**REMEDIATION PLAN**

Problem Statement: Company identifies a security vulnerability in their IT infrastructure:

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Example** |
| **1.** | Conducting a risk assessment | Identify the risk of a potential cyberattack due to outdated software and inadequate firewall protection. Assess the likelihood and potential impact of a security breach. |
| **2.** | Identifying the root cause of the problem | Determine that the outdated software and weak firewall configuration are the primary factors contributing to the vulnerability. |
| **3.** | Developing an action plan | Upgrade software systems to the latest versions, implement a more robust firewall solution, and conduct vulnerability assessments regularly. Set a timeline of one month for software upgrades, two weeks for firewall implementation, and monthly vulnerability scans. |
| **4.** | Assigning responsibilities and resources | Assign the IT department to handle software upgrades, hire an external cybersecurity consultant to configure the firewall, and designate a project manager to oversee the remediation process. Allocate a budget for software licenses, consultant fees, and necessary hardware upgrades. |
| **5.** | Monitoring progress and reporting results | Use a project management tool to track the progress of each task, including software upgrades, firewall configuration, and vulnerability assessments. Generate monthly progress reports to update senior management on completed actions, ongoing tasks, and any emerging risks or challenges. |