CSIM Coursework 1

Proposal of a Cyber Incident Plan

Student ID: 2136685

Table of Contents

Table of Figures

Index of Tables

1. Part A – NIST and SANS Frameworks

1.1 Background

When it comes to incident response frameworks, the most widely recognised are the NIST and the SANS frameworks. NIST, a US government agency, published the Computer Security Incident Handling Guide to help organisations across the United States with implementing guidelines for information security policies and incident response.

The SANS Institute is an organisation that specialises in information security, providing certifications and training materials for professionals. Much like the NIST framework, the SANS Incident Handler's Handbook provides a structured approach to incident response, offering a guide on effectively addressing security incidents (Lumifi, 2024; Newton, 2021).

1.2 The Scope

The NIST framework was designed to be able to be adaptable to various types of organisations and industries, aimed at businesses of all sizes, including ones that may not have any personnel with information security knowledge, such as an online store. Consequently, the NIST framework tends to be more generalised compared to the SANS framework, only slightly broadening its scope.

One may argue that the SANS framework is aligned towards organisations that are more directly involved in information security, i.e. a data science organisation, due to SANS' reputation and standing in the cyber security industry.

As a result, the SANS framework contains more detailed checklists. For example, the SANS framework outlines a checklist template where specific registry keys should be inspected in case of an incident occurring on a machine running Windows, whereas NIST lists registry keys as one of the many attack vectors that may be associated with an incident (Cichonski et al., 2012; Kral, 2011).

The procedures that must be followed for each incident response framework are ultimately the same, the wording and grouping only differing slightly, as the SANS framework splits some processes that the NIST framework has grouped together into separate steps, making the SANS framework more granular. We will discuss this difference in the chapter below (Cranford, 2023).

1.3 Framework Steps

The NIST framework breaks down the process of incident response into four steps. Conversely, the SANS framework consists of the same processes, but broken down into six steps. Moreover, the processes that the steps describe in each framework are essentially the same, except the wording and the grouping of the steps, especially step 3.

SANS making the containment, eradication and recovery steps separately shows that they believe that all threats should be contained first, then eradicated and only then will the recovery process begin. Contrarily, the NIST framework believes those steps overlap and therefore one should not wait to contain all threats before moving on to eradicating or recovery (Cranford, 2023; Girken, 2019; Lumifi, 2024).

Table 1: NIST and SANS Steps

NIST Steps	***SANS Steps***
Preparation	Preparation
Detection and Analysis	Identification
Containment, Eradication and Recovery	Containment
	Eradication
	Recovery
Post-Incident Activity	Lessons Learned

1.4 Conclusion

As discussed in the chapters above, the two frameworks do differ, although not enough to define any framework as superior. Ultimately, it comes down to the organisation's available resources and which framework would be a better fit for the organisation.

2. Part B – Standard Operating Procedure

2.1 Purpose

The General Data Protection Regulation and Data Protection Act legislations state thtat any type of data breach must be reported to the ICO (ICO, 2023a).

A data breach is defined by the ICO as:
"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data" (ICO, 2023b).

The following SOP outlines what a security incident is, how to report one and how to conduct one's self should one occur. This SOP outlines steps to ensure that ABC fully complies with UK GDPR and DPA legislations.

2.2 Scope

A security incident is any event that can lead to loss or damage to ABC's information assets. A security incident can cause a breach of legislation, regulation and confidentiality, integrity or availability (Police Scotland, 2019).

This SOP must be followed by all employees, defined in Chapter 2.3.

This SOP will only outline the incident response actions for the following incidents:

- Phishing incidents
- Ransomware incidents

The incidents above are the most likely to occur to ABC, therefore they must be prioritised when outlining how to handle security incidents. Any other type of security incident will not be discussed, and therefore neither will their response, as they fall beyond the scope of this SOP, for example denial-of-service incidents.

2.3 Responsibilities

The CTO is responsible for the information assets of ABC, overseen by the CEO as the owner of the assets. They are responsible for the security of ABC and the security actions of the staff. The CTO must keep the executive board in the know about any security concerns regarding ABC.

All staff of all departments have a responsibility to report suspicious activity to their respective managers. If the respective manager can not be reached, staff must notify the IT/CSIRT team manager

Managers must make a judgment whether the reported activity is truly suspicious, then contact the IT team manager if a security incident has occurred.

IT/CSIRT team manager must handle the creation of incident response policies, the IT team’s budget and the IT team’s staff. They must also communicate the security incidents effectively to the team and the CTO (Cichonski et al., 2012; Police Scotland, 2019).

