Project Proposal: Secure Network Development for Small Business

Introduction:

I propose the implementation of a comprehensive and secure network infrastructure for a new small business. The primary objective is to establish a robust and efficient network environment that ensures data integrity, confidentiality, and availability. The project will cover various aspects, including network design, firewall setup, WiFi configuration, Active Directory deployment, group policies, cybersecurity support, written information security plan (WISP), disaster recovery, and power outage planning.

Project Overview:

The project will be structured into the following key components:

1. **Network Map / Firewall Setup & WiFi Chart:**
   - Create a secure network map outlining the placement of virtual machines (VMs) and network components.
   - Configure a dedicated firewall VM using software such as pfSense or OPNsense to control traffic.
   - Establish a secure WiFi network with WPA3 encryption, separate internal and guest networks, and implement MAC address filtering.
2. **Active Directory Server:**
   - Deploy a Windows Server VM as the Active Directory Domain Controller.
   - Configure DNS and DHCP services on the server to streamline network management.
   - Create file shares on the server to facilitate seamless data access for business VMs.
3. **Group Policies:**
   - Implement Group Policy Objects (GPOs) to enforce security policies, limit user control, and manage software installations.
   - Control user permissions, restrict USB usage, and set login hours and other security-sensitive settings.
4. **Cyber Security Support Plan:**
   - Regularly update and patch all operating systems.
   - Install and maintain up-to-date antivirus and anti-malware software.
   - Develop and implement an incident response plan to address security breaches promptly.
5. **Written Information Security Plan (WISP):**
   - Define and classify types of data based on sensitivity.
   - Clearly outline access control policies for different data levels.
   - Implement physical security measures for servers and networking equipment.
6. **Disaster Recovery Plan:**
   - Develop a backup strategy, including regular backups of critical data to an offsite location.
   - Implement redundancy for critical systems to minimize downtime.
   - Create a plan for data restoration in case of data loss.
7. **Power Outage Plan:**
   - Install Uninterruptible Power Supply (UPS) devices for critical systems.

- Consider a generator for extended power outages.

Implementation Steps for VM1 (Example):

- Create a new VM in VirtualBox, install Windows, and allocate appropriate resources.
- Configure networking for internal communication and internet access.
- Install necessary Windows updates, security patches, and antivirus software.
- Join VM1 to the Active Directory domain and configure Group Policies.
- Set up access to the file share provided by the Active Directory server.
- Implement backup configurations and power management settings.

Conclusion:

The proposed project aims to create a secure and resilient network infrastructure tailored to the specific needs of the small business. By addressing key areas such as network design, access controls, cybersecurity, and disaster recovery, we aim to provide a comprehensive solution that ensures the integrity and security of the business's digital assets. The outlined steps for each component will guide the implementation process, leading to a well-protected and efficiently managed network environment.