IT SUBNET

RISK ASSESSMENT

Comprehensive Analysis of Infrastructure Vulnerabilities and Mitigation Strategies

Prepared by:

Jacob Garcia (garcia_j08018@utpb.edu)
Bryan Lim (lim_p65274@utpb.edu)
Casey Sharp (sharp_c55507@utpb.edu)
Raquel Lugo (lugo_r18456@utpb.edu)
Grzegorz Rudnicki (rudnicki_g60758@utpb.edu)

April 1, 2025

Contents

Executive Summary

This comprehensive risk assessment evaluates critical components of the organization's IT subnet infrastructure, including payroll systems, web servers, employee workstations, and network peripherals. The assessment identifies significant vulnerabilities, analyzes potential threats, and proposes targeted mitigation strategies prioritized by risk level and implementation feasibility.

Key findings indicate that the organization faces substantial risks from ransomware attacks, insufficient backup procedures, and limited security awareness among personnel. The proposed mitigation strategy focuses on implementing a multi-layered defense approach, with priority actions including:

- Deployment of multi-factor authentication across critical systems
- Implementation of robust backup and recovery procedures
- Enhancement of network segmentation and firewall configurations
- Development of a comprehensive security awareness program
- Establishment of formal incident response capabilities

The total estimated investment of $75,000-$125,000 (phased over 12 months) represents a prudent allocation given the potential impact of a security incident, which could exceed $250,000 in direct costs alone, not including reputational damage and operational disruption.

By adopting these recommendations, the organization will significantly improve its security posture, ensure operational resilience, protect sensitive data, and maintain stakeholder trust.

Chapter 1

Detailed Asset Valuation

This chapter provides a comprehensive valuation of the organization's IT assets, establishing the foundation for risk prioritization and mitigation resource allocation.

1.1 Payroll & Web Servers

Table 1.1: Payroll & Web Server Asset Valuation

Asset Component	Direct Cost	Indirect Cost	Total Valuation
Server Hardware	$5,000-$10,000	Configuration: $2,000	$7,000-$12,000
Server Software	$3,000-$8,000	Licensing: $1,500/yr	$4,500-$9,500
Operating System	$1,000-$2,000	Maintenance: $800/yr	$1,800-$2,800
Data Recovery (Backups)	$500-$2,000	Labor: $1,000	$1,500-$3,000
Data Recovery (Manual)	$10,000+	Labor: $5,000+	$15,000+

1.1.1 Operational Impact

- **Payroll Server Downtime:**
  - Employee frustration & potential legal repercussions: $500/hr
  - Delay in tax reporting: $1,000/hr
  - **Total Impact:** $1,500/hr
- **Web Server Downtime:**
  - Customer service disruptions: $300/hr
  - Potential loss of business: $1,500/hr
  - **Total Impact:** $1,800/hr
- Regulatory Penalties (Data Breach): Up to $100,000 depending on jurisdiction
- Legal Liability: Potential class-action lawsuits with settlements exceeding $250,000

1.1.2 Intangible Costs

- Employee Dissatisfaction: Increased turnover (15-20%)
- Reputation Damage: Customer trust erosion (10-30% customer loss)
- Brand Impact: Recovery time of 6-18 months

