an API key accidentally published to a public code version control site, continue to E22. Otherwise move to E25.

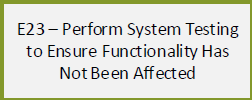
Depending upon the nature of the theft or leak, it may be necessary to follow both paths to get the misconfiguration resolved and contain/eradicate a system or credential compromise.



E22 – Work with the system owners/administrators to correct the misconfiguration(s). It is a good idea to have the system owners/administrators contact tech support to make sure the problem is fully corrected.

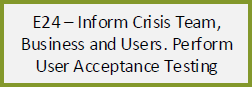
Depending upon the nature and scope of the incident, the system or service may need to be restored to a pre-breach state or imaged/rebuilt to fully restore positive control as it may not be possible to detect malicious actions in the environment while it was misconfigured.

Document actions taken to restore positive control as part of your incident artifacts per your Incident Response Program requirements.



E23 – Once configuration and restoration activities are complete, system and data owners should perform initial system checks at this time.

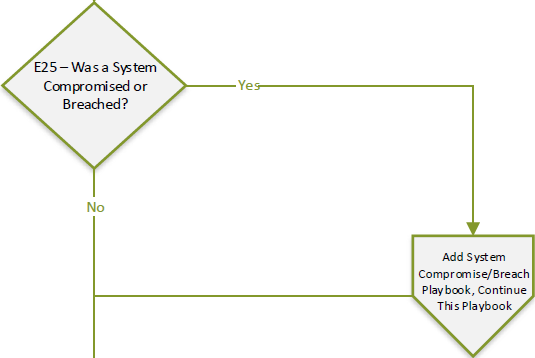
Document system checks performed as part of your incident artifacts per your Incident Response Program requirements.



E24 – Work with the Crisis Team, system owners, and data owners to inform users of the restoration activities. Coordinate user acceptance testing with the various stakeholders to assure expected system functionality and data availability.

Work with appropriate support resources to correct problems until the system passes user testing.

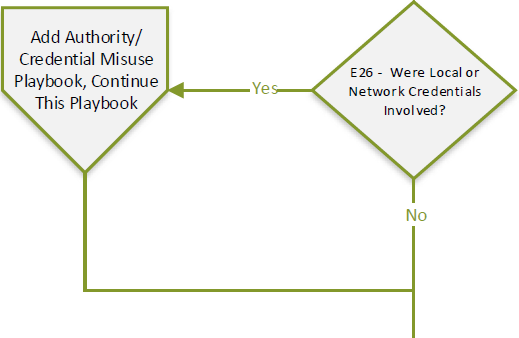
Document communications, user acceptance testing activities and results as part of your incident artifacts per your Incident Response Program requirements.



E25 – If the investigation and subsequent source remediation/containment point to system(s) being compromised or breached, add a System Compromise/Breach playbook and continue working this playbook in parallel.

If not, continue to E26.

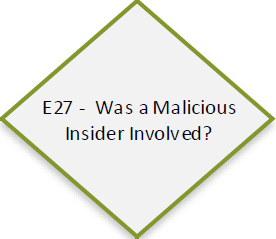
Any findings from system(s) that were compromised or breached should be formatted as a write-up and documented as part of your incident artifacts.



E26 – If the investigation and subsequent source remediation/containment point to credentials being misused or breached, add an Authority/Credential Misuse playbook and continue working this playbook in parallel.

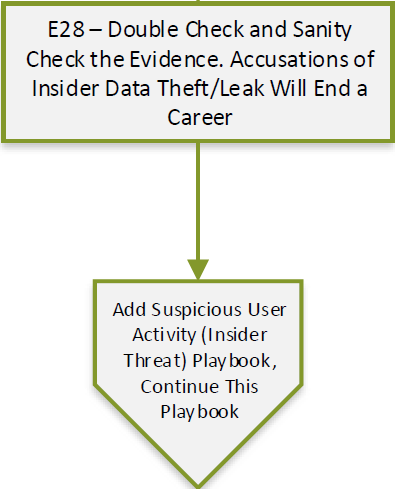
If not, continue to E27.

Any findings from credentials that were misused or breached should be formatted as a write-up and documented as part of your incident artifacts.



E27 – If the investigation and subsequent source remediation/containment point to a malicious insider being involved, move to E28.

If not, continue to E30.



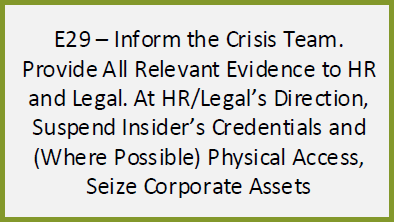
E28 – Before initiating an insider threat playbook, pause a moment and double-check your work. Sanity check the data. Make sure there is no other explanation other than malicious insider. Accusing someone of being a malicious insider can affect their career.

Make efforts to make sure you are not getting a false positive from an external entity. Logs should line up with the suspected insider’s physical presence. If not, dig deeper.

