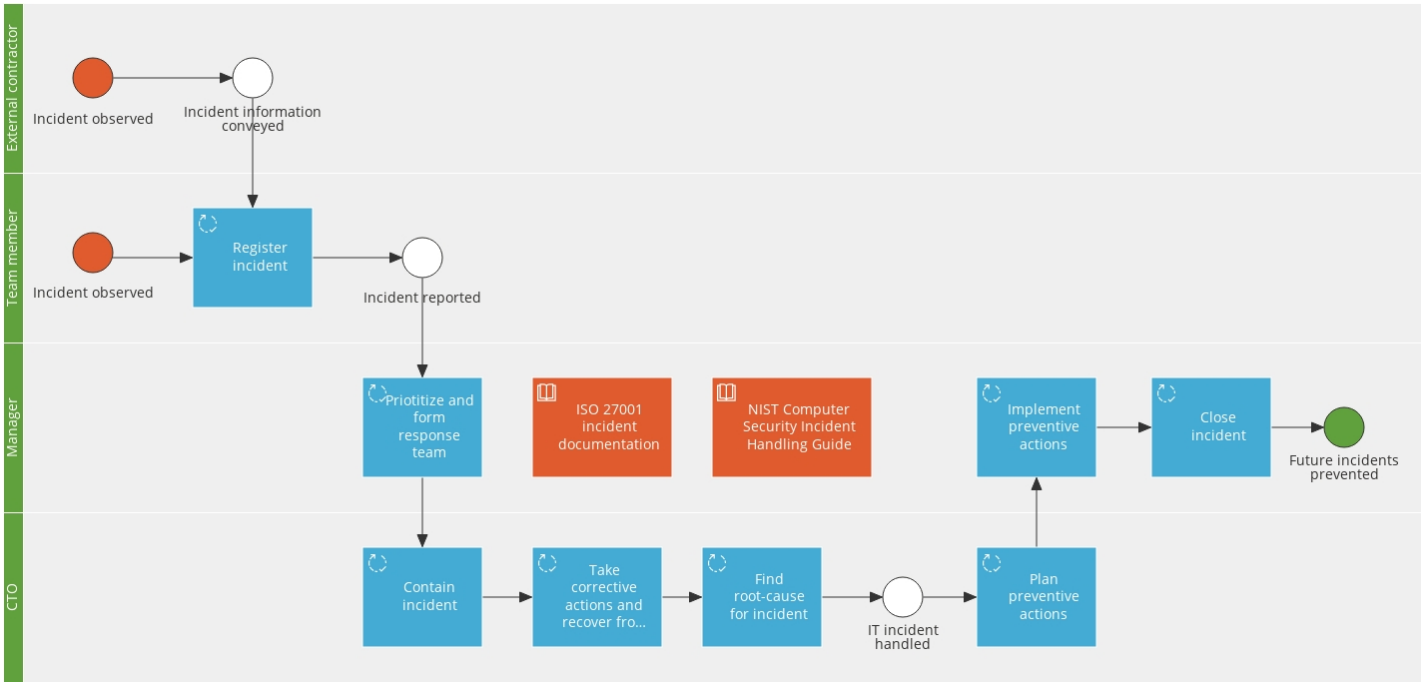
PROCESS

Manage IT security incident

Outcome: Incident has been logged, analysed and preventive measures has been taken

Make sure to get the latest version
Modified:
05 Oct 2023, 12:02
click to open in Gluu



Responsibilities

Owner
Søren Pommer

Editors
- no editors yet -

9 Role members	Role(s)
Ammar Kahrimanovic	Team member
Gabriela Delgado	Team member
Georgiy Zhuravlev	Team member
Hamza Mansouri	Team member
Jacob Carstensen	CTO, Manager, Team member
Juan Talamayan	Team member
Louie Allen Lacsamana	Team member
Louise Svenstrup	Manager, Team member
Søren Pommer	Manager, Team member

Register incident

Outcome: Incident has been registered

Responsible: Team member

Make sure to get the latest version
Modified:
05 Oct 2023, 12:31
click to open in Gluu

Why

Reporting it as soon as realised will greatly reduce the impact caused by the incident.

