LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC5052NI Risk, Crisis & Security Management

50% Individual Coursework

on

Security Policy, Standard, and Practices

Semester 3

2024-25 Autumn

Student Name: Gaurav Pratap Malla

London Met ID: 23047411

College ID: NP01NT4A230108

Assignment Due Date: Wednesday, November 20, 2024

Assignment Submission Date: Friday, January 10, 2025

Submitted To: Akash Ojha

Count: 2147

I confirm that I understand my coursework needs to be submitted online via MST/ My second teacher 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.

Semester 3

2024-25 Autumn

Student Name: Gaurav Pratap Malla

London Met ID: 23047411

College ID: NP01NT4A230108

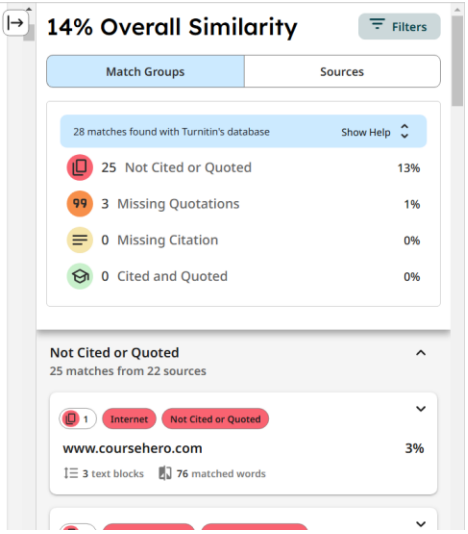
Assignment Due Date: Wednesday, November 20, 2024

Assignment Submission Date: Friday, January 10, 2025

Submitted To: Akash Ojha

Count: 2147

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



Acknowledgement

I am thankful of Islington College for providing me with the necessary skills to get this completed coursework. I would like to thank my lecturer Mr. Apil Chand, and tutor Mr. Akash Ojha for the most necessary guidance I got during the whole learning experience. Their guidance and support mentored my academic growth throughout my semester.

Abstract

The present research focuses on raising awareness regarding security awareness and training programs needed by organisations to enhance security. What it does is explain how such programmes enable the employees to recognise and be on the lookout for common threats such as phishing and social engineering, then arm them with the knowledge on how to deal with exposure of sensitive data. The report also presents some effects of ineffective training which for example the NotPetya cyber-attack in 2017 affected many companies inclusive of Maersk financially and operationally. The attack was able to identify the areas of system updates, network security, and data recovery points as vulnerabilities that are exploitable. Organizations should prevent cyber threats, recommend proper ways of training, and practice good security measures to enhance security and quick recovery from a security breach. It is this report's opinion that minimum security approaches should include awareness in addition to technical in order to protect an organization's assets and credibility.

Table of Contents

Table of figures

1. Introduction

Security policies are high level business rules organizations follow to mitigate risks and safeguard information. They outline “what” and sometimes “who” will handle these tasks. Security standards provide detailed guidelines for implementing policies using technology. A policy on information disposal may give rise to an Information Disposal Standard that describes how different type of media are destroyed. Security Procedures are systematic directions people will follow in the practice of policies (or even standards.) This includes the 'how’ into the business process where an information security control is translated. These really belong to a hierarchy where "standards" and "procedures" would perhaps provide that extra level of detail, sometimes necessary to make a policy enforceable in a variety of departments and technical environments. The organization keeps refining their processes in such a way that they do not look at these with a very clear and sharp unsure vision. The audiences are really made aware through different local offices and in-depth demonstrations from safety training. When organizations develop clear security policies, standards, and practices, they create a strong foundation to anticipate potential threats, meet legal and regulatory requirements, and build trust with stakeholders. Yet, a key aspect often underestimated is the human element. Security Awareness and Training Programs are essential in turning well-crafted policies into real-world practice, ensuring employees are engaged, informed, and prepared to uphold security measures effectively (Lineman, 2023).

1.1 Aim and Objectives

Aim:

This report highlights the importance of security Awareness and Training Programs in organizational security, discussing key approaches, potential issues and solutions.

Objective:

- In order to determine how security awareness and training programs are developed and implemented.
- In order to further explain how such programs can enhance the human factors in organizational security.
- To identify frequent actions, address challenges and recommend solutions for enhancing COPs.
- To assess the success and outcomes of these programs in regards to total security levels.

2. Literature review

Security awareness programs educate employees on cyber security threats, prevention measures and exception to safeguard organizational resources. These programs are designed to ensure that a number of people within an organization are aware of the various threats that are present in the cyber world, including phishing, social engineering and data theft among others, and also provide them with the tools that they require to deal with these threats (West, 2021).

