A white and gold logo

Description automatically generated

**Company Network Report Part 2**

**Prepared by: Team 3**

Brianna Baird, Christina Canady, Arianna DeNardo, Luke Jarrell, Kelsey Cox

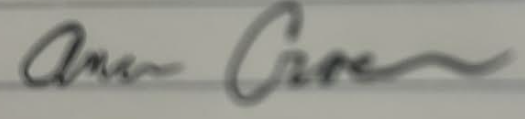
I \_\_\_\_\_\_\_\_\_\_\_\_ received this report and the findings have been discussed with me. This report can be shared with professor and students at ECU, but not posted online publicly without identifying details redacted.

Table of Contents

[Introduction 2](#_Toc1627906863)

[Project Scope 3](#_Toc1454121927)

[Company Overview 3](#_Toc1415904504)

[Company IT Governance 3](#_Toc602670456)

[Current Network 3](#_Toc1840717487)

[Current Physical Network Structure 4](#_Toc2086577226)

[Current Logical Network Structure 4](#_Toc1027651314)

[Enterprise Architecture 4](#_Toc919132804)

[Needs Assessment (completed by Christina Canady) 5](#_Toc982013177)

[Risk Assessment (completed by Arianna DeNardo) 5](#_Toc493275880)

[Threat Scenarios 5](#_Toc370457849)

[Risk 1: Theft of Customer Financial Data 6](#_Toc951203622)

[Risk 2: Theft of Employee devices (computers, phones, etc...) 7](#_Toc1102992360)

[Risk 3: Internet Access 8](#_Toc271321653)

[Risk 4: Natural Disaster 10](#_Toc487891733)

[Risk 5: Physical Location/Security Monitoring Tools 11](#_Toc126604462)

[Risk 6: Transaction Processing System 13](#_Toc726080867)

[Gap Analysis (completed by Christina Canady) 14](#_Toc1865830982)

[Gap Analysis Form: Network Security (completed by Christina Canady) 15](#_Toc1684528236)

[Gap Analysis Form: Employee Training (completed by Christina Canady) 16](#_Toc1371672513)

[Recommendations (completed by Arianna DeNardo) 17](#_Toc1633348718)

[Revised Physical Network Structure (completed by Kelsey Cox) 18](#_Toc1088071982)

[Revised Logical Network Structure (completed by Christina Canady) 18](#_Toc561592070)

[Migration Plan (completed by Brianna Baird) 18](#_Toc1233634449)

[Detailed Budget (completed by Christina Canady) 19](#_Toc121634783)

[Disaster Recovery Plan (completed by Christina Canady) 20](#_Toc873553277)

[Cybersecurity Plan (completed by Luke Jarrell) 21](#_Toc706783414)

[Conclusion (completed by Kelsey Cox) 21](#_Toc152409196)

[Appendix A – IT Governance Diagram (completed by Arianna DeNardo) 22](#_Toc932425417)

[Appendix B - Enterprise Architecture Diagram (completed by Brianna Baird) 22](#_Toc1561340214)

[Appendix C - Revised Logical Diagram (completed by Christina Canady) 23](#_Toc2017556878)

[Appendix D - Revised Physical Network Diagram (completed by Kelsey Cox) 24](#_Toc1220485866)

[Appendix E – SWOT Analysis (completed by Christina Canady) 25](#_Toc284128124)

[Appendix F – Migration Plan Timeline (completed by Brianna Baird) 26](#_Toc1178417802)

[Appendix G – Current Physical Network Diagram (completed by Kelsey Cox) 27](#_Toc1025595787)

[Appendix F – Current Logical Network Diagram (completed by Christina Canady) 28](#_Toc2015089201)

# Introduction

The salon industry is built around providing clients with exceptional service. Exceptional service includes more than just a great hairstyle; the salon must be a secure and pleasing environment for the clients. As technology has evolved, so have client needs. Clients must trust that the salon will ensure their safety and the safety of their data. Salons conduct most transactions electronically. This data must be communicated over a network. Data protection is essential to maintain the trust of clients and the law. Networks should be assessed regularly to ensure that sensitive data is transmitted securely.

Described below is the current state of Tanglez network as well as the next steps of the network analysis.