How

In simple terms

- If you think there is an incident it is better to report it than not.
- Gather what you can and pass it on to someone who can determine the severity.
- If you have received the information from an external please verify the claims.

Is this an incident?

An incident is defined as a threat to or a breach of information security, cyber security and/or privacy security.

If one or more of the 3 CIA criteria below do not hold true in a certain situation, this constitutes an incident.

- Confidentiality
- Integrity
- Availability

⚠ Unlike an actual data breach, a cyber security incident doesn't necessarily mean information is compromised; it only means that information is threatened. For example, an organisation that successfully repels a cyber attack has experienced an incident, but not a breach.

Tasks

- Collect as much information as you can regarding the incident
  - Log files
  - Screendumps
  - Emails
  - Photos
  - Meeting notes
  - etc.
- Fill in the **- missing data -** form and attach all information available.

Examples of cyber security incidents:

Phishing attack

Phishing scams are designed to trick people into handing over sensitive information or downloading malware.Crooks do this by sending a supposedly official correspondence that imitates a legitimate organisation. This is typically an email, but phishing can also take place on social media, text message or over the phone.

Brute-Force Attacks

In these attacks, hackers use software to repeatedly and systematically attempt password combinations until they find one that works. Given the sophistication of password cracking rigs, relying on a combination of letters, symbols, and numbers is no longer enough to provide strong protection. Limiting login attempts and enabling two-factor authentication are better preventative measures against brute-force attacks.

Ransomware

Ransomware is a type of malware that spreads through a computer or network, and is designed to encrypt files.The attackers then demand payment for a decryption key that will unlock the information. Ransom demands can vary greatly, depending on the size of the organisation – but experts urge organisations not to pay up however tempting it might seem.This is because the money helps to fuel the cyber crime industry and could make you a soft target for future attacks. Moreover, there is no guarantee that the criminals will keep to their word once they've received payment.

Malware

Malicious software, aka malware, infects devices without users knowing it's there. Examples include Trojan horses, spyware, ransomware, and viruses — and can have costly consequences. In 2021, Colonial Pipeline, the biggest oil supplier in the US, got caught up in a ransomware incident, lost days of business, and ultimately **paid off their attackers** approximately $5 million dollars in bitcoin. According to Bloomberg, the hackers got into the system via a **leaked password on an old account** that allowed employees to access company servers remotely through a VPN (virtual private network), and it did not require two-factor or multi-factor authentication. Once the hackers were in, they placed the malware, encrypted the company's data, and demanded a ransom.

DDoS (distributed denial of service attack)

DDoS attacks attempt to disrupt an organisation by flooding its network traffic with requests, which slows down its systems or causes them to crash.These attacks are conducted for a variety of reasons. They are often simply intended as a nuisance to annoy customers and give employees extra work. However, they can also be a distraction for more sophisticated attacks.

Drive-By Downloads

This is a way of distributing malware. Malicious code is added to a page's PHP or HTTP. When a user hits an infected site, the malware silently invades their device. These threats are hard to identify because websites can be compromised without knowing it, therefore users aren't alerted.

Man-in-the-Middle Attacks

Hackers position themselves as middlemen between users and eavesdrop, intercept, and/or manipulate communication between two parties. This often occurs on unsecured networks, like public WiFi.System misconfigurationUnlike the other examples, system misconfigurations don't involve criminal hacking.Rather, they occur when employees mishandle sensitive data and make it publicly accessible.This often happens when someone fails to password-protect a database that's stored in the Cloud.

SQL injection

Attackers can access an organisation's sensitive information when they target a server that uses SQL (Structured Query Language).They can do this by looking for security vulnerabilities in an application's software, which would enable them to insert malware and view or modify the organisation's data.

WORK INSTRUCTION back to process map

Priotitize and form response team

Outcome: The incident has been classified, an incident response team has been formed and stakeholders informed

Responsible: Manager

Make sure to get the latest version
Modified:
05 Oct 2023, 12:31
click to open in Gluu

Why

For an efficient response to the incident the severity and impact must be assessed in order to prioritise correctly.
A high priority incident requires an Incident response team to be formed.

