LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC5052NI Risk, Crisis & Security Management

50% Individual Coursework

on

Incident Response Policy and procedures

Semester 3

2024-25 Autumn

Student Name: Anshumala Bhandari

London Met ID:23047472

College ID:NP01NT4A230149

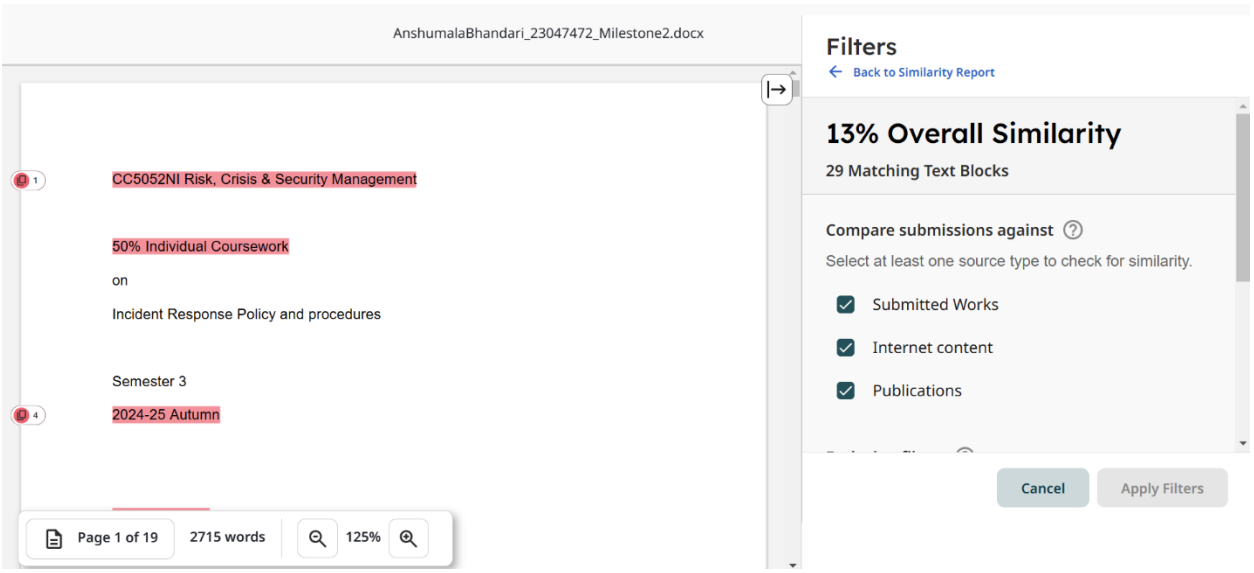
Assignment Due Date:10th January, 2025

Assignment Submission Date:10th January, 2025

Submitted To: Aakash Ojha

Count: 2011

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.


AnshumalaBhandari_23047472_Milestone2.docx
CC5052NI Risk, Crisis & Security Management
50% Individual Coursework
on
Incident Response Policy and procedures
Semester 3
2024-25 Autumn
Page 1 of 19
2715 words
125%
Filters
Back to Similarity Report
13% Overall Similarity
29 Matching Text Blocks
Compare submissions against
Select at least one source type to check for similarity.
Submitted Works
Internet content
Publications
Cancel
Apply Filters

Acknowledgement

I am extremely thankful to everyone who helped me throughout the completion of this coursework. Firstly, I am deeply thankful to my tutor, whose guidance, patience, and valuable feedback played an important role in shaping my work and helping me stay on the right track. I appreciated the encouragement they provided.

I would also like to acknowledge the knowledge I gained from various research papers, reports, and frameworks that I came across during my studies. These resources provided me with essential insights and ideas that were important in completing my work. I am also thankful to my friends and colleagues, who kept me motivated and supported me throughout the process.

To everyone who supported my learning experience, whether directly or indirectly, I am very grateful. This accomplishment would not have been possible without the help I recevied, and I sincerely appreciate every bit of support I received along the way.