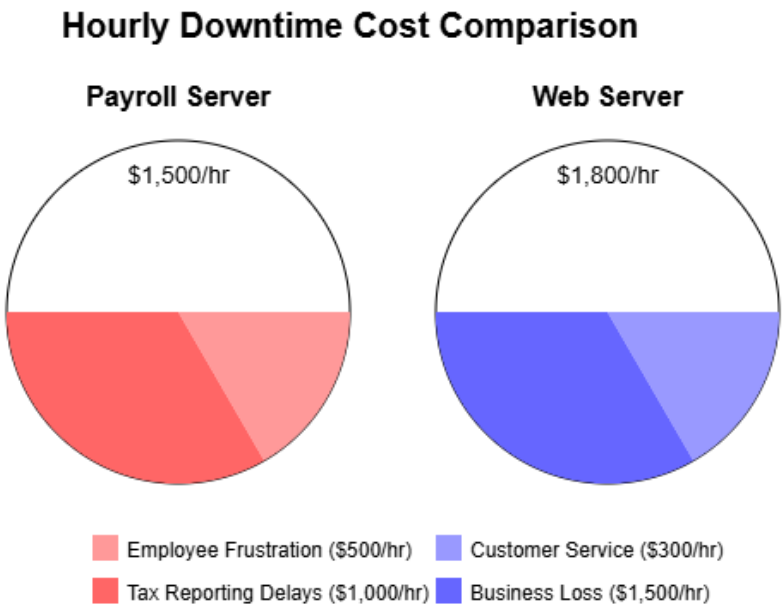

Figure 1.1: Hourly Downtime Cost Comparison for Server Infrastructure

1.2 Employee Workstations

Table 1.2: Employee Workstation Asset Valuation

Asset Component	Direct Cost	Indirect Cost	Total Valuation
Workstation Hardware	$1,200 each	Setup: $200 each	$1,400 each
Mobile Devices	$600 each	Configuration: $100 each	$700 each
Software Licenses	$300-$800 per seat	Renewal: $150-$400	$450-$1,200 per seat
Local Data	Variable	Recovery: $50-$500	Variable + recovery

1.2.1 Operational Impact

- Productivity Loss: $50/hr per employee
- Cumulative Organization Impact: $50 × n employees × hours of downtime
- For an organization with 100 employees: $5,000/hr total productivity loss

1.3 Printers/Copiers and Network Peripherals

1.3.1 Operational Impact

- Device Downtime: $50-$200/hr depending on department reliance
- Document Processing Delays: Variable based on business processes

Table 1.3: Network Peripherals Asset Valuation

Asset Component	Direct Cost	Indirect Cost	Total Valuation
Enterprise Printers	\$2,000-\$5,000 each	Maintenance: \$500/yr	\$2,500-\$5,500 each
Network Switches	\$1,000-\$3,000 each	Configuration: \$400 each	\$1,400-\$3,400 each
Routers/Firewalls	\$3,000-\$8,000 each	Setup: \$1,500 each	\$4,500-\$9,500 each