Figure 1 Corporate security training program

Security Awareness Training is a very important factor in the strategy of any organization in preventing cyber incidents. Through training of employees on the need to secure information, the tactics of the hackers and the measures that can be taken to avoid falling victim to the hackers, organizations can greatly lower their risk of being hacked. This all-encompassing guide to Security Awareness Training explores what it is, why it's important, what it entails, and how to effectively implement it (divyaja, 2024).

2.1 The need for training

Phishing: According to the below impact, insufficient security awareness training is tied to major cyber security threats in 2024. In fact, the costs of cybercrime are expected to reach $9.5 trillion USD in 2024, indicating companies are losing massive amounts of money due to a lack of sufficient cyber security practices. A faulty software update by cyber security firm Crowd Strike in July 2024 caused a global IT outage that crashed around 8.5 million Windows systems, causing widespread operational disruptions for businesses. In November 2024, the law firm Thompson Coburn and its client Presbyterian Healthcare Services faced a lawsuit for failing to protect personal health information. This leads to data breaches that damage their reputation (Keepnet, 2024).

Social Engineering: Social engineering is a technique employed by cybercriminals that manipulates people into revealing sensitive or personal information, which can then be used for malicious purposes. Unlike conventional hacking, which typically depends on technical methods to break into security systems, social engineering takes advantage of human psychology and trust to bypass security measures. One reason social engineering is so effective is the widespread lack of awareness and training among both individuals and organizations. Many people don't know how to spot the signs of a social engineering attack, which makes them more vulnerable to deceptive tactics that appear to be legitimate (Security, 2024).

Weak Password Practices: Organizations are aware that their employees can be a cyber-security risk, whether through mistakes, being targeted by attackers, or acting maliciously. Although security and awareness training aims to reduce this risk by fostering a cyber-security-conscious culture, it often has limitations, such as being time-consuming, disrupting productivity, and quickly being forgotten by end users.

Despite ongoing efforts to educate employees, bad habits like password reuse continue to persist. Research shows that many people manage passwords for multiple websites and admit to reusing them. While training on password security is valuable, organizations must go beyond education and implement strong access controls and security measures to enforce better practices and reduce vulnerabilities (White, 2024).

