Recommendations on Cyber Security

Harpreet Singh

Computer Engineering Technology - Computing Science

Algonquin College

January 22nd, 2024

ENL2019T 309

# Summary

The problem this report examines is the need for stronger cybersecurity measures.

This study explores cybersecurity solutions to protect digital systems and data.

The criteria the solution is tested against are effectiveness, cost, and ease of implementation.

The recommendation is to adopt comprehensive cybersecurity strategies.

Table of Contents

[Summary ii](#_Toc92203041)

[List of Figures iv](#_Toc92203042)

[List of Tables v](#_Toc92203043)

[1.0 Introduction 1](#_Toc92203044)

[2.0 Problem Statement 2](#_Toc92203045)

[2.1 Background - Problem: Increasing Cyber Threats 2](#_Toc92203046)

[2.2 Theory - Solution: Multi-Layered Cybersecurity Framework 2](#_Toc92203047)

[3.0 Criteria 3](#_Toc92203048)

[3.1 Maintenance 3](#_Toc92203049)

[3.2 Cost 3](#_Toc92203050)

[3.3 Performance 3](#_Toc92203051)

[4.0 Results and Discussion (Criteria vs. Solution) 4](#_Toc92203052)

[4.1 Faster Data Transfer 4](#_Toc92203053)

[4.2 Improved System Responsiveness 4](#_Toc92203054)

[4.3 Higher Durability and Energy Efficiency 4](#_Toc92203055)

[5.0 Conclusion 5](#_Toc92203056)

[6.0 Recommendation 6](#_Toc92203057)

[References 7](#_Toc92203058)

# List of Figures

[Figure 1: Meta Quest 3 [1] 2](#_Toc192326898)

[Figure 2: Meta Quest 3 with super-fast charging [2] 4](#_Toc192326899)

[Figure 3: Meta Quest 3 with affordable cost [3] 5](#_Toc192326900)

[Figure 4: Meta Quest 3 with high visual quality [4] 5](#_Toc192326901)

# List of Tables

[Table 1: Meta Quest 3 Recommendation Criteria 6](#_Toc192327177)

# 1.0 Introduction

The objective of this report is to provide a recommendation on cybersecurity solutions.  
The intended audience for this report includes technicians and professionals in the field of information security and technology. This report examines the issue of increasing cyber threats and the need for robust security measures. The proposed solution is the implementation of cybersecurity strategies, including encryption, firewalls, and threat detection systems, to protect sensitive data and systems.  
Chapter 2.0 of this report discusses the problem in detail and presents the proposed solution. Chapter 3.0 outlines the evaluation criteria used to assess cybersecurity measures.

# 2.0 Problem Statement

## 2.1 Background - Problem: Increasing Cyber Threats

Cyber-attacks have grown in sophistication and frequency as technology has advanced rapidly. Cyberattacks, such as malware, phishing, and data leaks, are serious threats to individuals, businesses, and governments. The rising reliance on digital infrastructure necessitates the implementation of robust security measures. Furthermore, cybersecurity threats are continually evolving, necessitating ongoing upgrades and changes to security processes to protect critical information.

## 2.2 Theory - Solution: Multi-Layered Cybersecurity Framework

A multi-layered approach protects against cyber attacks by combining multiple security mechanisms such as firewalls, intrusion detection systems, encryption, multi-factor authentication, and regular security audits. The solution must be cost-effective, scalable, and responsive to new security problems while providing adequate protection for digital assets.

# 3.0 Criteria

## 3.1 Maintenance

The cybersecurity framework should require minimal maintenance while ensuring continuous protection. Regular updates and security patches should be automated to reduce manual intervention, and system monitoring should be efficient to detect and respond to threats promptly.

## 3.2 Cost

## 3.3 Performance

# 4.0 Results and Discussion (Criteria vs. Solution)

## 4.1 Faster Data Transfer

The goal is to ensure that cybersecurity measures do not slow down data transfer speeds while protecting sensitive information.  
Data transfer performance is sourced from Cisco’s cybersecurity research, which provides insights into network security optimization.  
According to Cisco, modern encryption protocols and optimized firewall configurations allow for secure data transmission without significant latency [1].  
This passes the criterion for faster data transfer.

The multi-layered cybersecurity framework includes advanced encryption and optimized data routing to maintain high-speed data transfer (see Figure 1).

## 4.2 Improved System Responsiveness

The goal is to implement cybersecurity measures that do not hinder system performance or responsiveness.  
System responsiveness data is sourced from IBM Security, which evaluates the impact of security measures on computing performance.  
IBM Security reports that AI-powered threat detection and cloud-based security solutions enhance protection while minimizing delays in system operations [2].  
This passes the criterion for improved system responsiveness.

The cybersecurity framework ensures real-time threat detection with minimal impact on system speed (see Figure 2).

## 4.3 Higher Durability and Energy Efficiency

The goal is to implement a cybersecurity framework that is both long-lasting and energy-efficient.  
Durability and energy efficiency data are sourced from Microsoft Security, which highlights sustainable cybersecurity practices.  
Microsoft Security states that cloud-based security solutions and lightweight endpoint protection reduce power consumption while maintaining strong security [3].  
This passes the criterion for higher durability and energy efficiency.

The multi-layered cybersecurity framework ensures long-term protection with minimal energy consumption (see Figure 3).

*Figure 3: Energy-efficient cybersecurity infrastructure [3]*

# 5.0 Conclusion

Faster data transfer, improved system responsiveness, and higher durability & energy efficiency are the three main criteria for evaluating the multi-layered cybersecurity framework. These criteria demonstrate that the framework meets all security and performance requirements. The solution ensures secure and fast data transfer through advanced encryption without compromising network speed. Additionally, AI-driven threat detection enhances system responsiveness, maintaining seamless operations. The framework is also designed with energy-efficient security solutions, ensuring long-term durability while minimizing resource consumption. Because of these advantages, the multi-layered cybersecurity framework is an appropriate and cost-effective option for safeguarding digital assets from cyber threats. This research encourages the use of this architecture as a dependable and effective security solution for enterprises and individuals.

All criteria for the Cyber Security were passed (See Table 1).

Table 1: Cyber Security Recommendation Criteria

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Pass** | **Fail** |
| Battery life and charging | x |  |
| Cost | x |  |
| Display & Visual Quality | x |  |

# 6.0 Recommendation

Due to the faster data transfer, improved system responsiveness, and higher durability & energy efficiency provided, the multi-layered cybersecurity framework is recommended.

# References