IT/CSIRT team staff must appropriately investigate, eradicate and report a security incident, according to the SOP.

Lawyers must review that ABC is fully compliant with the UK legislations, including the SOP. Should an incident have legal ramifications, they must prepare evidence for any lawsuit that may occur (Cichonski et al., 2012).

Public relations staff must communicate the breach a security incident with the stakeholders and the general public, if the incident needs to be public (Cichonski et al., 2012).

Human resources must handle disciplinary action, should an employee is known to have caused the security incident (Cichonski et al., 2012).

2.3.1 Tools

The IT/CSIRT team must have tools readily available to be able to conduct a swift incident response. The tools should be packaged in a way that can be quickly grabbed and easily portable, for example, a backpack (Kral, 2011).

For swift communication, the backpack must include (Cichonski et al., 2012; Kral, 2011):

- Contact information for the CSIRT team
- Contact information for the CTO, should the security incident escalate
- Contact information for law enforcement
- Smartphone
- A copy of the SOP and an incident handling checklist

For handling the security incident, the following tools must be present (Cichonski et al., 2012; Kral, 2011):

- Laptop equipped with:
  - Packet sniffer software
  - Anti-malware software
  - Forensic software (FTK, Autopsy)
- Write blocker
- Blank USB drives
- Bootable Live USB drives with specific tools for incident response, such as FTK Imager
- Networking equipment, such as network cables
- Evidence gathering accessories, such as:
  - Notebooks
  - Digital camera
  - Audio recorder
  - Evidence bags, tags and tape, kept for legal evidence

2.5 Incident Handling

Upon detecting suspicious activity, **a staff member must**:

1. Report to their respective department manager
2. Cooperate with any requests the department manager has, within the scope of the security incident

Upon receiving a report, **a department manager must**:

1. Gather information from the reporting staff
2. Determine whether it is a true positive
3. Contact the CSIRT team manager with details about the new security incident
4. Communicate and coordinate with CSIRT team manager until the security incident is resolved

Upon receiving a report from a department manager, **the CSIRT team manager must**:

1. Communicate and coordinate with the department manager to get a comprehensive understanding of the security incident
2. Communicate with the CSIRT team and assign roles within it for an appropriate and detailed investigation of the security incident
3. The CSIRT team manager must report to and keep the CTO updated on the security incidents as the investigation progresses
4. Once the investigation has been completed, suggest the best course of action to the CTO, be it either, some or all of:
    - Involving the Human Resources department for disciplinary action, should a staff member have caused the security incident
    - Informing ABC’s lawyers, should the security incident be reported to the ICO
    - Informing the Public Relations staff, should the nature of the security incident require a disclosure to the stakeholders and/or the public

Upon receiving a report from the CSIRT team manager, **the CTO must**:

1. Communicate with the CSIRT team manager, to get the details about the security incident
2. Aid the CSIRT team with any requests that will ensure a swift incident response, such as acquiring a new tool.
3. Form a business incident summary for the executive board, as the security incident is being investigated
4. After the investigation has completed, form a comprehensive business report, to fully inform the executive board, including the recommended course of action from the CSIRT team.

2.5.1 Phishing Incident Handling

This section is an addition to the generalised steps described above. The section will **only** outline the additional steps required, without reiterating the steps outlined in the section above.

Moreover, this section will mainly outline the steps required for the CSIRT team to properly handle a phishing incident.

2.5.1.1 Unsuccessful Phishing Attempt

Upon detecting a phishing email, **a staff member must**:

1. Take note of the email, including the time it was received, the email address and the entity it is impersonating
2. Report the gathered information to the department manager

Upon receiving a ransomware report, **a department manager must follow the general steps.**

Upon receiving a phishing report from a department manager, **the CSIRT team manager must**:

1. Inform a CSIRT team member that can add the gathered information into the Mimecast Email filter.

The CTO does not need to be informed if the phishing attempt is unsuccessful.

2.5.1.2 Successful Phishing Attempt

Upon falling for a phishing email, **a staff member must**:

1. Take note of the email, including the time it was received, the email address and the entity it is impersonating
2. Explain the situation to the department manager
3. Inform the department manager of the information that was leaked

Upon receiving a ransomware report, **a department manager must follow the general steps.**

Upon receiving a phishing report from a department manager, **the CSIRT team manager must follow the general steps.**

The CSIRT team must:

1. Add the gathered information from the reporting staff member into the Mimecast Email filter.
2. Mitigate the risk that comes from the leaked information, be it:
    - A data leak, by invalidating the records (i.e. asking customers to change their passwords, should the data that was leaked be a user credentials database)
    - Staff member credentials leak, by temporarily restricting access and forcing a password change