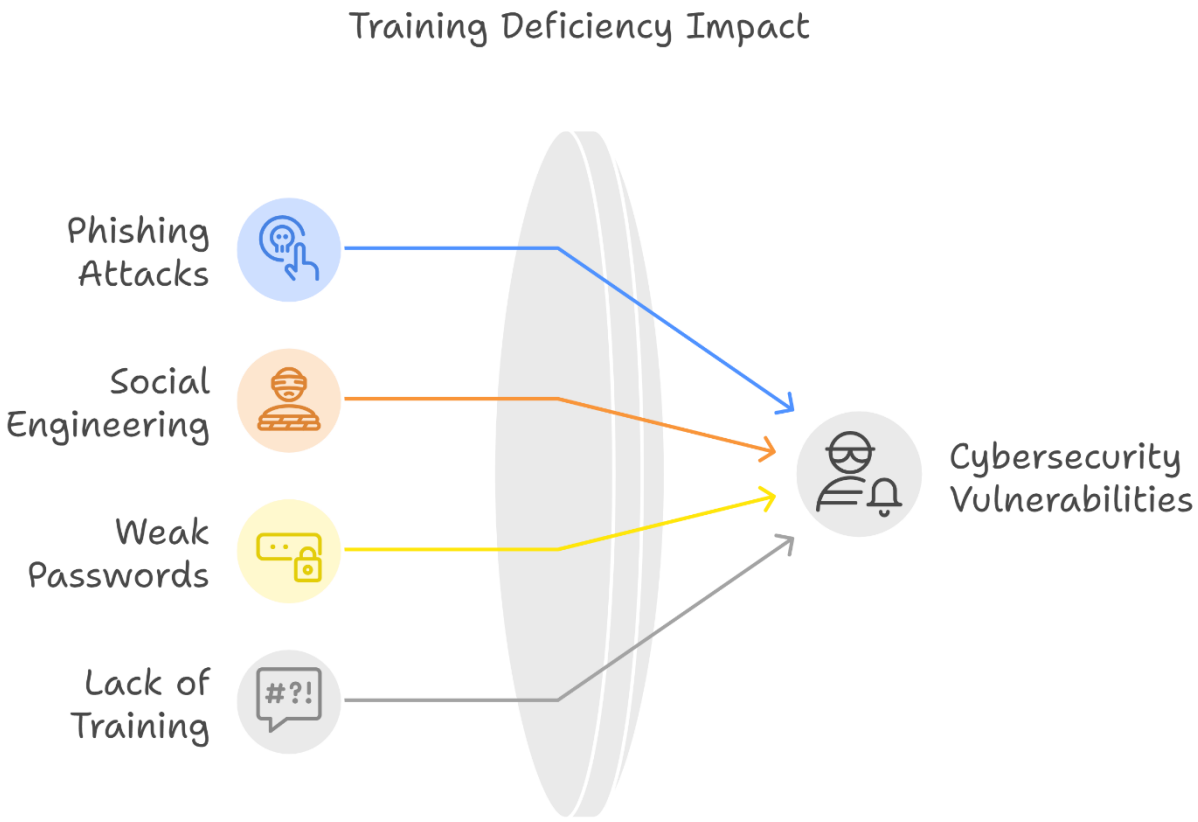


Figure 2 Lack of training

2.2 Types of training

- **Classroom Training:** Instructors can monitor attention, adjust approaches and provide instant feedback. Participants can ask questions and engage in discussions. However, it requires scheduling and may interrupt work routines.
- **Online Training:** Online training provides flexibility and growth options that established face to face sessions don't. Most employees can take online training modules from anywhere and at their own pace. This makes it easier to fit training into their schedules without losing productivity. This method enables businesses to produce identical content with the same outcome at scale while tracking participation and progress through an LMS.
- **Visual Aids and Reminders:** Having visual aids like posters and data visualizations in shared spaces like break rooms or hallways should not be used as the main method for training. They can serve as a great reinforcement for training though. When designed well, these reminders can reinforce cyber security concepts like password hygiene or phishing awareness so that users stay alert to cyber risks during the normal course of work.
- **Simulated Phishing Campaigns:** Phishing simulations provide one of the most powerful trainings, as they offer an opportunity to learn in the real world. Workers are sent fake phishing emails, and those who go for the bait quickly discover the consequences in a safe learning space. The goal of these campaigns is not to punish but to educate. Staff members who fail the test must be automatically put into further specific training to close gaps that may have impacted their understanding and awareness (Rapid7, 2024).

2.2 Effectiveness

- **Protects Sensitive Data:** Data protection is one of the largest needs for awareness training. Hackers usually break into companies to steal customer data, trade secrets and money-related information. Employees must be educated on how to safeguard this information, such as how to use and develop strong passwords, how to detect phishing scams, how to avoid falling for them, and finally how to store and share sensitive information securely. These days protecting anything personal has become crucial because it is important for organizations to comply.
- **Builds a security focused culture:** Developing a culture of security is a key thing to do. It means that security become the priority of everyone in the organization. This is done through security awareness training which educates employees of their roles and responsibilities. This makes them think it shifted from someone else's problem to my problem. As a result, they will be more likely to take action to protect sensitive data and report anything strange.
- **Supports incident response:** During a security incident, a swift and effective response is essential to minimize damage. Security awareness training empowers employees with the necessary knowledge and skills to react promptly and appropriately. By understanding their roles and responsibilities, employees can help contain the situation quickly, reducing both the impact and recovery time. In many cases, this can mean the difference between a manageable issue and a significant crisis.
- **Reduces human error:** Human error, often unintentional, is a primary cause of security breaches, such as clicking phishing links or mishandling sensitive information. However, with the right training, employees are much less likely to make these costly errors. Effective training equips them with the knowledge to recognize potential threats and avoid risky behaviours, ultimately saving the organization from the significant financial losses that often accompany security incidents (Pilot, 2022).

3. Analysis

NotPetya Attack (Case study)

3.1 The Notpetya cyber-attack fo june 2017 and its impact

The NotPetya attacked took place in June 2017 and aimed to disrupt businesses in Ukraine because of the geopolitical struggle between Ukraine and Russia. But its repercussions emerged as global, touching Multinational Business Enterprises such as the A.P. Møller-Maersk, which is the world's biggest shipping conglomerate. The attack froze Maersk operations, which affected the company's shipment booking interfaces and stopped port operations in 17 of the 76 global terminals. This led to an overcrowding of the ports and the workers using whatever tools they could lay hand on such as paperwork and personal email accounts to work. The direct consequences were estimated at running between $250-300m and other disturbances affected the Danish carrier and other companies itself by tens of millions of dollars. The attack cost an estimated $10billon globally which justified it as a terror event that disrupted international trade and transport.

