[Introduction 1](#_Toc2055349647)

[Task 1 - 3 different incident handling techniques used in cyber forensics 1](#_Toc353646347)

[SANS Incident Response Life Cycle 2](#_Toc1147688688)

[NIST Technique 3](#_Toc1804997292)

[CSIRT 3](#_Toc598018835)

[Strengths and Weaknesses 4](#_Toc1341509687)

[Case Study 4](#_Toc304381597)

[Conclusion 4](#_Toc1912010694)

# Introduction

In Cyber Forensics, incident response can have many benefits such as: Rapid Response and Damage Control which allows for minimal damage from the attack, Evidence Collection Proper incident handling which ensures evidence is collected and preserved in a forensically sound manner as well as Compliance and Legal Issues since many regulations require organizations to report security breaches. It's also useful in terms of Proactive Defense. By understanding the attacker's methods and the vulnerabilities exploited during the incident, organizations can strengthen their security posture.

For this assignment I will examine and differentiate between multiple incident handling methods applied in cyber forensics. The specific incident handling techniques chosen will be from the SANS, NIST and CSIRT. They all consist of the main phases which include Preparation, Identification and Assessment, Containment, Investigation, Recovery and finally Evaluation. This assignment will also cover the strengths and weaknesses of all these techniques while also providing a real-world scenario of when these IRLC were used during a major attack and their effectiveness.

# Task 1 - 3 different incident handling techniques used in cyber forensics

When cyber security attacks occur, there are usually set protocols in place to help companies streamline the recovery process *(WirexSystems, 2023)*. These are called incident handling techniques. These methods are crucial for collecting, preserving, analyzing, and presenting digital evidence in a way that adheres to legal standards. There are many different methods of incident handling and some work better than others depending on the scenario. The key methods included will come from the Incident Response Life Cycle

## SANS Incident Response Life Cycle

Incident Response Life Cycle or IRLC is a model used to effectively manage and respond to security incidents. The steps are as followed:

Preparation – in this phase, it is important to make sure that all access points are secured and that any potential weaknesses in the system have been resolved. This is important as preventing the attack from happening in the first place is much more effective than trying to resolve the issue after the damage has already been done. *(TitanFile, 2022)*

Identify and assess – let us say the 1st step has failed already. The next step in the cycle is to identify and assess whether the recent event is a cyber-attack or not. The organization can then decide the next appropriate steps. *(TitanFile, 2022)* This step is also important because it will also help the company know whether it was the fault of an internal employee or a genuine external cyber threat.

Containment – Now we know that the company has suffered a genuine cyber-attack, it is time to contain the threat. This is where various software such as antiviruses come into play. *(TitanFile, 2022)* They scan the system for the threat and quarantine the malicious files. This means they can no longer affect the system and they can be deleted without causing any further damage.

Investigation – this is where the “post attack phase begins.” It is crucial that the company does some investigating to find out how the attack started and where it came from. As mentioned earlier, it could have been internal (coming from the company) or external (a third-party threat such as a hacker). This links with the identify and assess step as it helps them recognize weaknesses in the system that can be exploited in the future. *(TitanFile, 2022)*

Recovery and restoration – Any company with good cyber security measures will have multiple backups of the data that is vulnerable to attacks. *(TitanFile, 2022)* The more sensitive the data, the more important it is to have this. The data recovery section involves restoring all affected systems to their “pre-attack state” and re-instating any data that was lost or corrupted.

Evaluation – Over “67% of companies that get hacked will suffer another attack within the same year.” (*security intelligence, 2023).* To prevent this, it is important for companies to keep data about the attack to evaluate their performance in handling the threat which will aid them in creating further prevention methods.

## NIST Technique

If the SANS technique is not best suited for a particular business, the NIST framework does a similar job with fewer steps. Its processes include:

Preparation – same as SANS, both require the company to make sure they are prepared for any attacks.

Detection and Analysis – combines the main bulk of the SANS method into one step. The threat is both found and analyzed in this step, allowing for a less thorough but quicker response time. *(NIST, 2019)*

Containment, eradication, and recovery – like the last step, the last few steps from the SANS technique have been combined into one. Here, the threat is sectioned off from the system, deleted and all files should be recovered here.

