A logo for a flower shop

Description automatically generated

**Organization Name:**

Wildflower Florist LLC

**Company Liaison:**

Jessica Wells; Owner

518 Greenville Blvd SE

Ste F

Greenville, NC 27858

**Project Name:** Wild MIS

**Members:**

Mikayla Hawley, Austin Bing-Zaremba, Jordan Moser, Tyler DeChellis, Savanna Pulver

**Liaison Approval**

I authorize permission for members from East Carolina University MIS 4123 class to utilize information regarding Wildflower Florist business operations and technology infrastructure for their network project.

Company Liaison: Jessica Wells, Owner

Signature: \_\_\_\_Jessica Wells\_\_\_\_\_

Date: \_\_\_\_2/5/2024\_\_\_

Business Overview

Wildflower Florist is located in the heart of Greenville NC. Jessica founded Wildflower Florist in 2020 and ran it out of her apartment. In 2022 she took the plunge and opened a storefront where the demand became more than her apartment could handle. They have a wide variety of arrangements to choose from for local delivery. They are different from the average florist because they give their customers the opportunity to build their own bouquet at their flower bar. The flower bar is priced per stem and has a variety of different flowers at different price points. Wildflower Florist also ships nationwide! The store front is also stocked with merchandise that can make the perfect gifts for everyone from soaps, plant accessories, stationery, candles and even locally made beef sticks. Opening the chicest and most modern “feel good” flower shop was a dream come true for Jessica.

Introduction

Wildflower Florist only has one location, but it is essential ensure their network is secure to keep sensitive business and customer information secure. Wildflower Florist is a small company that has a laptop and iPad used for order tracking and bookkeeping. There is a point-of-sale system used daily to ring up merchandise and charge customers for arrangements. There is a cellphone that is the shop phone that many customers call with any questions, concerns and to place orders. The employees also use their personal cellphones to see the deliveries they need to make and to follow a route. A printer is also part of their network as it is used daily and prints off customer orders the contain sensitive information. We will be analyzing Wildflower Florist network to find ways to improve and ensure that the network is secure.

IT Governance Structure

Most technological needs will be requested by the employees. They are taking customer orders that contain personal information and receiving online orders to enter them in their database. Being a small company there is no board of directors but any decisions regarding the implementation of innovative technology or changes to be made to existing technology would be made by the owner, Jessica Wells.

IT Governance Diagram

Wildflower Florist Employees

Wildflower Florist Owner; Jessica Wells

Enterprise Architecture

Wildflower Florist operations are conducted at their store front in Greenville, North Carolina. The storefront houses all their devices other than employee phones that come and go. They are currently using Metronet for internet services. Google Sheets is used to track the cost breakdown for events such as weddings and is shared between Wildflower employees and the customer. Each Google Sheet is specific based on the customer. A laptop and iPad are used at the shop location to manage current customers, orders, and more. Employees do use their phones to get delivery information while out on deliveries.

Enterprise Architecture Diagram:

A close-up of a computer

Description automatically generated

Project Scope

Our project's scope is to analyze the Wildflower Florist network in place. The project’s goal is to help Wildflower Florist have a more secure network. We will be conducting an analysis of the current system, and we will be proving recommendations to create a secure network.

Next Steps

1. Gather Information: Collect information about the company's current IT systems, security measures, and potential risks. Talk to people in the IT department and other relevant teams to understand their concerns and needs.

2. Assess Needs: Look at what the company needs to improve its IT systems and security. Figure out if there are outdated computers, software, or security measures that need upgrading.

3. Identify Risks: Think about what could go wrong with the company's IT systems. Consider things like hackers, computer viruses, or problems with physical equipment.

4. Find Gaps: Compare what the company has now with what it needs. Look for places where there's a difference, like missing security measures or outdated technology.

5. Make Recommendations: Come up with ideas for how to fix the problems and make improvements. This might involve things like upgrading computers, installing better security software, or training staff on cybersecurity.

6. Write Everything Down: Create a report that explains all your findings and recommendations. Make sure to include diagrams or charts to help people understand.

7. Present Recommendations: Share your report with the company's leadership or IT team. Explain your findings and why your recommendations are important.

8. Get Feedback: Listen to what people think about your recommendations. Make any changes or updates based on their feedback. 9. Implement Changes: Start putting your recommendations into action. This might involve buying new computers, installing software, or training staff.

10. Test Everything: Make sure all the changes work like they're supposed to. Test security measures to make sure they keep the company safe from hackers.

11. Monitor and Adjust: Keep an eye on the company's IT systems and security. If anything isn't working right, make adjustments to fix it.