3.2 How the Notpetya cyber-attack unfolded

It started with an update of M.E.Doc which is a popular Ukrainian tax accounting tool. Thieves were able to compromise the software provider's networks after they would get hold of an employee's password and an unpatched server which had not been patched for four years. They loaded backdoors into the update streams which many users, including Maersk, unknowingly downloaded. Once inside the systems, the attackers deployed NotPetya, a malware that combined two powerful tools: EternalBlue and Mimikatz. Unlike earlier exploits like the infamous EternalBlue, which was created by NSA and unfailingly exploited an unaddressed vulnerability of windows operating system to allow remote code execution. Sensitive information like passwords of the system were copied from the system memory by Mimikatz whereby the malware continued to jump from device to device in the network. In less than 10 minutes, Maersk's global IT systems were under attack from NotPetya, having caused the computers to freeze, encrypted data and critical systems to shut down.

3.3 Problems that enabled the Notpetya attack

The attack allowed the identification of the problems in Maersk's cybersecurity arrangement. There was a problem in the update and support of systems since the management failed to ensure appropriate IT provision even when the risks were pointed out by the in-house IT department. Security measures that were deemed fit to be introduced were sidelined since such changes were not related to performance goals of the executives. Lack of network segmentation propagation ensure that the malware can spread through the system and poor planning in data recovery made things worse. Overall, these problems reveal the implications of regards to cybersecurity as operational costs instead of genuine values.

3.4 How to defend against Notpetya

Such measures as proactive work against cyber-attacks could have taken be taken by Maersk include the following. Instead of allowing the malware overtake its global systems, network segmentation would have helped contain the malware impact to certain regions. Further, routine updates and patches of operating systems might have also solved some of the problems that were exploited by EternalBlue, and although patches were released before the attack. Like many other firms, Maersk also had unsafe systems that it still used, including Windows 2000, which lack proper security attributes found in more advanced operating systems. Moreover, the lack of an adequately defined data recovery plan was noted: all domain controllers were in sync; thus, there was only one backup. A stronger and well distributed recovery protocol could have helped in fast recovery process and thereby less down time (Steinberg, 2021).

Figure 3 NotPetya

4. Conclusion

Therefore, security awareness, and training programs are crucial in enhancing an organization's cyber security posture particularly in controlling the risks occasioned by human failures and cyber incidences. As NotPetya revealed the inefficiency of information protection rules, obsolete technologies, and employees' unawareness can lead to essential material losses and stopped business processes. Peering into Maersk Incident it was found out that there were issues with system maintenance, patching, network segmentation and planning for data recovery. The above gaps can however be closed by well executed security awareness programs that teach the employees about security, improve on the password usage and train the employees on how to handle phishing and social engineering scams. Besides, many of such programs create an organizational security culture where each employee acts responsibly for securing any sensitive data. If more organizations want to avoid similar mishaps, they need to regularly train their employees, ensure they are aware of changes to the system, incorporate strong forms of network segmentation, and create concrete recovery mechanisms. Finally, convection with security awareness training and technical controls to a minimum level in an organization will decrease the chances of cybercrime and protect the organization's stakeholders.

5. References

divyaja, 2024. *Phish Grid.* [Online]
Available at: https://phishgrid.com/blog/security-awareness-training/#:~:text=Security%20Awareness%20Training%20is%20a,and%20best%20practices%20for%20implementation.
[Accessed 1 December 2024].

Keepnet, 2024. *KeepNet.* [Online]
Available at: https://keepnetlabs.com/blog/2024-security-awareness-training-statistics
[Accessed 1 December 2024].

Lineman, D., 2023. *InformationShield.* [Online]
Available at: https://informationshield.com/2023/10/27/security-policies-standard-and-procedures-whats-the-difference/
[Accessed 29 November 2024].

Pilot, C., 2022. *CyberPilot.* [Online]
Available at: https://www.cyberpilot.io/cyberpilot-blog/7-benefits-of-security-awareness-training
[Accessed 2 December 2024].

Rapid7, 2024. *Rapid7.* [Online]
Available at: https://www.rapid7.com/fundamentals/security-awareness-training/
[Accessed 2 December 2024].

Security, S., 2024. *Samurai Security.* [Online]
Available at: https://samuraisecurity.co.uk/resources/news/why-social-engineering-is-effective/
[Accessed 1 December 2024].

West, J. O., 2021. Human error: The weakest link in cybersecurity. *Journal of Cyber Security Awareness,* 12(3), pp. 45-60.

White, M., 2024. *Specops.* [Online]
Available at: https://specopssoft.com/blog/security-awareness-training-passwords/
[Accessed 1 December 2024].