Post-incident activity – a broader version of the final point in SANS. The company is given more liberty to complete any steps of evaluation based on what policies they have in place.

## CSIRT

Another Technique used in the cyber forensics industry is the CSIRT method. It’s a team dedicated to handling any digital/cyber threats an organization might come across. The 3 main steps they will take include:

Preparation – same as SANS and NSIRT but has one main goal, prepare a team of staff who have the skills to deal with cyber-attacks as well as security measures they must follow. *(NCSC, 2019)*

Detection – just like the other methods. The CSIRT team uses their resources to detect whether a cyber-attack has occurred or not.

Analysis - the team does further investigations to find out how the attack started and where it came from. They also look for what exactly the attack did to figure out what kind of threat it was (malware, phishing attack etc.)

# Strengths and Weaknesses

SANS can be highly effective when handling serious cyber threats. The evaluation section allows companies to keep information about the attack to train staff to spot the signs of cyber-attacks which will drastically reduce the chance of another one in the future. Its weaknesses lie in the amount of time it may take for a company to execute the IRLC. Not every business will be able to operate on the time scale required for it to be effective. *(isaCyberSecurity, 2021)* The longer the recovery period, the more damage that can be done, especially when dealing with many customers. This is where companies will want to lean towards the NIST or CSRIT framework. It allows for a swifter response to attacks, with CSRIT moving the responsibility to an entire team meaning the business can operate smoothly. *(CSIRT, 2019)*

# Case Study

One example was when the NHS was infected by a ransomware attack in 2017 called “WannaCry”. Millions of windows users globally woke up to see their systems had been locked with them having to pay a ransom to receive their files back. *(kaspersky, 2019)* Since the evaluation section provides insight into prevention, the next preparation phase (in the SANS) that the NHS or Microsoft would have to go through would be much easier. Ideally, they would only have to install Windows security patches installed on their devices to prevent infection in the first place. In terms of the lessons learned in the evaluation section. Big companies like the NHS realized that they need to invest the time and finances into hiring the correct staff who know how to properly secure sensitive data. *(Acronis, 2020)* Based on this specific case and the nature of the company that was attacked by WannaCry, they most likely used the CSIRT or SANS method, it

# Conclusion

In conclusion, organizations use specific methods to handle cyber-attacks. These include the SANS, NIST and CSIRT method. They all use a mix of the same principles: Preparation, Identification and Assessment, Containment, Investigation, Recovery and finally Evaluation. In real world scenarios, each of the methods have their own benefits. SANS is more thorough and relies on a full organizational analysis whereas NIST is more compact which is great for companies operating on a smaller time scale. The CSIRT is perfect for established businesses with dedicated response teams allowing for a smooth threat response.

*References*

Acronis. “The NHS Cyber Attack.” *Acronis*, 7 Feb. 2020, www.acronis.com/en-gb/blog/posts/nhs-cyber-attack/.

“CSIRTs Network.” *Csirtsnetwork.eu*, 2019, csirtsnetwork.eu/.

ISA Cybersecurity. “Comparing NIST & sans Incident Frameworks.” *ISA Cybersecurity Inc.*, 3 Feb. 2021, isacybersecurity.com/comparing-nist-sans-incident-frameworks/.

Kaspersky. “What Is WannaCry Ransomware?” *Kaspersky.com*, Kaspersky, 2019, www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Montag, Gal. “SANS Incident Response Framework.” *WireX*, 31 Jan. 2023, wirexsystems.com/resource/sans-incident-response-framework/#:~:text=The%20SANS%20Incident%20Response%20Framework.

National Cyber Security Centre. “Build: A Cyber Security Incident Response Team (CSIRT).” *Www.ncsc.gov.uk*, 19 Sept. 2019, www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team.

NIST. “NIST Cybersecurity Framework.” *NIST*, 7 Feb. 2019, www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0.

Rodrigues, Joakim. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.

---. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.

---. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.

---. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.

---. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.

---. “7 Phases of Incident Response.” *TitanFile*, 3 Oct. 2022, www.titanfile.com/blog/phases-of-incident-response/.