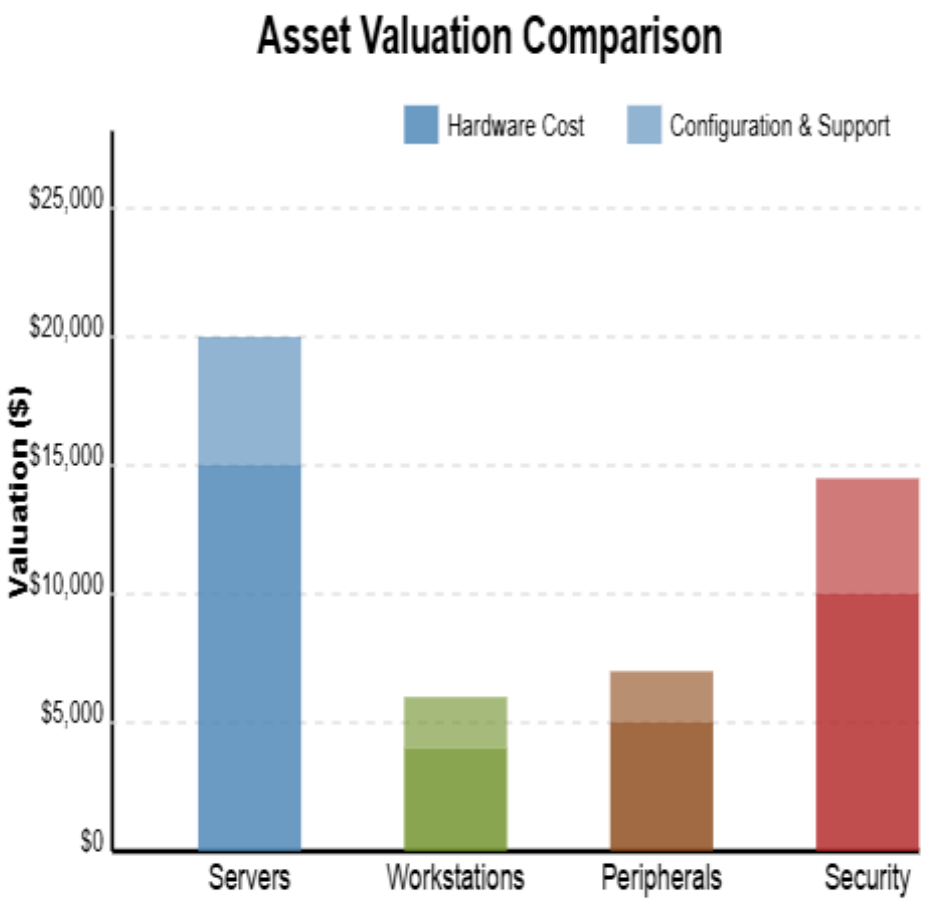

Figure 1.2: Comparative Asset Valuation Across Infrastructure Categories

Chapter 2

Threat Landscape

This chapter identifies and categorizes potential threats to the IT subnet infrastructure, providing a comprehensive overview of risks that could impact operations, data integrity, and system availability.

2.1 Key Threat Analysis

Table 2.1: Key Threat Analysis Summary

Threat	Likelihood	Impact	Risk Score	Description
Ransomware	4	5	20	Data encryption, operational halt, financial loss
Social Engineering	4	5	20	Credential theft, phishing, systems compromise
Unpatched Systems	4	5	20	Vulnerability exploitation, system compromise
SQL Injection	3	5	15	Database compromise, data theft
DDoS Attacks	4	3	12	Service disruption, customer frustration
Hardware Failure	3	4	12	Component malfunction, data loss

Worst Case Scenario

Complete encryption of all systems, data loss, and extended downtime (3-7 days), resulting in financial losses exceeding $100,000 and significant reputation damage.

2.2 External Cyber Threats

2.2.1 Ransomware

- **Threat Pattern:** Increasingly sophisticated attacks targeting organizations of all sizes
- **Impact:** Data encryption, operational disruption, potential data exfiltration
- **Worst Case:** Complete enterprise encryption requiring ransom payment or lengthy recovery
- **Recent Trend:** Double-extortion tactics where attackers both encrypt data and threaten to publish

2.2.2 SQL Injection & Web Application Attacks

- **Threat Pattern:** Exploitation of input validation flaws in web applications
- **Impact:** Unauthorized database access, credential theft, data exfiltration
- **Worst Case:** Complete compromise of customer and financial records
- **Recent Trend:** Automated scanning tools making these attacks more prevalent

2.2.3 DDoS Attacks

- **Threat Pattern:** Volumetric attacks designed to overwhelm network resources
- **Impact:** Service unavailability, customer frustration, reputation damage
- **Worst Case:** Sustained multi-vector attack lasting several days
- **Recent Trend:** Increasing attack sizes due to IoT botnets and amplification techniques

2.3 Internal Threats

2.3.1 Accidental Data Exposure

- **Threat Pattern:** Unintended sharing or misconfiguration of access controls
- **Impact:** Sensitive data exposure, compliance violations, reputation damage
- **Worst Case:** Large-scale exposure of PII or financial data
- **Recent Trend:** Increasing risk due to remote work environments

2.3.2 Shadow IT

- **Threat Pattern:** Unauthorized software, cloud services, or devices
- **Impact:** Unmanaged security risk, data leakage, compliance violations
- **Worst Case:** Sensitive data stored on unsecured third-party platforms
- **Recent Trend:** Growth in SaaS adoption without IT oversight

2.4 Physical Threats

2.4.1 Hardware Failure

- **Threat Pattern:** Component degradation, power issues, manufacturing defects
- **Impact:** Service disruption, data loss if redundancy is insufficient
- **Worst Case:** Cascading failure affecting multiple systems simultaneously
- **Recent Trend:** Supply chain issues affecting replacement part availability

2.4.2 Power Outages & Environmental Issues

- **Threat Pattern:** Utility failures, weather events, HVAC malfunctions
- **Impact:** Service disruption, potential hardware damage
- **Worst Case:** Extended outage with generator failure
- **Recent Trend:** Increasing frequency of extreme weather events

Chapter 3

Detailed Mitigation Strategies

This chapter outlines specific, actionable steps to address identified risks, with detailed cost-benefit analysis for each recommendation.

