Cassandra Lalli

Incident Response Management

Table of Contents

Identify and Document an Incident.....3-4

Informminternal and External Individuals Affected.....4-5

Investigate the Breach.....5-7

Enforcement.....7-11

Cost 11-12

Response and Update Policies.....12-15

Identify and Document Incident

When responding to an incident it is important to refer to the list of commands and keep information on a need-to-know basis concerning the incident. An insider threat might be the cause of the incident violating laws or policies put in place by the company. Allowing them to know they are being watched or investigated allows them to destroy valuable evidence. An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response phases are

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Preparation

- Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of a data breach
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

2. Identification

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

3. Containment

- What's been done to contain the breach short term?
- What's been done to contain the breach long-term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all-access credentials been reviewed for legitimacy, hardened, and changed?

- Have you applied all recent security patches and updates?

4. Eradication

- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Recovery

- When can systems be returned to production?
- Have systems been patched, hardened, and tested?
- Can the system be restored from a trusted backup?
- How long will the affected systems be monitored and what will you look for when monitoring?
- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

6. Lessons Learned

- What changes need to be made to the security?
- How should employees be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?

Informminternal and External Individuals Affected

1.1 Incident command system for Few Yorks Finest

New yorks finest implements a well-known fire service to handle and respond to various incidents. We have classified cyber incidents as fires when dealing with them within computer systems and networks. This system is designed to allow inter-agency operation for incidents small to large and complex. The ICS is based on the following 14 management characteristics that provide strength and efficiency to the total system

• Common Terminology – Assures that all participants are using the proper terminology for incident response and required resources.
• Modular Organization – This allows for a compartmentalized approach that allows resources or functions to be brought in based on the complexity and severity of the incident.
• Management by Objectives – Establishes all-encompassing objectives and goals • Incident Action Planning – Provides a centralized approach to the planning of the response to the incident as well as setting priorities.
• Manageable Span of Control - Span of control defines how many people (or things) each individual can manage. The typical range is 3 to 7 with 5 being optimal.

• Incident Facilities and Locations – Numerous and varied facilities may be needed for the incident, these include command posts, staging areas, rest areas, etc.
• Comprehensive Resource Management – This means maintaining a comprehensive view of resource utilization. Resources, in this case, include equipment and personnel.
• Integrated Communications – Establishes a common communication system to address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.
• Establishment and Transfer of Command – At the beginning of any incident command (who is n charge?) must be established. As the incident grows it may be necessary to transfer the command, this requires a briefing that includes the current status, the plan, and other important information
• Chain of Command and Unity of Command – The chain of command assures that subordinates report to supervisors. The concept comes from the military where it is not desirable to have privates reporting to generals.
• Unified Command – This is a concept that allows various agencies and entities with different functional, geographical, and legal authorities to work together.
• Accountability – This is the management of personnel and resources involved in the incident.
• Dispatch/Deployment – Personnel and resources only respond when requested.
• Information and Intelligence Management – This is the process of gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

The incident command sections are defined as follows 15]:
• Command – Incident Commander (IC), Public Information Officer, Liaison Officer
• Operations – Manages the tactical operations
• Planning – Resources, Situation, Documentation (Understanding the situation, establish Priorities, and Strategy)
• Logistics – Communication, Food, Supply, Facilities
• Finance/Administration – Procurement, Compensations, Claims, Cost
• Intelligence/Investigations – Post-incident investigation or intelligence gathering.

Not all components of the ICS are invoked in every emergency incident. Each component is invoked as needed. The incident commander may also be the operations chief, planning chief, logistics chief, and finance chief.

investigate the breach

2.1 Identification

The goal here is to examine the events, analyze them, and determine if there is an incident. As mentioned previously, not all events are incidents. Examples of this are phishing emails that are

not opened, a user on a Linux system surfing a website with known windows exploits, and a large increase in FTP traffic that is authorized.

2.2 Containment

New yorks finest classified containment into two categories, Long term, and short-term goals. With the short-term goal of confinement, it is our cyber and IT team's job to

1. Stop communication with hackers from systems
2. Isolate all systems
3. Identify malware or malicious programs
4. unplug the network cable, disable the switch port, put in ACLs on routers or firewalls, and as a last resort unplug the power.
5. keep a low profile, do not let the attacker know that you have discovered their activity.
6. Make a system image to include the file system and memory.
7. Take pictures of the area and the current state of the screen\

All of these steps are important in knowing how the virus is working as well as proving that We at New Yorks Fines are not at fault, it is also instrumental that we report these findings to all agencies that are concerned within the first 72 hours of the initial breach.