How

In simpler terms

For an appropriate response to the incident you need to make a prioritisation of the incident. How bad is it?
Knowing what you deal with you must engage with relevant stakeholders and inform the management team (if very severe).
Forming an Incident response team is putting together the right people for the task.

Main tasks

1. Prioritise the incident according to the Severity/Impact-matrix
2. Form an Incident response team
3. Inform management (if High or Critical priority)
4. Inform/Engage with stakeholders

1. Prioritise the incident

Tasks

1. Prioritise the incident based on impact and severity.
2. Fill in the form with your assessment.
3. Decide on appropriate next step:
    a. If the priority is Insignificant, Low or Medium add the incident to the backlog of normal tasks and inform stakeholders and close the case
    b. If the priority is High or Critical form an Incident response team and inform management

Further reading

📖 NIST Computer Security Incident Handling Guide section 3.2.6 "Incident Prioritization".

1. Likelihood

An assessment of how likely you think the threat is?

Probability	Explanation
Rare	The event is the least probable to occur. Occurrence is unprecidented.
Improbable	Possible, but very unlikely. May occur very seldom.
Possible	As likely to occur as not. Occurrence is occasional.
Probable	More likely to happen than not. Occurs is probable.
Almost Certain	Surprising if the event not happens. Occurrence is expected.

2. Consequence

An assessment of how bad it is, should the threat materialise.

The columns are considerations from different parts of the business. Use them as guidelines for your assessment.

	Occurence pattern	**Performance impact**	**Data Breach**	**Reputation impact**	**Timeframe & resource**	**Financial costs**
Insignificant	Historical, Not spreading	None	None	Negligible	Regular	Negligible
Minor	Current, Not spreading	Reduced, Non critical functions	None	Minimal	Regular	Minimal
Moderate	Current, Slow spread	Stopped, Non critical functions	Unclassified data	Moderate	Supplemented	Moderate
Major	Current, Moderate spread	Reduced, Critical functions	Proprietary data	Significant	Extended	Significant
Catastrophic	Current, Fast spread	Stopped, Critical functions	Proprietary data	Severe	Irreversible effects	Severe

2. Form an Incident response team

Build a team of people to handle the incident.

A successful team will include **technical personnel, management personnel, and legal and communication experts**.

The team will have various ownership roles within the confines of the incident response system.

> ⚠ Find the right fit for the response team.
> Depending on the **priority of the incident** and **company size** the team members can overlap roles.
> There is no need to overcomplicate or overdo the

When you compile your team, you will need to consider the following roles and assign people to fill them:

Role	**Responsibility**
Incident response manager (mandatory)	Drives and coordinates all incident response team activity, and keeps the team focused on minimising damage, and recovering quickly.
Lead Investigator (mandatory)	Collects and analyses all evidence, determines root cause, directs the other security analysts, and implements rapid system and service recovery.

Role	Responsibility
Security analyst (optional)	Review alerts, identify possible incidents and perform an initial investigation to understand the scope of an attack.
Threat researcher (optional)	Responsible for providing contextual information around a threat, using information from the web, threat intelligence feeds, data from security tools, etc.
Communications Lead (optional)	Leads the effort on messaging and communications for all audiences, inside and outside of the company.
Documentation & Timeline Lead (optional)	Documents all team activities, especially investigation, discovery and recovery tasks, and develops reliable timeline for each stage of the incident.
HR/Legal Representation (optional)	Since an incident may or may not develop into criminal charges, it's essential to have legal and HR guidance and participation.