# Project Scope

The goal of this project is to examine and analyze the current network and suggest improvements for better performance of the network. It will encompass the entire salon and all devices connected to the network within it. We will also make a security assessment and suggest improvements on how to better secure the company’s data as well as its customers.

# Company Overview

Tanglez Salon is a small family-owned and run hair salon in Wilmington, NC. Tanglez opened in 2008 and has won multiple awards since then, including Best Salon and Best Stylist. Tanglez has 3 desktop PC’s as well as security cameras and a laptop that are all part of their network. Stylists and guests also log into the network throughout the day with their mobile devices. I worked there for many years and am related to the owners, so communicating with them will not be difficult.

# Company IT Governance

See Appendix A for IT Governance Diagram

Tanglez Hair Salon is a small business that is made up of three desktop computers, a router and modem with WIFI, as such there is no specific role at Tanglez Hair Salon that is solely responsible for IT. The leadership and IT governance of Tanglez Hair Salon and Spa includes Donnie Canady, the owner, Jenny Rojas as manager/stylist, and Amanda Crocker as office manager. Jenny Rojas and Amanda Crocker are tasked with identifying and troubleshooting any minor IT issues. Donnie Canady’s approval is required for all decisions requiring funding or impacting the status quo of the system. Any large projects or problems are contracted out to companies with expertise in the specific area of need.

# Current Network

## Current Physical Network Structure

[Refer to Appendix D for Current Physical Network Diagram](#_Appendix_G_–)

The salon layout is designed to facilitate efficient client service and administrative tasks. The placement of the modem and router in the office area ensures a stable internet connection throughout the salon. Laptops at workstations offer flexibility and mobility for stylists or staff to access necessary information while attending to clients. The desktop PC connected to the Square card reader provides a dedicated point for processing payments, ensuring smooth transactions for clients. This layout provides a functional and organized environment for running salon operations while incorporating necessary networking equipment and devices for connectivity and efficiency.

## Current Logical Network Structure

[Refer to Appendix F for Current Logical Network Diagram](#_Appendix_F_–_1)

Tanglez Salon is a small business that operates much like a home network. Their internet provider is Spectrum which provides them with a Spectrum modem. The modem operates on the datalink layer which brings information from the internet to the network. The modem is then connected to a router that is the central connection point for all of Tanglez network connected devices. This includes 3 desktops, two laptops, a tablet and any guest or employee smartphone that connects to the network. The router operates at layer 3 of the OSI model. The router is responsible for distributing the information to the connected devices. All the network devices are connected via the router’s WAP (wireless access point). There are no hardwired devices currently.

# Enterprise Architecture

[Refer to Appendix for Enterprise Architecture Diagram](#_Appendix_B_-)

Tanglez Salon's enterprise architecture is described below as the connection between the enterprise campus, the enterprise edge, and the ISP. To view the enterprise architecture diagram, please refer to Appendix B.

The business is connected to the local access network for the enterprise campus. The enterprise campus includes building access and building distribution. The building access includes three wireless desktop PCs, 3 laptops, a tablet, security cameras, and guest devices. The building distribution connects the wireless devices, security cameras, guest devices, and Square Payment Solutions card reader to the internet. A single router distributes Wi-Fi throughout the building. The router connects to the modem on the enterprise edge, which then connects to the internet, which resides on the service provider edge.  Spectrum provides internet services for the network.

The enterprise architecture is listed below.

* Enterprise Campus
* Building Access (LAN)
* Building Distribution(Wi-Fi)
* Telephone Access
* Enterprise Edge
* Internet Connectivity
* Service Provider Edge
* Spectrum

# Needs Assessment (completed by Christina Canady)

[Refer to Appendix D for Revised Physical Network Diagram](#_Appendix_D_-)

After working closely with the Tanglez IT governance team and gathering all necessary information, we narrowed our list down to three main areas that need improvement. These areas include training employees on basic security principles, purchase and utilize firewall security, improving WAP placement, and utilizing Carbonite services for Disaster Recovery.  As you can see from our physical diagram, the WAP is in the back of the salon, effectively giving the best signal to parts of the salon that clients and stylists are not located. If we moved this to a more central location the connectivity would be better for guests and employees alike. This proposal to enhance network connectivity will ideally improve performance in the company’s system software, and therefore improve the employees’ and end users' efficiency. Additionally, Tanglez is a small business, but it would cost little to nothing to train the relevant employees on basic security principles. Employee training and knowledge is the first defense against social engineered cybersecurity attacks. In order to enhance the overall network security, it is suggested Tanglez invest in a firewall such as SonicWall or Cisco FirePower. Firewalls provide protection against hackers, allow the company to block unapproved websites, and strengthen the overall security posture of the organization.  Carbonite is a cloud-based backup solution that provides unlimited data backup services. This service could be invaluable in the event of a natural disaster to get the business back operational as soon as possible.