Long-term goals are also important when it comes to these types of breaches below is an outline of long-term goals once a breach has happened:

1. applying patches to the affected system and other similar systems.
2. changing passwords
3. adding firewall rules
4. Remove any accounts that were used by the attacker
5. shutdown hacker processes

The hacker's malware must be removed fully and eradicated from the system so they were not able to achieve their goals, this is our priority.

2.3 Eradication

The eradication is one of the most important steps of this process, for this, the system will be cleaned and attacker artifacts are removed. From this point on we will be looking at the forensic analysis. When the malware is identified an internet or internal search will be run revealing the characteristics of the malware. If it can not be identified the malware will be exported to a VM and monitored closely until the team has a better understanding. Before executing the backup files they must be checked for malware and attacker signatures. If a rootkit was installed this will modify the operating system itself, in this case, reformating the hard drive and reinstalling the

operating systems will occur. Once the system is restored perform a vulnerability scan using Nessus and patch all vulnerabilities.

4.5 Recovery

Before putting the system back into production check the operation of the system against the test plan and baseline documentation. This should be done by the system administrator and the owner of the system. The owner of the system makes the final decision on putting the system back into production. Once in production monitor the system closely and check carefully for signs of compromise.

4.6 Follow-Up

In the follow-up phase, all weak links and lessons learned from the attack are documented. A report is generated by the cyber team this report should contain:

- how the attacker got in
- what was done
- how the issue was found
- what was done to fix it
- recommendations to prevent future attacks by the same method

4. 7 Seven Deadly Sins

1. Failure to report or ask for help
2. Incomplete or nonexistent notes
3. Mishandling or destroying Evidence
4. Failure to create working images
5. Failure to contain or eradicate
6. Failure to prevent re-infection
7. Failure to apply lessons learned

Enforcement

GDPR requirements

Security and breach reporting requirements are covered in Articles 32-34 of the GDPR. Controllers and processors are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The assessment of what might be appropriate involves considering the context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals. Appropriate measures are set out as possibly including

- pseudonymization and encryption;
- ensuring confidentiality, integrity, availability, and resilience of processing systems and services;
- ability to restore availability and access to personal data promptly in the event of an incident; and
- the regular testing and evaluating of technical and organizational measures designed to ensure the security of data processing.

Controllers and processors are also required to ensure anyone acting under their authority accessing the personal data, does so only in accordance with their instructions. Compliance may) be demonstrated by adherence to an approved code of conduct or certification mechanism.

The Article 29 Working Party (WP29) guidance identifies three types of breaches. Some breaches may engage all three elements:

- confidentiality breach – unauthorized or accidental disclosure of or access to personal data;
- integrity breach – unauthorized or accidental alteration;
- availability breach – accidental or unauthorized loss of access to or destruction of data (e.g. by a power cut or systems failure).

All breaches must be recorded alongside the decision-making process engaged to decide whether or not to report the breach. Only breaches that are likely to result in a risk to the rights and freedoms of data subjects have to be reported to the Supervisory Authority (SA).

Timing of breach reporting to the SA

Data controllers are required to report a personal data breach to the competent SA without undue delay and, where feasible, not later than 72 hours after becoming aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

If a notification is made after the 72-hour period has expired, the data controller must explain the reasons for the delay.

The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and an approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Communication of a personal data breach to the data subject

Where a breach is reported to an SA and not to the data subjects, the SA may subsequently require the data controller to notify affected data subjects. There is no requirement to make a notification to the data subject where any of the following conditions have been met:

- technical and organizational measures have been applied to the personal data which will render it unintelligible to unauthorized persons (such as encryption);
- the controller has taken steps to ensure the originally high risk is no longer likely to materialize; or
- to notify each data subject would involve disproportionate effort, in which case a public communication or other methods of information can be used which would inform the affected data subjects in a similarly effective manner.

How to notify data subjects

The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Breach reporting obligations on processors

Data processors are required to notify controllers of a personal data breach without undue delay, which effectively means immediately.