Consider team engagement

- Does incident response need to be available 24/7?
  - Do incident responders need to be on-site or is phone contact sufficient? Real-time availability and on-site presence is best because it allows immediate response to an incident, which can prevent damage.
- Should staff be part-time or full-time?
  - Part-time employees can be used to make up a virtual incident response team, like a volunteer emergency response unit. When an incident occurs, the IT help desk can be the first point of contact. They can perform an initial investigation, rapidly call on incident response team members, and whomever is available can respond to the incident.
- Should staff be security experts?
  - What level of expertise is needed? Incident response requires broad knowledge of IT systems, communication protocols, attack techniques, and also the organisation's environment, systems and procedures. Outsourced teams typically have stronger security expertise, but employees have a better understanding of the IT environment, normal vs. malicious behavior, and of which systems are critical, etc.
- How much will the incident response team cost?
  - Because incident responders need special expertise, and are often required to be on-site 24/7, they can represent a major investment. Managed Security Service Providers (MSSP) can also be costly, and there is an additional cost of security tooling, physical facilities and secure communication methods.

3. Inform management

If the priority is deemed "High" or "Critical" inform your management group.

Example email

Subject:

"Information regarding security incident"

Body:

"Hi,

For your information, we have encountered a IT security incident on [insert IT system].

The incident priority is [High/Critical] as the severity is [High, Extreme] and it impacts [One or few users,A small contained group of users,Department or branch, the operation, our entire business].

To contain and analyse the incident I've put together an incident response team consisting of:

- [Name 1] from [department]
- [Name 2] from [department]

[Name] is team leader and will keep you posted as we learn more.

All the best,"

4. Inform / Engage with stakeholders

Inform and engage with the stakeholders affected by the incident.

Example email

Subject:

"Information regarding security incident"

Body:

"Hi,

For your information, we have encountered a IT security incident on [insert IT system].

The incident priority is [High/Critical] as the severity is [High, Extreme] and it impacts [One or few users,A small contained group of users,Department or branch, the operation, our entire business].

I hope to get your help, as needed to sort out the situation at hand.

To contain and analyse the incident I've put together an incident response team consisting of:

- [Name 1] from [department]
- [Name 2] from [department]

I will keep you posted as we learn more.

All the best,"

⚠ Make sure to consider whether the incident has ramifications under EU GDPR regulations: Manage GDPR incident

Why

Containing the incident limits the impact by:

1. preventing further loss
2. preventing escalation

3. preserving the system for forensic analysis

How

Your containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration of the solution—a temporary solution for a few hours, days or weeks, or a permanent solution.

Containment is often accomplished in sub-phases:

- **Short term containment**—immediate threats are isolated in place. For example, the area of your network that an attacker is currently in may be segmented off. Or, a server that is infected may be taken offline and traffic redirected to a failover.
- **Long term containment**—additional access controls are applied to unaffected systems. Meanwhile, clean, patched versions of systems and resources are created and prepared for the recovery phase.

This activity is the short term containment, as the long term requires further analysis to complete and will be handled later in the process.

In simpler terms

There is no "one size fits all" for containment of an incident.

Containment strategies vary based on the type of incident.

For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack.

Tasks

1. Identify and block attacker
2. Reduce impact

Further reading

- missing data - section 3.3.1 "Choosing a Containment Strategy".

1. Identify and block

Identify the attacking host and validate its IP address. This allows you to block communication from the attacker.

Consider alternative communication channels they may be using.

Attack vectors (from NIST section 3.2.1)

- External/Removable Media
  - An attack executed from removable media or a peripheral device - for example, malicious code spreading onto a system from an infected USB flash drive.
- Attrition
  - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- Web
  - An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- Email
  - An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

- Impersonation
  - An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- Improper Usage
  - Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- Loss or Theft of Equipment
  - The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
- Other
  - An attack that does not fit into any of the other categories.

2. Reduce incident impact

Various measures that can be used to contain security incidents and eradicate the intruder include:

- Blocking all incoming network traffic on border routers
- Blocking networks and incoming traffic on firewalls
- Blocking particular services (e.g., ftp, telnet) and ports on firewalls
- Disconnecting infected systems from the network
- Shutting down the infected system
- Locking compromised accounts
- Changing passwords on compromised systems
- Refrain from accessing compromised systems.
- Isolate compromised systems from the network.
- Store system logs for in scope systems as digital forensic evidence after a security incident has been detected.
- Change authenticators after a security incident has been detected.
- Refrain from turning on any in scope devices that are turned off when a security incident is detected.
- Record actions taken by investigators during a forensic investigation in the forensic investigation report.