12. Review and Update: Regularly review the company's IT systems and security measures. Update things as needed to keep the company safe and efficient.

Logical Network Diagram

A diagram of a computer network

Description automatically generated

Physical Network Structure

A blueprint of a store

Description automatically generated

Needs Assessment:

After meeting with Jessica, we found that the main concern is network security. With being a small business, she does not have the budget that other companies have to spend on improving network security

Need #1: Secure WiFi Information

|  |  |
| --- | --- |
| Statement of Purpose | To ensure sensitive customer information regarding customer orders is secure, Wildflower Florist needs to protect sensitive information such as their WiFi password. |
| Situation / Goals | Currently Wildflower Florist keeps their WiFi information taped to a wall by the bathroom. This creates a security risk as customers ask to use the bathroom in the back. |
| Process | Jessica will take down the WiFi information on the wall by the bathroom and keep their information in a secure spot only employees will know about. |

Need #2 Two-Factor Authentication

|  |  |
| --- | --- |
| Statement Of Purpose | A two-factor authentication will help secure the iPad at the shop that holds important information in it. Instilling a two-factor system such as Face ID and receiving text messages within a code to log in or receiving in through email will help secure the devices limiting potential hazards like a password being leaked and giving access to the iPad from a 3rd party device. |
| Situation/Goals | The two-factor system being installed will limit the number of potential hackers trying to get into the system due to their being a required code. |
| Process | When an employee is logging into an iPad, after they input the correct password exclusively correlated to their account. They will receive a one-time code to their personal phone number or email that they will then put in the iPad to confirm the login. |

Threats

1. Data Breach: The risk of unauthorized access to customer and business data, including personal information and financial records, poses a significant threat. This could result from hacking attempts, phishing attacks, or insider threats.
2. Network Vulnerabilities: Weaknesses in the network infrastructure, such as outdated software, unpatched systems, or misconfigured devices, expose Wildflower Florist to the risk of malware infections, data theft, or disruption of services.
3. Physical Security: The physical security of devices and equipment, including laptops, iPads, and the printer, is crucial. Theft, damage, or unauthorized access to these assets could disrupt business operations and compromise sensitive information.
4. Third-Party Risks: Dependencies on third-party services, such as Metronet for internet connectivity or Google Sheets for data storage, introduce risks related to service outages, data breaches, or compliance issues.
5. Employee Training: Insufficient training or awareness among employees regarding cybersecurity best practices increases the risk of human error, social engineering attacks, and inadvertent data breaches.
6. Regulatory Compliance: Failure to comply with relevant regulations, such as data protection laws or payment card industry standards, may lead to legal penalties, financial losses, and damage to company’s reputation.

Risk Analysis

1. Likelihood: The likelihood of a data breach or network compromise is moderate to high given the prevalence of cyber threats targeting small businesses. Physical security risks are relatively lower but still significant.
2. Impact: The impact of a data breach or network intrusion could be severe, resulting in financial losses, reputational damage, legal consequences, and disruption of business operations. Physical security incidents may lead to equipment downtime and productivity losses.
3. Risk Rating: Based on the likelihood and impact, the overall risk rating for data breaches and network vulnerabilities is considered high, while physical security risks are moderate.

Risk Strategies

1. Implement Robust Security Measures: Deploy firewalls, antivirus software, and intrusion detection systems to protect against cyber threats. Regularly update and patch software to address vulnerabilities.
2. Enhance Access Controls: Implement strong password policies, multi-factor authentication, and least privilege access to limit unauthorized access to systems and data.
3. Physical Security Measures: Secure devices and equipment with locks, surveillance cameras, and access control systems. Store sensitive information in locked cabinets or safes.
4. Vendor Risk Management: Assess the security practices of third-party vendors and ensure compliance with data protection regulations. Maintain backups of critical data stored with third-party providers.
5. Employee Training: Provide regular cybersecurity awareness training to employees to educate them about common threats, phishing scams, and best practices safeguarding data.
6. Compliance Management: Establish processes and controls to ensure compliance with relevant regulations, including data protections and privacy laws. Conduct regular audits to assess compliance posture.

Risk Conclusion

By conducting a thorough risk assessment and implementing appropriate mitigation strategies, Wildflower Florist LLC can actively mitigate potential threats and vulnerabilities to its IT infrastructure and operations. Proactive risk management is essential for safeguarding sensitive information, maintaining business continuity, and preserving the trust of customers and stakeholders.