Abstract

This report focuses on the importance of having a clear and effective Incident Response Policy and Procedure in organizations to manage security breaches and cyber incidents. It covers the main steps of an incident response plan, such as preparation, identifying and containing problems, fixing the issue, recovering, and learning from the experience. The report also explains best practices for creating and following these plans to help organizations react quickly, reduce harm, and return to normal operations. It looks at common challenges organizations face during cyber incidents and highlights the roles of different teams in managing them.

Through real-life examples, such as the SolarWinds cyberattack, this report shows how incident response plans can make an organization's ability to handle cyber threats, protect valuable data, and improve overall cybersecurity stronger. Through understanding these processes, businesses can be prepared in a better way to manage incidents while minimizing the impact of cyber-attacks. The report focuses on the need for continuous improvement, training, and real-time monitoring to address increasing threats.

It also discusses the importance of keeping incident response plans updated, as new cyber risks are constantly evolving. A strong incident response plan not only helps businesses recover quickly but also makes organizations strong against future attacks, ensuring long-term cybersecurity protection. By updating plans, improving monitoring, enhancing training, protecting assets, and addressing evolving risks efficiently.

Table of Contents

Table Of Figures

1. Introduction

Organizations nowadays are facing many cyber threats which includes data breaches, malware attacks and hacking. Without a proper plan to handle these incidents it is difficult for organizations to respond quickly and effectively which leads to significant financial loss, data theft, and damage to their reputation.

Due to the cyber-attacks being more frequent and complex it is very important for businesses to follow an Incident Response Policy and Procedures properly. A good Incident response plan is very necessary to reduce damage, ensuring fast recovery and to protect sensitive data. It also helps businesses to follow regulations and maintain customer trust.

Creating a successful Incident Response Plan is not simple as cyber threats are always changing and many companies do not have the resources or expertise to handle them. Without proper preparation, it can be difficult to respond quickly, leading to more damage and longer recovery times.

Many incident response plans right now are outdated or incomplete. Some businesses also cannot keep their plans up to date or don't provide enough training for employees. This leaves them unprepared when a cyberattack happens, making it difficult to react effectively.

This report focuses on the key steps in an incident response process while including preparation, detection, containment, recovery, and post-incident review. It also discusses the challenges organizations face and offers best practices for developing a strong IRP.

1.1 Aim

This report aims to explain why having a good Incident Response Policy is important. It focuses on the key steps to handle cyber incidents effectively and gives simple suggestions to help organizations to be prepared for cybersecurity threats. It also looks at common challenges and gives suggestions to improve incident response strategies to properly handle modern cybersecurity threats.

1.2 Objectives

- To understand the basics of Incident Response by learning the main steps and parts of an incident response plan for handling cyber incidents.
- To identify common problems by spotting typical issues, like slow detection and lack of preparation, that affects response.
- To provide practical advice by offering tips for creating a strong response plan that helps to reduce damage.
- To learn from real examples by studying real incidents, like SolarWinds, and see what can improve responses.
- To suggest future improvements by recommending ways to improve response plans, including better tools and training.

2. Literature Review

Incident response frameworks are very essential tools as it manages and reduces cybersecurity threats. Among these, the **NIST Cybersecurity Framework** is one of the most widely known cybersecurity Framework and it is utilized globally. It is Published by the **National Institute of Standards and Technology (NIST)**, this framework provides a proper way to manage cybersecurity risks and responding to incidents effectively (National Institute of Standards and Technology (NIST), 2022).

NIST Cybersecurity Framework

It is valuable because it has detailed guidelines for building Incident Response Plans (IRPs). It help's organizations to identify, protect, detect, respond, and recover from cybersecurity incident. It is used across industries, making it an adaptable tool for many organizations. It has been known for its clear structure and practical application in various sectors, making it a foundation for many organizations incident response strategies (National Institute of Standards and Technology (NIST), 2022).