# Risk Assessment (completed by Arianna DeNardo)

These risk scenarios were identified:

* Customer financial data
* Employee devices (computers, mobile phones, etc.)
* Internet access
* Natural Disaster
* Physical location/ Security monitoring tools
* Transaction Processing System

## Threat Scenarios

### Risk 1: Theft of Customer Financial Data

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Customer financial data and records | |
| Asset Importance | | Critical | |
| Threat | | Unauthorized access to customer data through data breaches, hacking, insider threats and malware attacks | |
| Description | | Unauthorized users access confidential data | |
| Likelihood | | High (2) | |
| Impact on | | \_X\_ Confidentiality  \_X\_ Integrity  \_X\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | High (3) | High (3) | 9 |
| Reputation | High (3) | High (3) | 9 |
| Productivity | Medium (2) | Medium (2) | 4 |
| Legal | High (3) | High (3) | 9 |
|  | | Impact Score | 31 |
| Risk Score (Likelihood x Impact Score) | | 62 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_ Accept  X Mitigate  \_\_ Share  \_\_ Defer | |
| Risk Mitigation Controls | |  | |
| Access Controls | | Create access control | |
| Update encryption protocol | | Implement strong encryption protocols. | |

### Risk 2: Theft of Employee devices (computers, phones, etc...)

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Employee devices | |
| Asset Importance | | High | |
| Threat | | Theft, loss, malware, and phishing attacks | |
| Description | | Unauthorized access to company data, customer data, compromised network security and loss of productivity due to loss of device | |
| Likelihood | | Medium (2) | |
| Impact on | | \_X\_ Confidentiality  \_X\_ Integrity  \_\_\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | High (2) | Medium (2) | 4 |
| Reputation | High (2) | High (2) | 4 |
| Productivity | Low (3) | Low (3) | 9 |
| Legal | High (2) | High (2) | 4 |
|  | | Impact Score | Sum 21 |
| Risk Score (Likelihood x Impact Score) | | 42 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_\_Accept  \_X\_Mitigate  \_\_\_Share  \_\_\_Defer | |
| Risk Mitigation Controls | |  | |
| Updated software and security | | Regularly update software, enforce strong password policies | |
| Training | | Train employees on recognizing phishing attacks | |
| Security monitoring | | Cameras in the building can help stop physical loss of items | |

### Risk 3: Internet Access

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Servers, Organizational Data, Software | |
| Asset Importance | | High | |
| Threat | | Malware, phishing attacks, denial-of-service (DoS) attacks. | |
| Description | | Manipulation of internet traffic, potentially stealing sensitive information or injecting malicious content. | |
| Likelihood | | High (3) | |
| Impact on | | \_X\_ Confidentiality  \_X\_ Integrity  \_X\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | Medium (2) | High (3) | 6 |
| Reputation | Medium (2) | High (3) | 6 |
| Productivity | Medium (2) | High (3) | 6 |
| Legal | Medium (2) | Medium (2) | 4 |
|  | | Impact Score | Sum 22 |
| Risk Score (Likelihood x Impact Score) | | 66 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_\_Accept  \_X\_Mitigate  \_\_\_Share  \_\_\_Defer | |
| Risk Mitigation Controls | |  | |
| Firewall implementation | | Implementation of firewalls add a layer of network security | |
| VPN Connections | | Use secure VPN connections to ensure only authorized users have access to the network | |
| Monitoring | | Monitoring network traffic to catch and stop suspicious activity | |