NISD requirements

NISD is relevant to you if you are an Operator of an Essential Service (OES) or if you are a Digital Service Provider (DSP). Where sectors are subject to sector-specific Union legal acts relating to information and network security, these will take precedence.

How will organizations be regulated?

Organizations will be regulated in the Member State of their main establishment which will be where their head office is located. Where an organization is subject to NISD but does not have a main establishment in the EU, it must appoint a representative in one of the Member States in which it offers services and it will be subject to regulation in that Member State.

Incident response will be separate from incident reporting. The National Cyber Security Centre (NCSC) will be the UK's Computer Security Incident Response Team (CSIRT). Voluntary reporting can be made to either the CA or the NSCS. Incident response support on cyber-related

incidents will be provided by the NCSC where required. CAS or possibly the relevant Lead Government Department will provide support for non-cyber or resilience incidents (e.g. hardware failure, fire, physical damage).

Operators of essential services

- Member States are required to identify OESs in categories set out in Annex II of the Response with an establishment in their territory by 9 November 2018. These categories include operators of essential services in the energy, transport, financial services (including banks), health and drinking water supply, and digital infrastructure (including internet exchange points, domain name system service providers, and top-level domain name registries). Lists must be reviewed and updated at least every two years. The UK has published its list of OESs and their Competent Authorities (CAs) in the Response.
- Member States may make their own rules as to how to identify OESs in each sector but this is to be decided against the broad criteria that the entity provides a service essential for the maintenance of critical societal and/or economic activities where the provision of that service depends on network and information systems and an incident to the network and information systems of that service would have significant disruptive effects on its provision. Whether or not a disruption has a significant disruptive effect should take into account the number of users relying on the service, the dependency of other essential service sectors on it, the impact the incident might have, the market share and geographic reach of the entity and its importance in maintaining a sufficient level of service taking into account availability of alternative providers.

Security and notification requirements for operators of essential services

- Member States must ensure all OESs take appropriate and proportionate technical and organizational measures to manage risks (defined as “any reasonably identifiable circumstances or event having a potentially adverse effect on the security of networks and information systems”) posed to the security of networks and information services which they use to deliver their services and to minimize the impact of any network security incidents to ensure continuity of service.
- OESs must notify the competent authority or the CSIRT of incidents having a significant impact on the continuity of the service they supply. Notifications must be made without undue delay (and within 72 hours in the UK) and must contain enough information to allow the competent authority or the CSIRT to determine any cross-border impact of the incident. To assess the nature of the incident, the number of affected users, the duration of the incident, and the geographical spread of its impact must be taken into account.
- The public may be informed of an incident by the CA or the CSIRT.

2.2 HITECH Act The HITECH Act was implemented as part of the American Recovery and Reinvestment Act of 2009. Under this act, HIPAA was strengthened to include fines and a data

breach notification. To determine if a breach occurred the Hospital must perform an investigation to determine what data may have been breached. Civil Penalties are listed in the Table below :

Violation category	Each violation	All such violations of an identical provision in a calendar year
Did Not Know	$100–$50,000	$1,500,000
Reasonable Cause	$1,000– $50,000	$1,500,000
Willful Neglect—Corrected	$10,000– $50,000	$1,500,000
Willful Neglect—Not Corrected	$50,000	$1,500,000

Cost

Cost elements can be divided up into the following:
1. Per-incident loss estimates based on insurance claims, payout data, and activity-based incident cost estimates
2. Aggregate loss or impact estimates on the national scale
3. Academic or research papers on the short- and long-term impacts of cyber incidents
4. Individual case studies with scenario-based impact estimates.

These elements are what help New Yorks fines make their assumption about the overall cost of a company breach. While the numbers aren't exact and may vary depending on the severity of the breach this is the estimate we have concluded to.

(Cost per event in the millions)

Event Type	Number of Events	Mean	Standard Deviation	Median	Max
Data Breach	602	$5.87	$35.70	$0.17	$572
Security	36	$9.17	$27.02	$0.33	$100

Incident					
Privacy Violation	234	$10.14	$55.41	$1.34	$750
Phishing	49	$19.99	$105.93	$0.15	$710
Total	921	$7.84	$47.28	$0.25	$750

Response and Update Policies

Below are the steps that New yorks fines takes to review their response plan as well maintain and update to fit the new cyber threats that have arisen. We learn and are always adapting and improving on our risk models.
1) The person who discovers the incident will document all actions taken from this point on. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
a) Helpdesk.
b) IT Manager.
c) government entity

List all sources and check off whether they have contact information and procedures. Each source will contact one 24/7 reachable entity such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.

