**IT Subnet Risk Assessment**

**Payroll & Web Servers**

**Valuation**

* **Cost to Replace:**
  + **Indirect Costs:**
    - Downtime leading to payroll delays and employee dissatisfaction
    - Loss of company reputation due to potential payroll issues
  + **Equipment Value:**
    - **Direct Cost:** $5,000 ~ $10,000 per server
    - **Labor Cost:** ~$2,000 for setup and configuration
  + **Cost to Recover Data:**
    - **Restoring backups:** $500 ~ $2,000
    - **Rebuilding lost data manually:** ~$10,000+ (if backups are unavailable)
* **Cost per Hour of Downtime:**
  + **Payroll server outage:**
    - Employee frustration & potential legal repercussions: ~$500/hr
    - Delay in tax reporting: ~$1,000/hr
  + **Web server outage:**
    - Customer service disruptions: ~$300/hr
    - Potential loss of business: ~$1,500/hr

**Threats**

* **Cyberattack (DDoS, SQL Injection, Ransomware)**
  + Worst case: Complete data loss and downtime for multiple days
  + Average case: Service interruption for a few hours, requiring reconfiguration
* **Hardware Failure**
  + Worst case: Complete server failure requiring replacement ($10,000+)
  + Average case: Partial failure with downtime of several hours ($1,000+ loss)
* **Fire/Flooding/Physical Damage**
  + Worst case: Total asset loss, rebuilding takes weeks
  + Average case: Damage requiring repairs and temporary service loss

**Vulnerabilities**

* Lack of failover servers for payroll & web systems
* Insufficient firewall and intrusion detection configurations
* Lack of redundant backups
* Poor employee awareness of phishing/social engineering threats

**Mitigations**

* Implement redundant failover servers ($10,000+)
* Strengthen firewall and IDS rules ($5,000+)
* Ensure off-site, air-gapped backups ($3,000+)
* Conduct security awareness training for employees (~$1,500 annually)

**Employee Workstations (computers and phones)**

**Valuation**

* **Cost to Replace:**
  + **Computers:** ~$1,200 each
  + **Phones:** ~$600 each
* **Cost per Hour of Downtime:**
  + Employee productivity loss: ~$50/hr per employee

**Threats**

* **Malware/Ransomware**
  + Worst case: All workstations compromised, requiring full wipe and restore
  + Average case: Individual device compromise, partial downtime
* **Phishing/Social Engineering**
  + Worst case: Credential theft leading to broader network compromise
  + Average case: Individual account compromise requiring resets
* **Hardware Failure**
  + Worst case: Multiple devices fail simultaneously, leading to major productivity loss
  + Average case: Single device failure requiring replacement

**Vulnerabilities**

* Lack of endpoint protection and monitoring
* Weak or reused passwords
* No multi-factor authentication (MFA) for critical systems

**Mitigations**

* Deploy enterprise-grade endpoint protection ($3,000+ annually)
* Enforce MFA for all internal systems (~$2,000 one-time setup)
* Conduct phishing training & periodic audits (~$1,500 annually)

**Printers/Copiers**

**Valuation**

* **Cost to Replace:** ~$2,000 each (~$4,000 total)
* **Cost per Hour of Downtime:** Minimal, but can slow down workflows (~$50/hr)

**Threats**

* **Unauthorized Access (Compromised Network Printer)**
  + Worst case: Attackers use the printer as a foothold for network compromise
  + Average case: Sensitive documents leaked due to misconfiguration
* **Hardware Failure**
  + Worst case: Complete failure requiring replacement
  + Average case: Temporary outage requiring minor repairs

**Vulnerabilities**

* Default credentials not changed
* Lack of firmware updates
* No segmentation of printer network

**Mitigations**

* Change all default credentials ($0 cost, immediate implementation)
* Implement firmware update policy (~$1,000 annually for monitoring)
* Segregate printers onto a separate VLAN (~$500 setup cost)

**General IT Subnet Recommendations**

* **Network Security Enhancements:**
  + Implement strict firewall rules (~$5,000)
  + Deploy intrusion detection/prevention systems (~$8,000)
  + Regular penetration testing (~$10,000 annually)
* **Backup & Disaster Recovery Plan:**
  + Implement automated nightly backups (~$3,000)
  + Ensure offsite storage for critical backups (~$2,000 annually)
* **Incident Response Planning:**
  + Develop & test an incident response plan (~$5,000 annually)
  + Train employees on security best practices (~$2,000 annually)