### Risk 4: Natural Disaster

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Servers, Computers, Building | |
| Asset Importance | | Critical | |
| Threat | | Natural disasters (fire, floods, tornadoes, etc.…) | |
| Description | | Destruction of equipment, disruption of operations, loss of physical assets. Extended power outage can also make files, data, and applications unavailable | |
| Likelihood | | Medium (2) | |
| Impact on | | \_\_\_ Confidentiality  \_\_\_ Integrity  \_X\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | Low (3) | Low (3) | 9 |
| Reputation | Low (1) | Low (1) | 1 |
| Productivity | High (3) | High (3) | 9 |
| Legal | Low (1) | Low (1) | 1 |
|  | | Impact Score | Sum 20 |
| Risk Score (Likelihood x Impact Score) | | 40 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_\_Accept  \_X\_Mitigate  \_\_\_Share  \_\_\_Defer | |
| Risk Mitigation Controls: | |  | |
| Create backups | | Move/store data in cloud platforms | |
| Fire alarms/sprinklers | | Use fire alarms and sprinkler system to stop damage | |

### Risk 5: Physical Location/Security Monitoring Tools

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Servers, Computers, Building | |
| Asset Importance | | Critical | |
| Threat | | Unauthorized access, theft, compromise of monitoring systems, false positives/negatives. | |
| Description | | Break ins to the building, security system through physical or digital means | |
| Likelihood | | Medium (2) | |
| Impact on | | \_X\_ Confidentiality  \_X\_ Integrity  \_X\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | High (3) | High (3) | 9 |
| Reputation | Medium (2) | High (3) | 6 |
| Productivity | Medium (2) | High (3) | 6 |
| Legal | High (3) | High (3) | 9 |
|  | | Impact Score | Sum 30 |
| Risk Score (Likelihood x Impact Score) | | 60 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_\_Accept  \_X\_Mitigate  \_\_\_Share  \_\_\_Defer | |
| Risk Mitigation Controls: | |  | |
| Implement access controls such as keycard or biometric system | | Using key cards or biometrics can cut down on outsider access to areas they shouldn’t, ensures a way to track who is entering and exiting the building | |
| User Training | | Provide user training to improve awareness and prevention. | |
| Use surveillance cameras | | Cameras help monitor the physical location | |
| Use security monitoring system | | Security system for the building ensures any intruders or emergency will trip the alarm alerting fire responders | |

### Risk 6: Transaction Processing System

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | | Financial statements, data, and information | |
| Asset Importance | | Critical | |
| Threat | | Data Breachers, hacking and system failures | |
| Description | | Transaction or financial data is hacked, stolen by insider or outsider actor | |
| Likelihood | | Medium (2) | |
| Impact on | | \_X\_ Confidentiality  \_X\_ Integrity  \_X\_ Availability | |
| Impact Area | Priority | Impact | Score |
| Financial | High (3) | High (3) | 9 |
| Reputation | Medium (3) | High (3) | 9 |
| Productivity | Medium (3) | High (3) | 9 |
| Legal | High (3) | High (3) | 9 |
|  | | Impact Score | Sum 36 |
| Risk Score (Likelihood x Impact Score) | | 72 | |
| Adequacy of Existing Controls | | Low | |
| Risk Control Strategy | | \_\_\_Accept  \_X\_Mitigate  \_\_\_Share  \_\_\_Defer | |
| Risk Mitigation Controls: | |  | |
| Enforcement of access controls | | Create logins to track transaction history and allow access to transaction history | |
| Compliance with financial regulations | | Following GLBA and PCI DSS to protect customer financial data and maintain regulatory trust. | |
| Conduct security audits | | Regularly conducting audits will catch any issues and allow for updating the system | |

# Gap Analysis (completed by Christina Canady)

[Refer to Appendix E for SWOT Analysis diagram](#_Appendix_E_–)

A gap analysis is an in-depth review that helps the organization determine the difference between the current state of their information security to specific industry requirements. It allows organizations to identify areas of weakness within their network security controls to ensure that the network is robust and effective. To identify gaps the team conducted interviews from users and reviewed relevant parts of the networks hardware and software.

1. Better wi-fi coverage throughout salon

The wireless signal is weakest where most clients and stylists are located. The access point is at the furthest part of the salon away from where it is needed most.

1. Establish network security

There is little to no network security at this time, which makes this the most pressing issue. Industry standard is to have anti-virus and a network firewall, Tanglez has neither. This leaves them vulnerable to cybersecurity attacks.