2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step four.

3) The Helpdesk/manager/IT Staff will refer to the IT emergency contact list or affected department contact list and call the designated numbers in order on the list. The Helpdesk will log:
a) The name of the caller.
b) Time of the call.
c) Contact information about the caller.
d) The nature of the incident.
e) When the event was first noticed, supporting the idea that the incident occurred.

4) The IT staff member or affected department staff member who receives the call will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will

contact the incident response manager using both email and phone messages. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could add the following:
a) Is the system affected business-critical?
b) What is the severity of the potential impact?
c) Name of the system being targeted, along with the operating system, Internet Protocol (IP) address, and location.
d) IP address and any information about the origin of the attack.

5) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
a) Is the incident real or perceived?
b) Is the incident still in progress?
c) What data or property is threatened and how critical is it?
d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
e) What system or systems are targeted, and where are they located physically on the network?
f) Is the incident inside the trusted network?
g) Is the response urgent?
h) Can the incident be quickly contained?
i) Will the response alert the attacker and do we care?
j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

6) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
a) Category one - A threat to public safety or life.
b) Category two - A threat to sensitive data.
c) Category three - A threat to computer systems.
d) Category four - A disruption of services.

7) Team members will establish and follow one of the following procedures basing their response to the incident assessment:
a) Worm response procedure.
b) Virus response procedure.
c) System failure procedure.
d) Active intrusion response procedure - Is critical or sensitive data (Personally Identifiable Information (PII), CJI, etc.) at risk?
e) Inactive Intrusion response procedure.
f) System abuse procedure.
g) Property theft response procedure.
h) Website denial of service response procedure.

i) Database or file denial of service response procedure.
j) Spyware response procedure. The team may create additional procedures which are not foreseen in this document. If there is no application procedure in place, the team must document what was done and later establish a procedure for the incident.

8) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

9) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

10) Upon management approval, the changes will be implemented.

11) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
a) Reinstall the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
b) Make users change passwords if passwords may have been sniffed.
c) Be sure the system has been hardened by turning off or uninstalling unused services.
d) Be sure the system is fully patched.
e) Be sure real-time virus protection and intrusion detection is running.
f) Be sure the system is logging the correct events to the proper level.

12) Documentation—the following shall be documented:
a) How the incident was discovered.
b) The category of the incident.
c) How the incident occurred, whether through email, firewall, etc.
d) Where the attack came from, such as IP addresses and other related information about the attacker.
e) What was the response plan was.
f) What was done in response?
g) Whether the response was effective.

13) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond, in case of an appeal.

14) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

15) In the event of a loss or suspected loss of criminal justice information, contact the Michigan State Police Information Security Officer via the CJIS-016 Form available on the MSP LEIN website

16) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

17) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
a) Consider whether an additional policy could have prevented the intrusion.
b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
c) Was the incident response appropriate? How could it be improved?
d) Was every appropriate party informed promptly?
e) Were the incident response procedures detailed, and did they cover the entire situation? How can they be improved?
f) Have changes been made to prevent reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?
g) Have changes been made to prevent a new and similar infection? h) Should any security policies be updated?
i) What lessons have been learned from this experience?

References

Criminal justice Information Center. (2020). *Example Incident Response Plan*. michigan.gov. https://www.michigan.gov/documents/msp/Example_Incident_Response_Policy_666657_7.pdf.

Cybersecurity & Infrastructure Security Agancy. (2020, October 26). *CO S ST OF A CYBER INCIDENT: SYSTEMATIC REVIEW AND CROSS-VALIDATION*. cisa. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Heywood, D. (2018, March 2). *Cybersecurity, data breach and incident reporting under the GDPR and NISD*. Lexology. https://www.lexology.com/library/detail.aspx?g=1b4a3144-6f76-40dd-b62f-588dc7ea004c.

Lessons Learned Information Sharing. (2020). *Emergency Management Programs for Healthcare Facilities: The Incident Management System* . LLIS.gov. file:///C:/Users/cassa/Downloads/765413.pdf.