WORK INSTRUCTION back to process map

Find root-cause for incident

Outcome: The cause for the incident has been found.

Responsible: CTO

Why

To find the root cause for the incident to prevent similar future incidents

How

In simpler terms

To fully resolve an incident you need to know what caused it, so it can be eradicated and prevented.

There are several methods to conduct a root cause analysis. The choice of which to use largely depends on preference.

The high level questions regarding root cause finding is to answer:

- What happened?
- Why it happened?

- What to do to reduce the likelihood of it happening again?

> ⚠ Remember that the most common cause for incidents are human error

Once you know what and why it happened you can prevent it from happening again.

Tasks

1. Conduct a root cause finding analysis
2. Inform stakeholders and management

Further reading

- missing data - section 3.2.4 "Incident analysis".

1. Root cause finding

ISO 45001 has a great description of root cause analysis:

"Root cause analysis refers to the practice of exploring all the possible factors associated with an incident or nonconformity by asking what happened, how it happened and why it happened, to provide the input for what can be done to prevent it from happening again."

And: *"This analysis can identify multiple contributory failures, including factors related to communication, competence, fatigue, equipment or procedures."*

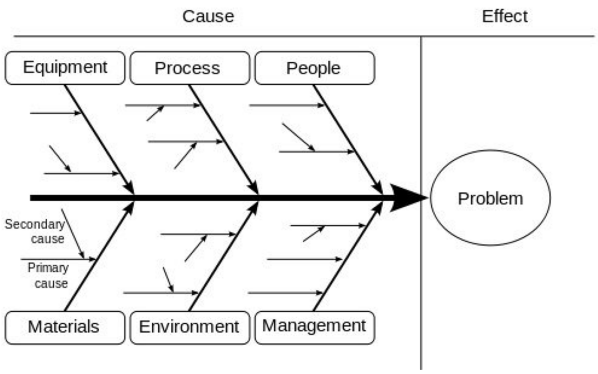
Use the following 4 steps and their sub-steps:

1.1. Define event

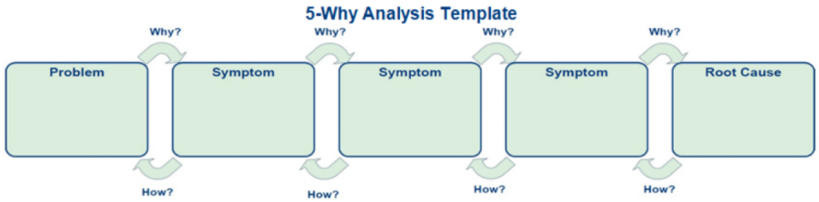
- What happened?
- Where did it happen?
- When did it happen?
- What systems were involved?

1.2. Find causes

Option 1: Fill out a Fishbone diagram



Option 2: The 5 whys



The Five Whys Procedure

1. Assemble the Incident response team and any relevant stakeholders or SMEs
2. Write out a description of what is known about the problem. Document the Problem/Incident and describe it as completely as possible.
3. Refine the definition with the team. Come to an agreement on the definition of the Problem/ incident at hand.
4. Have the team members ask "Why" the Problem/Incident as described could occur, and write the answer down underneath the description. Use the validation step (below) to ensure the answer provided is valid.
5. If the answer provided from 3 (above) does not solve the Problem, repeat steps 3 and 4 until solved.
6. If the answer from step 3 (above) seems likely to solve the Problem, make sure the team agrees and attempt a resolution using the answer.

1.3. Finding the root cause

Given the past two steps, the team should have gathered enough information to assess the situation and come up with some potential reasons for the root of the problem.

This step should focus on discovering and uncovering. The team or organisation can leverage the security systems that come with cybersecurity architecture.

Security Information and Event Management (SIEM) or logs can be audit as part of this step, making finding the root cause easier.

1.4. Find solutions

Knowing the root cause(s) should give a direction on how to find solution or at least where to look for solution.