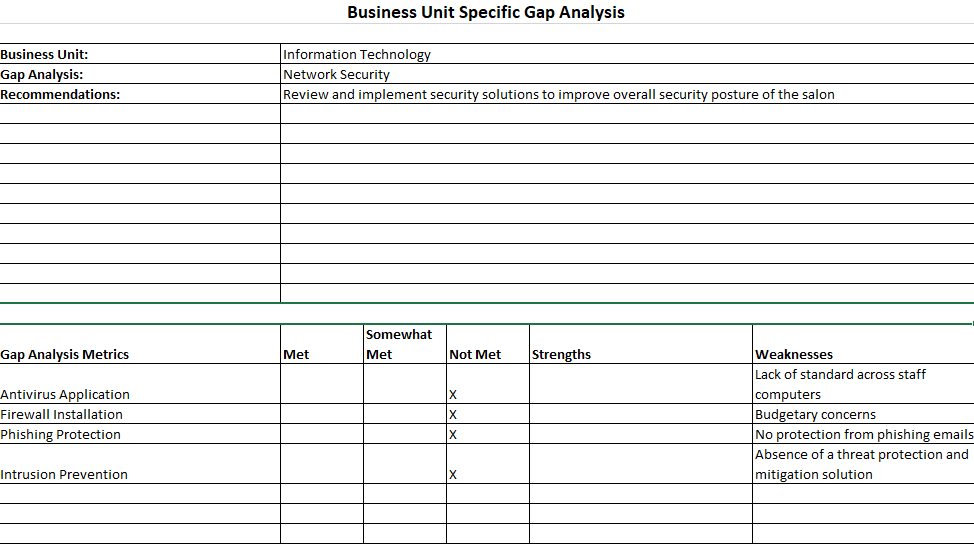
1. Employee training

Currently it is industry standard to have employees minimally trained in basic phishing, social engineering, and malware/hacking defense and detection. Training employees in basic security principles could offer significant security improvements to the current system at minimal cost.

1. Data loss prevention

There is currently no data-loss prevention in place at Tanglez. Implementing software such as Carbonite would save the company valuable time and money in the event of a disaster. It is industry standard to have some type of data loss prevention.

## Gap Analysis Form: Network Security (completed by Christina Canady)



## Gap Analysis Form: Employee Training (completed by Christina Canady)

A close-up of a document

Description automatically generated

# Recommendations (completed by Arianna DeNardo)

Based on the risk assessment, gap analysis and critical findings, the following suggestions are made to enhance Tanglez's cybersecurity and address urgent problems. The most urgent suggestion is to establish firewalls and access controls, such as passwords and account management, for customer data, financial records, and employee devices. These actions will also secure financial data and records to maintain confidentiality. Keep hardware and software up to date to patch vulnerabilities and strengthen security. Set up cameras for monitoring and prevention as well as a full security system for the building, including alarms and keypad entry. Install fire detection and prevention measures to lower the risk of natural disasters. Also, create and enforce controls and locks to safeguard physical assets and sensitive areas. Establish backup systems to avoid data loss and ensure business continuity in case of disasters. Offer comprehensive training to employees on cybersecurity best practices, including phishing, social engineering, and malware defense. Raise awareness of security protocols and the significance of keeping a secure network environment.

## Revised Physical Network Structure (completed by Kelsey Cox)

[Refer to Appendix D for Revised Physical Network Diagram](#_Appendix_D_-)

The revised network diagram is included, and the only changes are related to the modem and router. With the relocation of the modem and router from the back office and the addition of a table/cabinet near the washing stations, the strength of the internet signal will be better for the PCs  and tablet near the front of the salon with minimal effect on the devices in the office and wax/facials area. This will fix any signal related issues that the salon has had in the past.

## Revised Logical Network Structure (completed by Christina Canady)

[Refer to Appendix E for Revised Logical Network Diagram](#_Appendix_C_-)

The revised logical network structure includes the addition of a network firewall. The firewall will provide protection against outside cyberattacks by shielding the network from malicious or unnecessary network traffic. It will also prevent malicious software from accessing a computer or network via the internet.

# Migration Plan (completed by Brianna Baird)

[Refer to Appendix F for Migration Plan Timeline](#_Appendix_F_–)

Our objective over a 4-month timeline is to enhance network security and performance at Tanglez Salon & Spa within the allocated budget of $2,723.99. The plan is structured to prioritize critical tasks and allocate resources effectively.