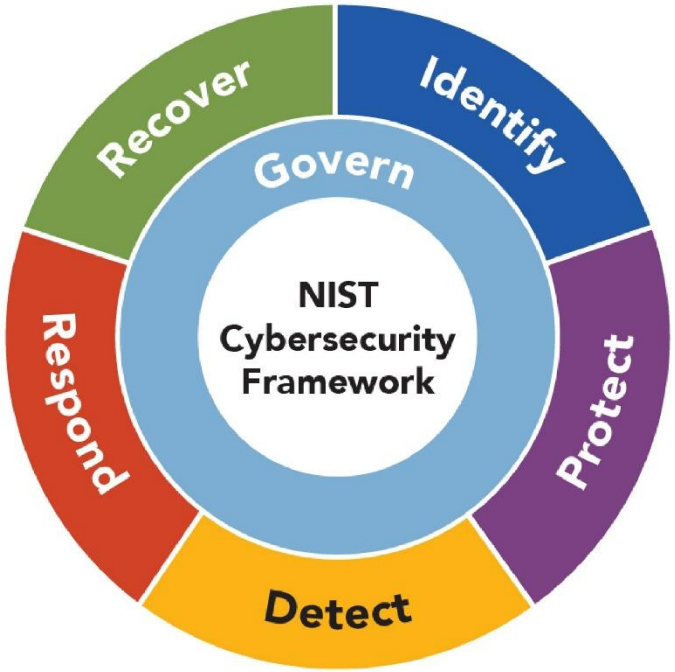


Figure 1:Cybersecurity Framework

However, some researchers argue that the NIST framework can be too general for addressing industry-specific challenges. For example, the **U.S. Government Accountability Office (GAO)** highlights that organizations in highly regulated sectors like healthcare and finance may need more specific guidance (U.S. Government Accountability Office (GAO), 2024). Despite this limitation, the NIST framework is very important in cybersecurity planning due to its focus on preparation and continuous improvement (National Institute of Standards and Technology (NIST), 2022).

Phases of IRP

The NIST framework divides the incident response process into six key phases. Each phase provides a well-prepared way to handle and mitigate the effect of cybersecurity incidents effectively:

1.Preparation

Preparation is the first and most crucial step in incident response. It involves setting up plans, policies, and procedures to handle potential cybersecurity incidents. Organizations make sure that their teams are well-trained, know their roles, and have access to necessary tools like antivirus software, firewalls, and backup systems. Regular simulations or practice drills are conducted to make sure everyone is ready to act during an actual incident. Its main goal is to build a strong foundation to deal with any threats effectively (David Geer, 2024).

2. Detection and Analysis

This phase is about identifying when something unusual or suspicious happens in the system. Organizations use monitoring tools, such as intrusion detection systems and log analyzers, to detect unusual activity. When an alert is generated, the team investigates to determine if it's a real threat and how severe it is. Quick action and thorough analysis help to understand what happened and guide the next steps (David Geer, 2024).

3. Containment

Containment focuses on stopping the incident from causing further damage. For example, if a system is compromised, it may be isolated from the network to prevent the attack from spreading. Temporary fixes are often applied during this stage while a permanent solution is being planned.

This step helps to minimize the impact of the incident while keeping essential systems keep working (Fahri Yesil, 2024).

4. Eradication

Once the threat is under control, the next step is to remove it completely. This includes deleting malware, closing backdoors used by attackers, and fixing any vulnerabilities that were exploited. The team carefully checks to ensure that all traces of the threat are eliminated. This step makes sure the attackers cannot re-enter the system using the same methods (Fahri Yesil, 2024).

5. Recovery

After the threat is eradicated, systems need to be restored to their normal state. This involves reinstalling clean backups, patching vulnerabilities, and ensuring the system is secure. The team tests the systems to make sure they are working properly and monitors them closely to confirm that no further suspicious activity occurs. This phase ensures the organization can resume regular operations safely (Fahri Yesil, 2024).