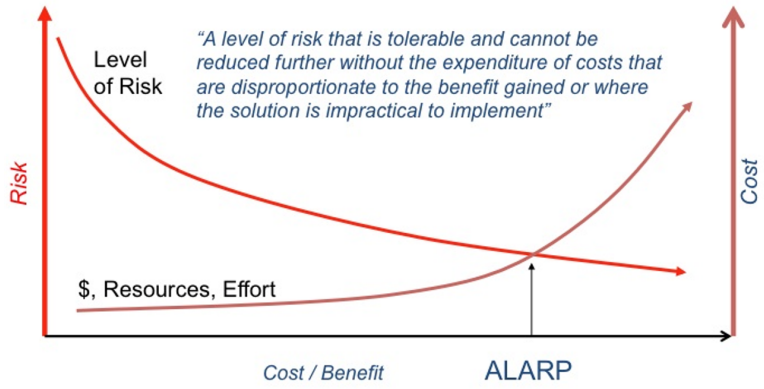
But if you have no idea where to start, try using some of the common tools listed below:

- Interviewing – subject matter experts or industry experts
- Running diagnostic tools when the root cause is found
- Checking forums and messaging boards for common solutions to known problems

These techniques should be enough to get you started on the right track. Keeping in mind that no one will know your business as your staff does, be sure to leverage their business operations and systems knowledge.

⚠ Please chose a balanced approach and keep in mind that the solution should not be worse than the problem.
Example: You could stop all access to emails in order to prevent phishing email issues. This might be very effective, but would make it hard for co-workers to get work done. In reality you may install software to scan all incoming emails and stops as many malicious emails as possible.

Apply the ALARP ("As Low As Reasonably Practicable") -principle to the situation:



Plan preventive actions

Outcome: A Preventive action plan has been created

Responsible: CTO

Why

To learn from the incident and ensure that measures are implemented in the organisation to reduce the likelihood of incidents.

How

In simple terms

This step is the reaction to the knowledge gained from the root cause finding.

There is no "one size fits all", but nonetheless preventive actions should be considered.

The goal is to find organisational measures that can help prevent security incidents from happening again. Often incidents spawn from people unintentionally misusing privileges or systems, so targeting KPIs, training and education, response and policies can be very effective.

Tasks

1. Consider best fit for organisation
2. Create a preventive action plan
3. Re-evaluate response plan and collect lessons learned
4. Create a follow-up report

Further reading

- missing data - section 3.4.1 "Lessons learned" and 3.4.2 "Using collected incident data".
- missing data - 8.3 "Preventive actions" of the ISO27001-2005 documentation.

1. Consider best fit for organisation

The following considerations are probably not all necessary, but provides a list of areas to improve in order to prevent similar incidents from emerging:

- **Training and education**
  - Should this incident be used as an example in future training material in the IT areas?
  - Is there a need to improve onboarding training for new employees?
- **Policies**
  - Review current policies - can anything existing be improved?
  - Would additional policy could have prevented the intrusion?
- **KPIs**
  - Do we need to improve existing KPIs?
  - Are there any KPIs the needs to be added?
- **Sourcing future IT systems**
  - Can the knowledge from this incident improve the selection criteria for future systems?

2. Create a preventive action plan

Based on the consideration regarding best fit a preventive action plan must be created. Please fill in the Gluu form to ensure that documentation are kept for future use. Upload any documentation relevant for future use.

3. Re-evaluate response plan and collect lessons learned

Please consider the following (non-exhaustive) list:

- What indicators worked and what didn't work when the incident was discovered?
- Did the chain of command work during incident handling?
- Did the team have sufficient tools at hand to swiftly contain, eradicate and analyse the incident?
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- What feedback did the Incident response team receive during the phases?
- Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
- Was there any relevant documentation lost during any of the phases?
- What lessons have been learned from this experience?

4. Create follow-up report

The follow-up report must be a brief document outlining the incident, the response (containment and eradication), Incident response team, timelines and solution.

WORK INSTRUCTION back to process map

Take corrective actions and recover from incident

Outcome: The IT system is back on operation

Responsible: CTO

Make sure to get the latest version
Modified: 05 Oct 2023, 12:31
click to open in Gluu

Why

To get the system safely back into operation.