Gap Analysis

|  |  |  |
| --- | --- | --- |
| INFORMATION SECURITY | MET, PARTIALLY MET, NOT MET | Description |
| Password and Information Security | Partially met | All technology owned by the company has been given a unique password as well as each employee assigned a unique and complex username. Two-Factor authentication is still being implemented into Wildflower's technology. |
| Secure Wi-Fi Password | MET | Complex Wi-Fi passwords are only given to employees with no access to the public. |
| Firewall | NOT MET | Still working on finding a suitable firewall for an added layer of protection for the information and Wi-Fi. |

II. Resource Gaps:

A. *Resource Allocation and Utilization*:

1. Allocation: Limited budget allocated for network security and maintenance.

2. Utilization: Lack of dedicated IT staff to monitor and manage network security.

B. *Current Resource Availability:*

1. Limited budget for network security measures such as firewall, antivirus software, and regular updates.

2. Lack of IT staff to handle network security issues and perform regular maintenance tasks.

C. *Required Resource Levels*:

1. Increased budget allocation for network security measures to ensure adequate protection against cyber threats through firewalls.

2. Hiring or contracting dedicated IT staff or training current employees to monitor and manage network security and perform regular maintenance tasks.

SWOT



Disaster Recovery Plan

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Critical System** | **Threat** | **Response Strategy** | **Response Action Steps** | **Recovery Strategy** | **Recovery Action Steps** |
| Confidential Data | Security threat to information | Make sure important information is highly secured using the previously implemented two factor auth | Make sure important data is always password protected | Immediately disconnect the compromised device or devices from the network. Disable remote access to the network if possible, to prevent further unauthorized access. | Analyse what has been compromised and asses from there |
| Outdated Technology | Out of date systems | Buy up to date technology if the latter can no longer hold the information needed securely. | Purchase new technology | Identify the specific technology needs based on current requirements and future growth projections. | Figure out what technology needs to be updated and purchase the up-to-date software or version |

Cybersecurity Plan:

In the event of a breach of Wildflower Florist network, we advised her to think proactively on ways to protect her companies sensitive information by implementing data encryption to make the data unreadable to anyone who is unauthorized to view that information.

Migration Planning

Wildflower Florist LLC is embarking on a migration project to enhance its IT infrastructure and improve network security. This migration will involve upgrading software, implementing new security measures, and ensuring minimal disruption to business operations. This following migration plan outlines the steps, timelines, and diagrams for a successful transition.

Objective

1. Upgrade software and hardware components to improve network security and efficiency.
2. Implement robust security measures to safeguard sensitive business and customer information.
3. Minimize downtime and disruption to business operations during the migration process.
4. Ensure compliance with relevant regulations and standards, including data protections laws.

Plan

1. Assessment Phase (Week 1-2)
   1. Conduct a comprehensive assessment of existing IT infrastructure, software, and security measures.
   2. Identify current vulnerabilities, risks, and areas for improvement.
   3. Develop migration goals, objectives, and success criteria.
2. Planning Phase (Week 3-4)
   1. Develop a detailed migration plan outlining tasks, responsibilities, and timelines
   2. Procure necessary hardware, software licenses, and security tools.
   3. Define roles and responsibilities for team members involved in the migration process.
3. Preparation Phase (Week 5-6)
   1. Backup all critical data and systems to ensure data integrity and continuity.
   2. Conduct employee training sessions on new software, security protocols, and best practices.
   3. Perform system tests and simulations to identify and resolve potential issues.
4. Execution Phase (Week 7-10)
   1. Install and configure new hardware, software, and security measures according to the migration plan.
   2. Migrate data and applications to the new infrastructure while ensuring minimal disruption to business operations.
   3. Monitor the migration progress and address any issues or concerns in real-time.
5. Validation Phase (Week 11-12)
   1. Conduct thorough testing and validation of the migrated systems to ensure functionality and security.
   2. Verify data integrity and accessibility across all applications and devices.
   3. Obtain feedback from users and stakeholders to identify any remaining issues or areas for improvement.
6. Transition Phase (Week 13)
   1. Finalize the migration process and officially transition to the new IT infrastructure.
   2. Update documentation, user manuals, and standard operating procedures to reflect the changes.
   3. Conduct a post-implementation review to assess the success of the migration and identify lessons learned.

Conclusion

By following this migration plan, Wildflower Florist LLC can successfully upgrade its IT infrastructure, enhance network security, and ensure minimal disruption to business operations. With careful planning, thorough preparation, and effective execution, the migrating process will position the company for improved efficiency, compliance, and resilience in the ever-evolving digital landscape.

Network Security:

Wildflower Florist already has their own wireless internet, but we decided the main thing needed right now to promote security is relocating their WiFi information that includes the password. This is a simple fix that will drastically increase the security with no cost to them. The cost is important when it comes to the budget for network security. This was not costly and benefited the business overall.

