

**USE COMPUTER TECHNOLOGY TO RESEARCH A COMPUTER TOPIC**

Cyber Security



July 3, 2024

HCL TEch

59 Sunninghill, Sandton

**Members**

* Mzwakhe Hamnca 9801285595080
* Rethabile Kondowe 9611150486089
* Neo Khambule
* Avile Bantwini

**Unit Standard Number:** 114079

# **Topic: Evaluating Utilization of Cyber-security in the corporate world**

Table of Content

[**Topic: Evaluating Utilization of Cyber-security in the corporate world** 0](#_Toc170926769)

[**Evaluating Utilization of Cyber-security in the corporate world** 2](#_Toc170926770)

[**Relevance of the Topic** 2](#_Toc170926771)

[**Key Challenges** 2](#_Toc170926772)

[**Background of Cyber Security** 3](#_Toc170926773)

[**Conduct of Security Audit and identification of Vulnerabilities** 3](#_Toc170926774)

[**Implementation and Security Measures for Desktops and Multi User- systems** 3](#_Toc170926775)

[**Monitoring of Network Traffic for Suspicious activity** 3](#_Toc170926776)

[**Development of a response plan for potential data breaches** 4](#_Toc170926777)

[**Educating Staff on Best Practices for Data Security** 4](#_Toc170926778)

[References 5](#_Toc170926779)

Scenario no 5: Cyber-security

# **Evaluating Utilization of Cyber-security in the corporate world**

This research topic focuses on threats, vulnerabilities, data breaches and response plans implemented in the corporate world. It aims to assist the corporate to be more aware of these threats and vulnerabilities and impose ways on how to mitigate them in an efficient way, while taking into consideration the company policies and rights. This research will ensure that corporate employee and administrators are well aware of internal and external threats while providing awareness to the teams.

### **Relevance of the Topic**

The aim of this research is to identify threats and vulnerabilities that are experience d in the corporate world. In that way, it will assist us to gain more practical knowledge of the threats, vulnerabilities, security measures that must be taken into considerations to eradicate all the above mentioned threats. This aligns with the learning objective of understanding cyber-security measures, incident response, data protection, and employee training.

### **Key Challenges**

* Finding relevant literature reviews that evaluate vulnerabilities and conducting security audits.
* Finding the right tools to monitor the network and also taking into considerations finding the right literature.
* Finding effective response plans that were utilized by past researchers.
* Developing best practices of educating staff on best practices for data security.

## **Background of Cyber Security**

Computer Security is sometimes known as the protection of computer systems and networks from theft, damage, disruption, or unauthorized access. It encompasses a variety of practices, technologies, and policies aimed at safeguarding data and ensuring the integrity, confidentiality, and availability of information. The evolution of computer security began with the early mainframes, where physical security was the main concern. Today it is the critical aspect of organizational strategy, driven by the need to protect sensitive data and maintain trust. According to a report by the National Institute of Standards and technology, effective cyber-security practices involve continuous risk management, regular updates, and employee training (NIST, 2018).

## **Conduct of Security Audit and identification of Vulnerabilities**

Security audits are systematic evaluations of an organization’s information systems to assess the effectiveness of security measures and identify vulnerabilities. These audits involve reviewing policies, procedures and technical controls. The most common methods include vulnerability scanning, penetration testing, and compliance checks against established security standards. Vulnerability scanners like Nessus identify known weaknesses, while penetration tests simulate cyber-attacks to discover exploitable flaws. The goal is to pinpoint areas of risk and recommend improvements to enhance security posture. According to a study by SANS institute =, regular security audits are vital for detecting potential threats and mitigating risks before they can be exploited (SANS, 2021).

## **Implementation and Security Measures for Desktops and Multi User- systems**

Implementing security measures for desktops and multi-user systems involves deploying various technologies and practices to protect against unauthorized access and threats. For desktops, this includes installing antivirus software, enabling firewalls, applying regular software updates, and enforcing strong passwords policies. Multi-user systems require additional controls like user access management, role based access control (RBAC), and regular monitoring of user activities. Encryption of data at rest and in transit is also crucial. According to a research paper by IEE, effective implementation of these measures significantly reduces the risk of data breaches and enhances overall system security (Chauhan, 2019).

## **Monitoring of Network Traffic for Suspicious activity**

Network traffic monitoring is the process of observing and analyzing network data to detect unusual or suspicious activities that could indicate a security threat. Tools like intrusion prevention system and Intrusion Detection are commonly used for this purpose. These tools analyze network packets in real time, looking for patterns that match known attack signatures or anomalies that deviate from normal behavior. By continuous monitoring traffic, organizations can quickly identify and respond to potential threats, thereby minimizing the impact of cyber incidents. A case study of Cyber-security and Infrastructure Security Agency (CISA) emphasizes the importance of network traffic monitoring in maintaining robust cyber-security defenses ( Bonaccorsi, 2021).

## **Development of a response plan for potential data breaches**

A response plan for data breaches outlines the steps an organization should take in the event of security incident to minimize damage and facilitate recovery (CISA, 2022). This plan typically includes procedures for detecting and analyzing breaches, containing the incident, eradicating the threat, and restoring affected systems. This also involves communicating strategies for informing stakeholders and regulatory bodies. Regular drills and updates to the plan ensure preparedness. According to the international journal of Information Management, having a well-defined and tested response plan is crucial for minimizing the financial and reputational impact of data breaches (Collange, 2020).

## **Educating Staff on Best Practices for Data Security**

Educating staff on best practices for data security is essential for creating a culture of security awareness within an organization (IJIM, 2021). Training programs should cover topics like recognizing phishing attempts, using strong passwords, safely handling sensitive information, and understanding the importance of regular software updates. Regular refresher courses and simulated phishing exercises can reinforce learning. According to a report by Gartner, organizations that invest in comprehensive security training for employees see a significant reduction in security incidents caused by human error (Alassafi, 2021). Effective training empowers employees to act as the first line of defense against cyber threats.

# References

 Bonaccorsi, A. C. (2021). SSH researchers make an impact differently. Looking at public research from the perspective of users. ,. *Research Evaluation*.

 Nearing, G. S. (2020). Does Information Theory Provide a New Paradigm for Earth Science? . *Hypothesis Testing.*

Alassafi, M. O. (2021). Success indicators for an efficient utilization of cloud computing in healthcare organizations: Saudi healthcare as case study. . *Computer Methods and Programs in Biomedicine*.

Chauhan, A. (2019). Intrusion Detection in Cloud Computing Environments using Deep Learning Algorithms. . *Turkish Journal of Computer and Mathematics Education* .

CISA. (2022). Importance of Network Traffic.

Collange, J. &. (2020). Using virtual reality to induce gratitude through virtual social interaction. . *Computers in Human Behavior,*.

Gartner. (2020). Comprehensive Security Training .

IEEE. (2020). Implementation Of Security Measures .

IJIM. (2021). Journal of Infromation Management.

Khoufi, E. (2021). The phenomenon of data loss and cyber security issues in Ghana. *Forsight*.

NIST. (2018). Cybersecurity Practices .

SANS. (2021). Security Audits .