After all other avenues for investigation are exhausted, if the incident still points to a malicious insider being the source of the data loss or corruption, add a Suspicious User Activity (Insider Threat) playbook and continue this playbook in parallel.

Document the evidence and activities of your double-check as part of your incident artifacts.

Additionally, any findings from your Suspicious User Activity investigation should be formatted as a write-up and documented as part of your incident artifacts.



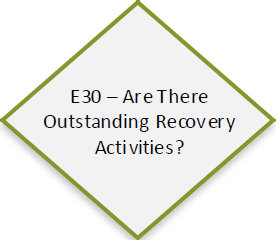
E29 – Present the insider threat information collected in prior steps to the Crisis Team. If your Crisis Team does not have HR and/or Legal representatives, work with the Crisis Team to get it to the appropriate decision makers and policy enforcers.

Given the severity of the accusations, provide as much supporting documentation as possible and expect questions.

At the direction of HR and/or Legal, suspend the insider’s credentials, cut off their physical access to company locations and assets, and seize any company assets in their possession.

Document tools and procedures used to automatically or manually suspend credentials, cut-off physical access, and seize corporate assets here.

Document your communication to the various stakeholder groups and any actions taken at their direction to suspend credentials, cut-off physical access, and seize corporate assets as part of your incident artifacts per your Incident Response Program requirements.

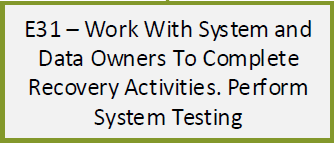


E30 – Most recovery activities will have been completed by this step, either as part of this playbook or one of the others that has been added. Take a moment to make sure everything has been covered. What needs to be checked will depend upon the nature of the incident and what actions have been taken.

Items to consider include (not comprehensive):

* Deferred actions from other playbooks called in previous steps
* Dismantle/delete data troves or exfiltration staging areas
* Review programs or scripts created/installed by insider
* Remove fraudulent operations or transactions made by malicious insider

If no additional recovery activities are identified or required, move to E15. Otherwise continue to E31.



E31 – Initiate outstanding recovery activities with appropriate internal teams, keeping the Crisis Team informed and involved. If the activities affect data or systems, system and data owners should perform system checks after completion.

Document recovery activities and system checks performed as part of your incident artifacts per your Incident Response Program requirements.

Continue to E14.

# Post-Incident

The Post-Incident phase covers the assessments and activities that occur after the loss/leak has been remediated. These include various reviews and reports that are sent to upper management and are stored; gap assessments, corrective actions, additions or modifications to playbooks, internal documentation, and TTPs.



F1 - Incident Review is an event and report for stakeholders and upper management to review and provide input about what happened, when it happened, how it happened, how it was investigated, and how it was remediated.

Summarize and cover everything documented throughout the various phases and steps. Identify improvement opportunities and roadblocks.

The ultimate goals are to communicate damages the business sustained, how they were dealt with, and what will be done different in the future to stop it from happening again. Additionally, cover any continuing actions (legal action, regulatory action, other playbooks triggered, technical or procedural improvements, etc.) and who is handling them.

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 44)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 21)



F2 – The Lessons Learned Review may be spliced into F1 for smaller incidents. Stakeholders and upper management is invited to review and provide input.

This event and report will cover the “what-if” scenarios.

* Could any unforeseen events during the incident have been detected earlier or prevented?
* What precursors did we miss?
* How can we handle this type of event better in the future?
* What would we do different next time?
* What was stopping us from making progress on the incident that we didn’t recognize at the time?

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 44)



F3 – The Lessons Applied Review may be spliced into F1 for smaller incidents. Again, stakeholders and upper management is invited to review and provide input.

This event and report will cover any corrective actions that have been taken, or will soon be taken, as a result of the incident. These may be policy or procedure changes, hardware/software/network changes, etc. At minimum this will include actions taken during E16. If additional/updated tools or TTPs will be deployed, they should be reported about here.



F4 – This step takes the information from F1 – F3 and puts it to use with appropriate analysts and engineers to find gaps in your organization’s security tools and TTPs. Executable corrective action plans with required budget are submitted to management.

If the incident was ruled a false-positive from Detect, this step is optional.



F5 – In this step the responders update documentation based on information discovered during the incident and the assessments/reviews above. Internal documentation, help desk documentation, internal procedures, playbooks, network diagrams, inventories, etc. are updated and fed back into the prepare phase to be applied to other phases in this playbook and other playbooks.

If the incident was ruled a false-positive from Detect, this step is optional.

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 45)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 22)



F6 – In this final step before the incident is completely finished, all final reports (from above) are sent to appropriate stakeholders and upper management. Wait until the end of the process to send them as responders may find additions or changes need to be made to the reports based on the updates in F5.

If the incident was ruled a false-positive from Detect, this step is optional.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 54)