In the first month, our immediate focus will be on the purchase and setup of the SonicWall TZ370 firewall appliance. This includes conducting research, selecting the appropriate firewall, configuring it to protect the network from cyberattacks, and ensuring its proper functionality through installation and testing. Moving to the second month, we will proceed with the implementation of Carbonite for Data Backup. This involves purchasing a subscription for data backups, setting up the Carbonite backup solution, and thoroughly testing data backup and recovery procedures to ensure functionality and reliability. Data backup is crucial to ensure business continuity and mitigate the risk of data loss in the event of a disaster.

In the third month, we will proceed with the implementation of Antivirus Software and the Wireless Access Point (WAP). We will purchase and install AVG Antivirus Business Edition for 5 devices, and provide training to employees on antivirus software usage and best practices for malware protection. Simultaneously, we will install the WAP to improve connectivity throughout the salon, ensuring optimal performance for both guests and employees.

Finally, in the fourth month, we will shift our attention to Employee Training on Basic Security Principles. We will develop a comprehensive cybersecurity training plan utilizing free resources available on LinkedIn. Subsequently, we will conduct training sessions for all employees to enhance their awareness and preparedness against cybersecurity attacks. Empowering employees with knowledge is essential to strengthen the overall security posture of the organization.

Throughout the project, we will maintain regular communication with stakeholders and continuously monitor progress to ensure that objectives are met within the allocated budget and timeline. Adjustments may be made as needed based on emerging requirements or challenges encountered during implementation.

# Detailed Budget (completed by Christina Canady)

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Yearly Cost** | **Benefit** | **Comments** |
| **SonicWall TZ370** | **1825.00** | **Protects from cyberattacks, controls unwanted websites, filters traffic in and out of network** |  |
| **Antivirus** | **99.99/5 devices** | **Protects from malware, trojans, ransomware** | **Many types, suggested is AVG antivirus business edition** |
| **Wireless Access Point** | **200$** | **Better connectivity throughout salon** |  |
| **Employee Training** | **0$** | **Employees are better prepared to defend company from cybersecurity attacks** | **Can be found free on LinkedIn** |
| **Carbonite** | **599$** | **Data backups in the event of disaster** |  |

**Total: 2723.99**

# Disaster Recovery Plan (completed by Christina Canady)

Currently, Tanglez does not have a Disaster Recovery Plan in place in case of natural disasters, power outages, or cyber-attacks. A DRP is created for an organization so an organization can have detailed instructions on how to respond to these unplanned incidents and disruptive events. Tanglez does not currently have any plan in place and therefore is left vulnerable in the unlikely event of a disaster. Our recommendation would be to invest in Carbonite Recovery Disaster services. Carbonite is a cloud-based backup solution that provides unlimited data backup services. Listed below are the steps necessary to implement a Disaster Recovery or Cyberattack Plan.

**Step One**: Put together a team of employees with at least one member being technologically literate.

**Step Two**: Set clear RTO’s and RPO’s. The RTO (recovery time objective) is the length of time an application can be down before business is negatively impacted. An RPO (recovery point objective) is the most data that can be lost before business is significantly harmed.

**Step Three:** Take detailed inventory of al lhardware and software being used as well as any asset in the organization’s possession. This is a crucial step because you want to prioritize this list in the event of a disaster.

**Step Four**: Outline roles and responsibility for all members of team. Create a call sheet with everyone’s contact information along with their role and responsibilities within the group.

**Step Five:** Document a recovery strategy. This should include how to access data backups, communication procedures and post-disaster activities.

**Step Six:** Create a crisis communication plan. This is where public relations would get involved if they are present. Be sure to have a clear strategy to keep stakeholders informed and up to date with what is happening.

**Step Seven:** Test all plans! Update plans with necessary revisions if needed.

# Cybersecurity Plan (completed by Luke Jarrell)

Currently, Tanglez does not have a Cybersecurity plan in place which could leave businesses vulnerable to cyber-attacks. For Tanglez to be prepared for a cyberattack we have created a cybersecurity plan to implement, the plan consists of steps and procedures to ensure the security of Tanglez. Those steps include:

* **Knowing the risks**: Understanding what could go wrong and how to properly protect your data
* **Teach your team**: Teach staff how to target threats and prepare them to deal with these situations
* **Keeping Updated**: Ensure technology has up-to-date security fixes
* **Backing up data**: Have copies of important information on site in case something goes wrong
* **Keep learning**: Stay up to date on new ways to keep Tanglez safe from hackers