6. Post-Incident Activity

This phase focuses on learning from the incident. The team reviews what happened, how it was handled, and identifies areas for improvement. A detailed report is created, and the incident response plan is updated based on the lessons learned. This helps the organization to strengthen its defenses and be better prepared for future incidents (simeononsecurity, 2023).

Strengths and Limitations

The NIST framework's clear structure and detailed approach makes it highly effective for guiding incident response. Its adaptability allows organizations to customize it to their specific needs. However, it requires more changes for industry-specific challenges. Additionally, implementing the framework fully requires significant resources and expertise, which might not be possible for smaller organizations (U.S. Government Accountability Office (GAO), 2024).

Focusing on the NIST Cybersecurity Framework highlights the importance of having a well-defined incident response process. By breaking down the phases, it becomes clear how each step contributes to minimizing the impact of cybersecurity incidents. This detailed explanation shows the value of preparation and continuous improvement to making an organization strong against cyber threats (National Institute of Standards and Technology (NIST), 2022).

3. Analysis

Incident response techniques play a critical role in managing cybersecurity threats. To analyze these techniques, this section discusses the SolarWinds cyberattack as a case study. The SolarWinds attack highlights the challenges faced in detecting and mitigating advanced persistent threats (APTs). Reflections on insights gained through this study offers a deeper understanding of the practical application and limitations of incident response strategies.

Figure 2: SolarWinds

Issues Identification, Comparative Analysis, and Case Study

The **SolarWinds cyberattack** is one of the most well-known cybersecurity breaches that has occurred. In this attack, malicious hackers exploited vulnerabilities in SolarWinds' Orion software, a network monitoring tool, to distribute malware and infiltrate numerous organizations. This breach affected several big organizations and government agencies and private companies. The attack demonstrates issues related to detection, containment, and recovery in the incident response process.

1. **Detection Challenges**: Despite having advanced monitoring systems, the attack was undetected for months. The malware that was used was very undetectable and use of proper

credentials were also made which caused the activities to be hidden which made detection difficult. This shows the limitations that traditional detection methods have while identifying complex threats.

The attackers inserted malicious code in a legitimate software update, a tactic known as a supply chain attack, which bypassed standard detection mechanisms (Cybersecurity and Infrastructure Security Agency (CISA), 2020).

If organizations used advanced anomaly detection systems, such as AI-based monitoring it might have identified unusual behaviors sooner (National Institute of Standards and Technology (NIST), 2022)

2. **Containment Difficulties**: After the breach was discovered, containing the attack was very difficult due to its widespread nature. The malware had infiltrated multiple systems which required detailed isolation strategies.

   Government agencies had to disconnect entire networks to prevent the attack to spread further, which disrupted operations (U.S. Government Accountability Office (GAO), 2024).

   Organizations with a segmented network architecture managed to contain the damage more effectively compared to those with flat network structures (Cybersecurity and Infrastructure Security Agency (CISA), 2020).

3. **Recovery and Post-Incident Challenges**: Recovery was time-consuming and resource-intensive, as affected organizations had to rebuild compromised systems, replace hardware, and strengthen security measures. The lack of an established incident response playbook increased the recovery process for some organizations.

   Companies that had not conducted regular incident response drills found it difficult to restore operations quickly (Symantec Corporation, 2017).

   Organizations with predefined recovery plans resumed operations more efficiently, highlighting the importance of preparation and training (National Institute of Standards and Technology (NIST), 2022).

Figure 3: Lessons Learned

Reflection and Insights

Analyzing the SolarWinds case study provides valuable information about the use of incident response techniques:

1. **The Importance of Detection Tools**: The case proves that traditional detection tools may not be enough for complex attacks. Machine learning and behavior-based detection systems should be included for identifying abnormal behavior that may indicate a breach is going to occur (National Institute of Standards and Technology (NIST), 2022).
2. **Preparedness and Adaptability**: A key information we can learn from this is the need for strong preparation, including segmented networks, incident response drills, and real-time monitoring. Organizations that invested in these areas faced fewer disruptions and recovered faster (U.S. Government Accountability Office (GAO), 2024).
3. **Continuous Improvement**: The SolarWinds breach demonstrates the importance of post-incident reviews in improving incident response plans. Regular updates and adaptability make's sure that organizations can handle evolving threats properly (Cybersecurity and Infrastructure Security Agency (CISA), 2020).