Upon receiving a phishing report from the CSIRT team manager, **the CTO must**:

1. Inform the public relations and ABC's lawyers, should the incident be in need of being disclosed to the stakeholders or the public
2. Task the lawyers with gathering evidence for a potential legal proceedings
3. Task the lawyers with reporting the security incident to the ICO, should the CSIRT team determine that ABC's data has been breached

2.5.2 Ransomware Incident Handling

Upon detecting ransomware, **a staff member must**:

1. Report the specific machine affected to the department manager

Upon receiving a ransomware report, **a department manager must follow the general steps.**

Upon receiving a ransomware report from a department manager, **the CSIRT team manager follow the general steps.**

The CSIRT team must:

1. Assess the damage done to ABC's information assets
2. To gather evidence, complete a full forensic analysis of the machine, gathering any indicators of compromise from the ransomware
3. Check for the latest available backup
4. Explain the extent of the data that was lost to the CSIRT team manager
5. Restore the machine from backup

Upon receiving a report from the CSIRT team manager, **the CTO must**:

1. Inform the public relations department and ABC's lawyers as this security incident must be disclosed to the stakeholders and the public
2. Task the lawyers with gathering evidence for potential legal proceedings
3. Task the lawyers with reporting the ransomware incident to the ICO

References

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, [online] 2(2). doi:https://doi.org/10.6028/nist.sp.800-61r2.

Cranford, J. (2023). *Incident Response Steps: How to Respond to Data Breach | CrowdStrike*. [online] crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/ [Accessed 21 Feb. 2024].

Girken, E. (2019). *Incident Response Steps Comparison Guide for SANS and NIST*. [online] Att.com. Available at: https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide [Accessed 21 Feb. 2024].

ICO (2023a). *Personal data breaches*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/personal-data-breaches/ [Accessed 23 Feb. 2024].

ICO (2023b). *Personal Data breaches: a Guide*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/ [Accessed 23 Feb. 2024].

ISA Cybersecurity (2021). *Comparing NIST & SANS Incident Frameworks*. [online] ISA Cybersecurity Inc. Available at: https://isacybersecurity.com/comparing-nist-sans-incident-frameworks/ [Accessed 21 Feb. 2024].

Kral, P. (2011). *Incident Handler's Handbook*. [online] Egnyte. Available at: https://sansorg.egnyte.com/dl/6Btqoa63at [Accessed 21 Feb. 2024].

Logsign (2023). *Incident Response Steps for SANS & NIST Frameworks*. [online] www.logsign.com. Available at: https://www.logsign.com/blog/incident-response-steps-for-sans-nist-frameworks/ [Accessed 21 Feb. 2024].

Lumifi (2024). *NIST and SANS Incident Response Frameworks Explained*. [online] Lumifi Cybersecurity. Available at: https://www.lumificyber.com/blog/nist-and-sans-incident-response/ [Accessed 21 Feb. 2024].

Newton, S. (2021). *Understanding Incident Response Frameworks - NIST & SANS*. [online] www.stickmancyber.com. Available at: https://www.stickmancyber.com/cybersecurity-blog/incident-response-frameworks-nist-sans.

Police Scotland (2019). *Information Security Incident Reporting Standard Operating Procedure*. [online] Available at: https://www.scotland.police.uk/spa-media/eswm0eog/information-security-incident-reporting.pdf [Accessed 23 Feb. 2024].

Appendix

A.1 Assumptions

1. Assuming that ABC is a business operating solely out of the United Kingdom.
2. Assuming that ABC has an existing risk assessment and owners of the assets have been established.
3. Assuming that ABC has these additional employees:
    - Lawyers
    - Public relations staff
4. Assuming that the CSIRT team exists and it consists of the IT team and lawyers, public relations and human resources staff.
5. Assuming that the IT team has staff that are technical in:
    - Network Administration (Firewalls, topology)
    - Network Analysis (Analysing packet captures)
    - Security Alerts Monitoring (Analysing intrusion detection system alerts)
    - System Administration (Maintaining servers – keeping software up-to-date, applying patches)
    - Incident Detection and Analysis (Log collecting and analysing)
6. Assuming that the IT staff has been trained in incident response.
7. Assuming that ABC uses an intrusion detection system.
8. Assuming all staff has been trained in simple information security training, such as detecting phishing emails.
9. Assuming that ABC has an information security policy in place.
10. Assuming that ABC has an incident handling checklist.
11. Assuming that ABC does regular backups of their machines.

A.2 Figures

Figure 1: "ABC" Organisational Chart