# Conclusion (completed by Kelsey Cox)

Tanglez Salon is running is running a network very similar to a home network layout with a simple modem and router. Because it is a small business, this is the most ideal setup for their environment, and nothing is hardwired. We have made recommendations and plans that would help improve performance, efficiency, and security measures. These include a wireless access point, a Carbonite data backup system, antivirus software, and basic employee training to lessen the risk of cybersecurity attacks. Changing default credentials, setting up a separate guest network, and using strong passwords will also improve their network posture and protect accessible client data. Additionally, after identifying problems in the logical and physical network, we chose to move the modem and router to a more centralized location in the salon to increase connectivity and signal. With a small investment in protective software measures, Tanglez Salon can ensure that no one breaches their customer data from the outside. They can also feel better knowing that only authorized users, such as employees and the owner, can access this information. We believe that these changes will help the salon in the long run by making customers feel more comfortable knowing that Tanglez is protecting their information and can be trusted with it.

# Appendix A – IT Governance Diagram (completed by Arianna DeNardo)

A group of people with text

Description automatically generated with medium confidence

# Appendix B - Enterprise Architecture Diagram (completed by Brianna Baird)

A diagram of a computer network

Description automatically generated

# Appendix C - Revised Logical Diagram (completed by Christina Canady)

A diagram of a network

Description automatically generated

# Appendix D - Revised Physical Network Diagram (completed by Kelsey Cox)

A diagram of a room

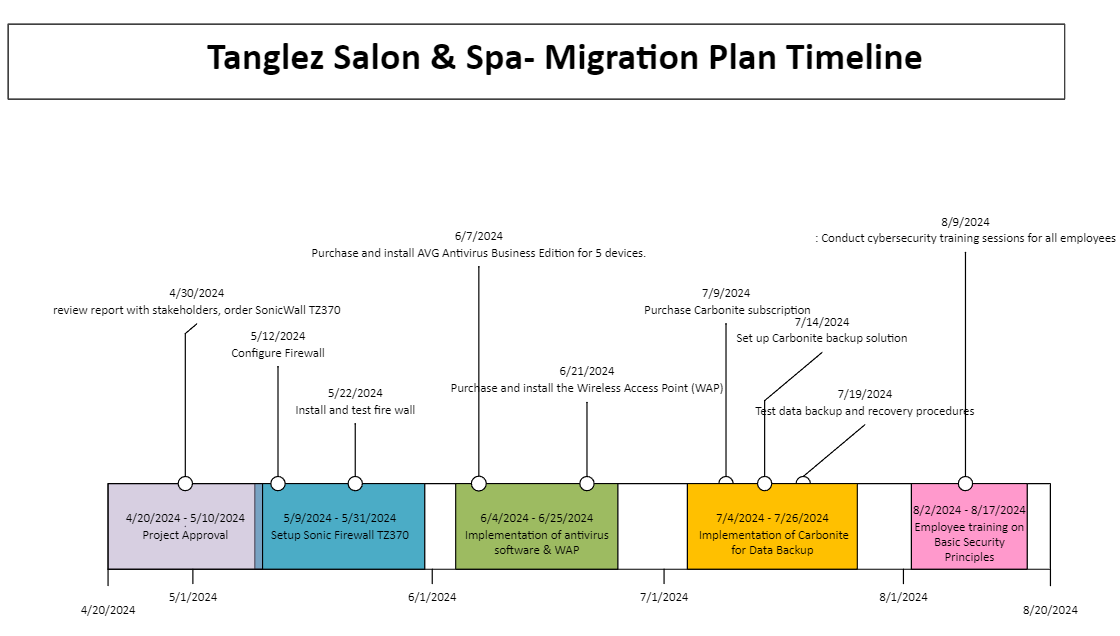
Description automatically generated

# Appendix E – SWOT Analysis (completed by Christina Canady)

A diagram of a business

Description automatically generated with medium confidence

# Appendix F – Migration Plan Timeline (completed by Brianna Baird)



# Appendix G – Current Physical Network Diagram (completed by Kelsey Cox)

A floor plan of a room

Description automatically generated

# Appendix F – Current Logical Network Diagram (completed by Christina Canady)

