|  |  |
| --- | --- |
| A picture of a winding road and trees  Problem Statement | Solomon Morongwa Moshokoa: ST10229897  Bornwise Nkateko Baloyi: ST10105509  Roandiswa Mbedzi: ST10064879  Mokgadi Mamabolo: ST10204666  WORK INTEGRATED LEARNING  Group 3  DMT2 |

**Table of content**

**Problem Statement and Recovery Plan**

* Project Overview
* Problem Identification
* Strengths
* Weaknesses
* Opportunities
* Threats
* Recovery Plan (SOP)
* Lack of Seamless Network Integration
* Inefficient Printing Infrastructure
* Conclusion and SWAT Analysis

**Wireless Connectivity**

* Installation of Wireless Access Points
* Challenges
* Large Number of Connected Users
* Simultaneous Transfer of Large Files and Data

**Network Monitoring**

* Use of Technologies for Network Monitoring
* Challenges
* Connection Issues
* Compatibility for Older Devices

**Internet Connectivity**

* Offering Dependable, High-Bandwidth Internet Access
* Challenges
* Rejection of Certain Sites
* Disturbance and Corruption

**Data Backup**

* Implementing Data Backup and Recovery Procedures
* Challenges
* Password Forgetting
* Automatic Backup Crushing

**Network Policy**

* Establishing and Implementing Network Usage Rules and Regulations

**Cost-effectiveness**

* Designing the Network with Long-term Sustainability
* Challenges
* Frequent System Updates
* Regular Expenses

**Integration**

* Guaranteeing Interoperability with Current and Future Technologies
* Challenges
* Time-Consuming Installation
* Specific Hardware and Software Requirements

**Risk Identification**

* Elements of Cybersecurity Risk Management
* Identifying Sources, Events, and Situations
* Identifying Assets at Risk

**Risk Analysis**

* Estimating Likelihood and Impact
* Qualitative or Quantitative Methods
* Reviewing Existing Controls and Vulnerabilities

**Problem Statement and Recovery Plan for Enhanced Network Infrastructure**

The project strives to ensure seamless and secure network access for our 100 active users across the college's three main buildings, each with distinct requirements and a lobby area needing wireless network access spanning 200 square feet. The primary goals encompass providing secure wireless and wired access to authorized personnel, internet sharing from the main building's high-speed cable connection, and reliable connectivity for all 100 users equipped with computer devices. However, the challenge arises from integrating three high-speed printers into each building's network infrastructure (Statham, 2019).

**Problem Identification:**

**Strengths (S):** The current network infrastructure ensures basic connectivity, allowing access to the internet and limited inter-building connectivity (Statham, 2019).

**Weaknesses (W):** The existing system lacks robust security protocols, struggles with inter-building connectivity, and cannot support the integration of high-speed printers without disruptions (Statham, 2019).

**Opportunities (O):** The potential for enhancing network security, facilitating seamless inter-building connectivity, and incorporating advanced printing capabilities to support academic and administrative needs (Statham, 2019).

**Threats (T):** The risks of potential network conflicts during installation and compatibility issues between software and devices, hindering seamless implementation and user experience (Statham, 2019).

**Recovery Plan (SOP):**

**Problem: Lack of Seamless Network Integration** **Side-effects:** Current limitations in security protocols and inter-building connectivity could lead to data breaches and inefficiencies. **Solution:** Implement a systematic network assessment to pre-empt conflicts, rigorously test the network functionality, and execute regular updates and patches to ensure software and device compatibility (Statham, 2019).

**Problem: Inefficient Printing Infrastructure** **Side-effects:** Incompatibility issues between printers and the network could disrupt printing services across the buildings (Statham, 2019).

**Solution:** Devise a comprehensive installation and configuration plan, allowing IT technicians to seamlessly integrate printers, conduct thorough testing, and provide necessary training sessions for end-users on printer operations and network usage (Statham, 2019).

**Conclusion and SWAT Analysis:** The project aims to fortify network accessibility, security, and efficiency across college buildings. Threats include potential conflicts during installation and compatibility issues. To counter these, a detailed SOP encompasses pre-deployment network assessments, rigorous testing, regular updates, and comprehensive training sessions. By addressing weaknesses, leveraging opportunities, and proactively mitigating threats, the project aims to revolutionize network functionality, delivering seamless and secure connectivity for our college community within the specified timeframe and budget (Statham, 2019).

**wireless Connectivity**: Install a reliable network of wireless access points with smooth roaming in every building. The challenges will be if the user is connected in large number, transferring of large files and data at the same time due to the connectivity (Smith, 2022).

**Network Monitoring**: Use technologies for network monitoring to quickly detect and fix problems. The challenged will be the connection and for user who will be using old devices they will be forced (Smith, 2022)

**Internet connectivity**: Offer dependable, high-bandwidth internet access. There are some sites that the system will reject and might block, disturb the corrupt (Smith, 2022).

**Data Backup**: To protect important data, put data backup and recovery procedures in place. overall campus. If the user forgets the password. Automatically the backup will crush (Smith, 2022).

**Network Policy**: Establish and implement rules and regulations for network usage.

**Cost-effectiveness**: When designing the network, keep long-term sustainability and economical options in mind. The system needs a frequently update. Which is not expensive but its regularly (Smith, 2022).

**Integration**: Guarantee interoperability with both current and upcoming technological advancements. Using the best and newly system. It takes long time to install and it need specific (hardware and software) which are not easy to find. Making maintain to take time (Smith, 2022).

**Risk identification**

The first element of a cybersecurity risk management framework is risk identification. 58 It is the process of identifying sources, events, and situations that could harm your network, such as hackers, malware, natural disasters, human error, or device failure. You should also identify assets at risk, such as data, devices, systems or services, and their value to your organization. Risk identification helps you establish scope and context for managing your cyber security risks (Tyson, 2019).

**Risk analysis**

The second element of the cybersecurity risk management framework is risk analysis. This is the process of estimating the likelihood and impact of each risk identified on your network. You can use qualitative or quantitative methods or a combination of both to assess the likelihood and severity of risks. 59 You should also review existing controls and vulnerabilities that impact your cybersecurity. Risk analysis helps you prioritize risks and determine the level of risk you are willing to accept (Tyson, 2019).

**Risk handling**

The third element of the cybersecurity risk management framework is risk treatment and this is the process of selecting and implementing appropriate measures to address the risks you have analyses. There are four main strategies you can choose to address risk: avoid, reduce, transfer, or accept (Tyson, 2019). Avoiding risk means eliminating the source or activity that causes the risk. Risk reduction means implementing control or mitigation measures to reduce the likelihood or impact of a risk. Transferring risk means transferring responsibility or costs to another party, such as an insurance company or seller (Tyson, 2019).Accepting risk means recognizing and accepting it, either because it is too low or because handling it is too costly. Addressing risk helps you balance the costs and benefits of cybersecurity (Tyson, 2019).

# References List

Smith, J. (2022, September 22). *Chegg*. Retrieved from Chegg.com: http://www.chegg.com

Statham, J. (2019, October 21). *JSTOR* . Retrieved from jstor.org: http://www.jstor.org

Tyson, B. (2019, June 26). *ResearchGate*. Retrieved from researchgate.net: http://researchgate.net