Budget:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | |  | |  |  | **IT Security Budget** |  |  |
| **Project Proposed** | **Recommended Vendor** | **Systems** | **Link to Product Proposed** | **Cost Pm** | **Cost PY** |
| **Metronet** | **Metronet** | **Includes Modem/Internet Services** | [**I Want Fiber | Metronet Metronet internet costs - Search (bing.com)**](https://www.metronet.com/iwantfiber?serviceability=no&address=29601) | **$ 100.00** | **$ 1,200.00** |
| **Firewall** | **Aura Antivirus- Ultimate Plan** | **Up to !0 Systems** | [**Stop Viruses & Malware in Their Tracks | Aura Antivirus**](https://buy.aura.com/antivirus-intro-ni?irclickid=zVGTybRgRxyPT6zQA5wMK2VvUkHRtXzGIwJx1c0&iradname=Gtwy-AV%3A%20Top10%20Intro%20Desktop%20Simplified%20Plan%20Cards&iradid=1977578&irgwc=1&c1=34020&camp=12398&utm_source=top10&utm_medium=ir_affiliate&mktp=ir_affiliate&sharedid=uGsmU5vpq5&utm_gateway=av&utm_campaign=av-intro) | **$5.00** | **$59.00** |
| **Antivirus Software** | **Aura Antivirus- Ultimate Plan** |  |  | **Included w/Aura** | **Included w/Aura** |
| **Intrusion Detection System** | **Aura Antivirus- Ultimate Plan** |  |  | **Included w/Aura** | **Included w/Aura** |
| **VPN Cost** | **Aura Antivirus- Ultimate Plan** |  |  | **Included w/Aura** | **Included w/Aura** |
| **Cabinet and enclosure** | **ULINE** | **Protect Computer and house iPad securely** | [**Mobile Computer Cabinet - 23 x 25 x 64" H-7545 - Uline**](https://www.uline.com/Product/Detail/H-7545/Media-Carts/Mobile-Computer-Cabinet-23-x-25-x-64?pricode=WB8368&utm_source=Bing&utm_medium=pla&utm_term=H-7545&utm_campaign=Carts&utm_source=Bing&utm_medium=pla&utm_term=H-7545&utm_campaign=Carts&msclkid=686192a0b58c1919c765f4b3f6d5394f) |  | **$ 495.00** |
| **Surveillance Cameras** | **Simpli Safe** | **Monitor Store remotely- Sensors, Cameras, Surveillance System** | [**SimpliSafe vs. ADT vs. Ring | SimpliSafe Home Security https://simplisafe.com/build-my-system#Summary**](https://simplisafe.com/simplisafe-vs-adt-vs-ring?pcrid=&utm_campaign=bing.competitors.exact.tcpa&utm_term=catchall&utm_content=&utm_medium=search&utm_source=bing&utm_network=o&utm_device=c&utm_target=&utm_position=&msclkid=1d8c8964b7ed10dc814aef77f34d8e5f) | **$ 25.50** | **$ 611.89** |
| **Access Control System** | **Simpli Safe** |  |  | **Included w/Simpli Safe** | **Included w/Simpli Safe** |
| **Backup Data System** | **Acronis Cyber** | **Advanced Plan for Main computer backup** | [**Acronis Cyber Protect Home Office (Formerly True Image) - Integrated Backup and Anti Malware Protection**](https://www.acronis.com/en-us/products/true-image/?cjdata=MXxOfDB8WXww&utm_medium=affiliate&utm_source=5226272&utm_campaign=cj&utm_content=10562048&utm_term=051yf2UVmU7I0JrcaerWORd&cjevent=76d39f52f54611ee80b001ec0a1cb827) |  | **$ 42.49** |
| **Employee Training** | **Budget for 2 hours of Training every 6 months.** | **Training completed by Jessica Wells** |  |  | **$ 400.00** |
| **Maintenance** | **Acronis Cyber/SimpliSafe/Aura Included in Plans** |  |  | **Included** | **Included** |
| **Employee Cell phone expenses** | **Employee own cell phone provider** | **Use of Personal phone for 2 step verification codes and security checks** | **Recommend setting $15 per month or approximately 10% of total cell phone use per employee for personal use** | **$ 90.00** | **$ 1,080.00** |
|  |  |  |  |  |  |
|  |  |  | **Total Cost:** | **$ 195.00** | **$3,888.38** |

Appendix

Enterprise Architecture:

A close-up of a computer

Description automatically generated

Logical Network Diagram

A diagram of a computer network

Description automatically generated

Physical Network Structure:

A blueprint of a store

Description automatically generated