How

In simpler terms

All know (and reasonable) causes from the root-cause finding must to taken into account when reestablishing the system.

The overall goal is to prevent:

1. Similar incidents from happening,
2. Related or incidents in close proximity from happening

Get the affected systems into normal operation in a better state than prior to the incident (as the cause for the incident has been been fixed)

Ideally, systems can be restored without loss of data but this isn't always possible.

Tasks

1. Take corrective actions
2. Re-establish system and data
3. Inform end-users
4. Inform stakeholders and management

Further reading

- missing data - section 3.3.4 "Eradication and recovery".

1. Take corrective actions

1.1. Take action

Knowing a possible solution the team must take action and implement the corrective solutions proposed by roo-cause finding.

- Rebooting parts of the affected systems
- Updating software
- Patching vulnerabilities

1.2. Verify solution effectiveness

The final step is to see if the solution(s) works.

Continuing to use the example from previous sections, let's see if our solutions worked out.

If you used the five why's as a detection tool in step three, then checking for solution effectiveness should be based on those why's.

See if the solutions have solved the why's from the root-cause finding activities.

2. Re-establish system and data

Restore the affected system(s) to the uninfected state.
Consider any or more of the following:

- Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct events and to the proper level.

3. Inform end-users

Inform the end-users that the system will be back in operation.

Example email

Subject

"[System] back online"

Body

"Hi,

I'm very happy to inform that [system] is getting back in operation after the incident.

We expect that [system] will be available again from [date].

With regards to any user generated data, we will establish the latest backup from [date].

I'm sorry to inform you that all data between that date and the availability date will be lost.

We're logging the system to ensure that everything runs as planned, so please have patience for now.

If you notice anything suspicious when returning to the system do not hesitate to let us know.

All the best,"

4. Inform stakeholders and management

Inform the management and key stakeholders that the system will be back in operation.

Example email

Subject

"[System] back online"

Body

"Hi,

I'm very happy to inform that [system] is getting back in operation after the incident.

We expect that [system] will be available again from [date].

All the best,"

WORK INSTRUCTION back to process map

Implement preventive actions

Outcome: The Preventive actions plan has been implemented.

Responsible: Manager

Make sure to get the latest version
Modified:
05 Oct 2023, 12:31
click to open in Gluu

Why

The preventive actions must be implemented to gain any value to the organisation

---

How

In simple terms

All the newfound knowledge must be implemented to prevent similar incidents from re-emerging.

Use the Preventive action plan and put it into action.

Tasks

1. Review and revise Preventive action plan
2. Implement Preventive action plan

1. Review and revise Preventive action plan

Carefully consider how the proposed steps in the Preventive action plan can be implemented in the organisation.

If needed do several feedback sessions with the Incident respsonse team to ensure that every aspect is understood for its intended purpose.

2. Implement Preventive action plan

Ensure that all parts of the (revised) Preventive action plan are implemented.

Close incident

Outcome: All have been informed and incident has formally been closed

Responsible: Manager

Why

Closure and an organisation update is needed to return to normal operation.

How

In simpler terms

An organisation can quickly become reluctant to use an IT system if there is uncertainty regarding an IT system (eg. will my work be saved/stolen etc.)

A formal closure of an incident leaves no misunderstandings.

Once the organisation has been informed decide on a record retention period (usually 1-5 years).

Tasks

1. Inform end-users and key stakeholders
2. Inform management
3. Decide on records retention period

Further reading

- missing data - section 3.4.3 "Evidence retention".

1. Inform end-users and key stakeholders

An email is usually enough. For major incidents consider meeting participation or town-hall meetings.

Email

Subject

"[System] back online"

Body

"Hi all

I'm very happy to announce that [System] is back online and fully operational.

All the best,"

2. Inform management

Email

Subject

"[System] back online"

Body

"Hi all

I'm very happy to announce that [System] is back online and fully operational.

All the best,"

3. Decide records retention period

There can be internal policies determining how long records are kept depending on the severeness and impact of an incident.

Ranging between month to years is it a good measure to decide how long data from this incident should be kept.
