Page | 1

Recommendations on Cyber Security

Harpreet Singh

Computer Engineering Technology - Computing Science

Algonquin College

January 26th, 2024

ENL2019T 309

Page | 2

# Introduction

The purpose of this report is to examine cybersecurity and propose solutions to mitigate emerging digital threats. The audience for this report is IT professionals and security experts. This report discusses the issues raised by cyberattacks, such as data breaches, ransomware, and malware threats. The solution is to create advanced security systems that incorporate AI, machine learning, and encryption technologies. Chapter 2.0 of this report provides an overview of cybersecurity challenges and proposed solutions. Chapter 3.0 discusses the evaluation criteria for successful cybersecurity systems.

Page | 3

# 2.0 Problem Statement

2.1 Background: Problem – Increasing cyber threats

As digital transformation gains momentum, businesses are confronted with growing cyber threats that threaten confidential data and business continuity. Ransomware, zero-day vulnerabilities, and phishing assaults are frequent problems. Since human mistakes, inadequate encryption, and out-of-date software frequently cause current cybersecurity systems to fail, strong and flexible security measures are necessary to effectively counter these threats.

2.2 Theory: Solution – Multi-layered cybersecurity framework

This framework includes firewalls, intrusion detection and prevention systems, and endpoint protection to defend against unauthorized access. Regular vulnerability assessments and network segmentation will enhance the defense-in-depth approach, ensuring that even if one layer is breached, others will mitigate potential damage.

Page | 4

# 3.0 Criteria

3.1 Maintenance

Regular maintenance is necessary to keep cybersecurity systems current with the most recent threat classifications and updates. Every piece of hardware and software needs to be free of errors, flaws, and vulnerabilities. Maintaining strong security procedures requires routine audits and penetration tests.

3.2 Cost

Cybersecurity solutions should be cost-effective. A single free-of-cost security assessment or update service should be provided as part of the package.

3.3 Performance & protection Quality

Cybersecurity systems should provide advanced protection against a wide range of threats, including malware, ransomware, and phishing attacks. They need to make use of advanced technology, like real-time monitoring and AI-driven threat detection, to guarantee improved performance. High encryption standards should be supported by systems in order to protect sensitive information and guarantee a safe and dependable environment.

.