Through this reflection we know the value of applying a structured approach to incident response, such as the NIST Cybersecurity Framework, which focuses on preparation, detection, containment, recovery, and continuous improvement (National Institute of Standards and Technology (NIST), 2022).

4. Conclusion

The report includes the importance of having a clear and effective Incident Response Plan to handle cyber threats. It explains how the NIST Cybersecurity Framework, with its structured approach such as preparation, detection, containment, recovery, and post-incident review helps organizations manage cybersecurity risks effectively. The SolarWinds cyberattack case study demonstrates the challenges of detecting advanced threats, the difficulty in containing widespread attacks, and the importance of recovery strategies. Organizations with proper preparation, such as segmented networks and regular incident response drills, were able to recover faster and limit damage.

The report also discusses the importance of advanced tools, like AI-based anomaly detection as they can improve early threat detection and traditional detection tools may not be enough for modern, complex threats. Continuous updates and regular training are necessary to keep incident response plans relevant as cyber risks are evolving. Organizations that adapt and improve their plans after each incident become stronger against future attacks.

The SolarWinds case study focuses on the need for a well-prepared approach such as Strong preparation, adaptable strategies, and continuous improvement that makes sure that organizations can reduce harm, recover quickly, and strengthen their defenses. By investing in these areas, businesses can protect valuable data, maintain customer trust, and ensure long-term cybersecurity protection. In today's world, where cyber threats are increasing and becoming more complex, implementing and having a strong incident response plan is not just important it is also essential.

5. References

Symantec Corporation, 2017. *Cyberattack Response: Lessons Learned from Major Breaches,* Mountain View, California: Symantec Corporation.

Cybersecurity and Infrastructure Security Agency (CISA), 2020. *Cybersecurity Advisory: SolarWinds Orion Compromise.* [Online] Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-352a[Accessed 26 December 2024].

David Geer, 2024. *Building an incident response framework for your enterprise.* [Online] Available at: https://www.techtarget.com/searchsecurity/tip/Incident-response-frameworks-for-enterprise-security-teams?utm_
[Accessed 9 January 2025].

Fahri Yesil, 2024. *Incident Response: A Comprehensive Guide for Businesses and Cybersecurity Professionals.* [Online] Available at: https://infosecwriteups.com/incident-response-a-comprehensive-guide-for-businesses-and-cybersecurity-professionals-f4debbcb5ecc
[Accessed 9 January 2025].

IBM Security, 2024. *Cost of a Data Breach Report 2024,* Cambridge, MA: IBM Security.

National Institute of Standards and Technology (NIST), 2022. *NIST Cybersecurity Framework Version 1.1,* Gaithersburg: NIST.

simeononsecurity, 2023. *Mastering Cybersecurity Incident Response: A Definitive Guide for Success.* [Online] Available at: https://simeononsecurity.com/articles/mastering-cybersecurity-incident-response-guide/?utm_
[Accessed 9 January 2025].

Software Engineering Institute, Carnegie Mellon University, 2020. *Incident Management Capability Metrics,* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

U.S. Government Accountability Office (GAO), 2024. *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation,* Washington, DC: U.S. Government Accountability Office.

U.S. Government Accountability Office (GAO), 2024. *The SolarWinds Cyberattack and Federal Response,* Washington, D.C.: U.S. Government Accountability Office.

Verizon Enterprise Solutions, 2014. *2014 Data Breach Investigations Report,* Basking Ridge, New Jersey: Verizon Communications Inc.