3.1 Critical Infrastructure Protections

Table 3.1: Critical Infrastructure Protection Strategies

Mitigation	Cost	Implementation Timeframe	Risk Reduction	ROI
Implement Redundant Failover Servers	$10,000-$15,000	1-2 months	80% downtime reduction	High
Enhance Firewall & IDS Rules	$5,000-$8,000	2-4 weeks	70% intrusion reduction	High
Implement Off-Site, Air-Gapped Backups	$3,000-$6,000	1 month	90% data loss reduction	Very High
Deploy Network Segmentation	$7,000-$12,000	2-3 months	65% lateral movement reduction	Medium

3.1.1 Redundant Failover Server Implementation

- **Current Vulnerability:** Single point of failure for critical payroll and web servers
- **Solution Details:**
  - Deploy high-availability clusters with automated failover
  - Implement real-time data replication between primary and secondary servers
  - Configure heartbeat monitoring and automated service migration
- **Expected Benefits:** Near-continuous uptime even during hardware failure or maintenance, with Recovery Time Objective (RTO) of ¡ 15 minutes

3.1.2 Enhanced Firewall & IDS Configuration

- **Current Vulnerability:** Basic firewall rules with minimal intrusion detection capabilities
- **Solution Details:**

  - Implement application-aware inspection for all traffic
  - Deploy behavioral analytics to identify suspicious patterns
  - Create granular rules based on least-privilege access principles
  - Enable real-time alerting for suspicious activities
- **Expected Benefits:** Significantly reduced risk of unauthorized access and early detection of potential breaches

3.1.3 Air-Gapped Backup Implementation

- **Current Vulnerability:** Backups vulnerable to same ransomware attacks as primary systems
- **Solution Details:**
  - Implement 3-2-1 backup strategy (3 copies, 2 different media, 1 off-site)
  - Create physically disconnected (air-gapped) backup copies
  - Establish write-once media backups for critical data
  - Institute regular backup verification and recovery testing
- **Expected Benefits:** Guaranteed recovery capability even in worst-case ransomware scenarios

3.2 Authentication & Access Controls

Table 3.2: Authentication & Access Control Strategies

Mitigation	Cost	Implementation Timeframe	Risk Reduction	ROI
Implement Multi-Factor Authentication	$2,000-$5,000	2-4 weeks	85% account compromise reduction	Very High
Privileged Access Management	$8,000-$15,000	2-3 months	75% privilege escalation reduction	High
Password Management System	$3,000-$6,000	1 month	60% credential attack reduction	Medium
Just-in-Time Access Provisioning	$6,000-$10,000	3-4 months	70% standing privilege reduction	Medium

3.2.1 Multi-Factor Authentication Deployment

- **Current Vulnerability:** Password-only authentication susceptible to credential theft
- **Solution Details:**
  - Deploy MFA for all critical systems, starting with administrative access
  - Implement a mix of authentication factors (something you know, have, and are)
  - Integrate with single sign-on (SSO) where possible to improve user experience
  - Enforce MFA for all remote access regardless of user level
- **Expected Benefits:** Near-elimination of risks from credential theft, phishing, and brute force attacks

3.3 Human Factors & Training

Table 3.3: Security Awareness and Training Strategies

Mitigation	Cost	Implementation Timeframe	Risk Reduction	ROI
Comprehensive Security Training Program	$1,500-$3,000 annually	Ongoing (quarterly)	70% social engineering reduction	Very High
Phishing Simulation Exercises	$2,000-$4,000 annually	Monthly	65% phishing susceptibility reduction	High
Security Champions Program	$1,000-$2,000 annually	2-3 months	50% security culture improvement	Medium

3.3.1 Security Awareness Program

- **Current Vulnerability:** Limited employee understanding of security threats and best practices
- **Solution Details:**
  - Develop role-based security training for different departments
  - Implement regular phishing simulations with targeted coaching
  - Create a security champions program to embed security culture
  - Establish clear incident reporting procedures with positive reinforcement
- **Expected Benefits:** Significant reduction in successful social engineering attacks and improved incident reporting

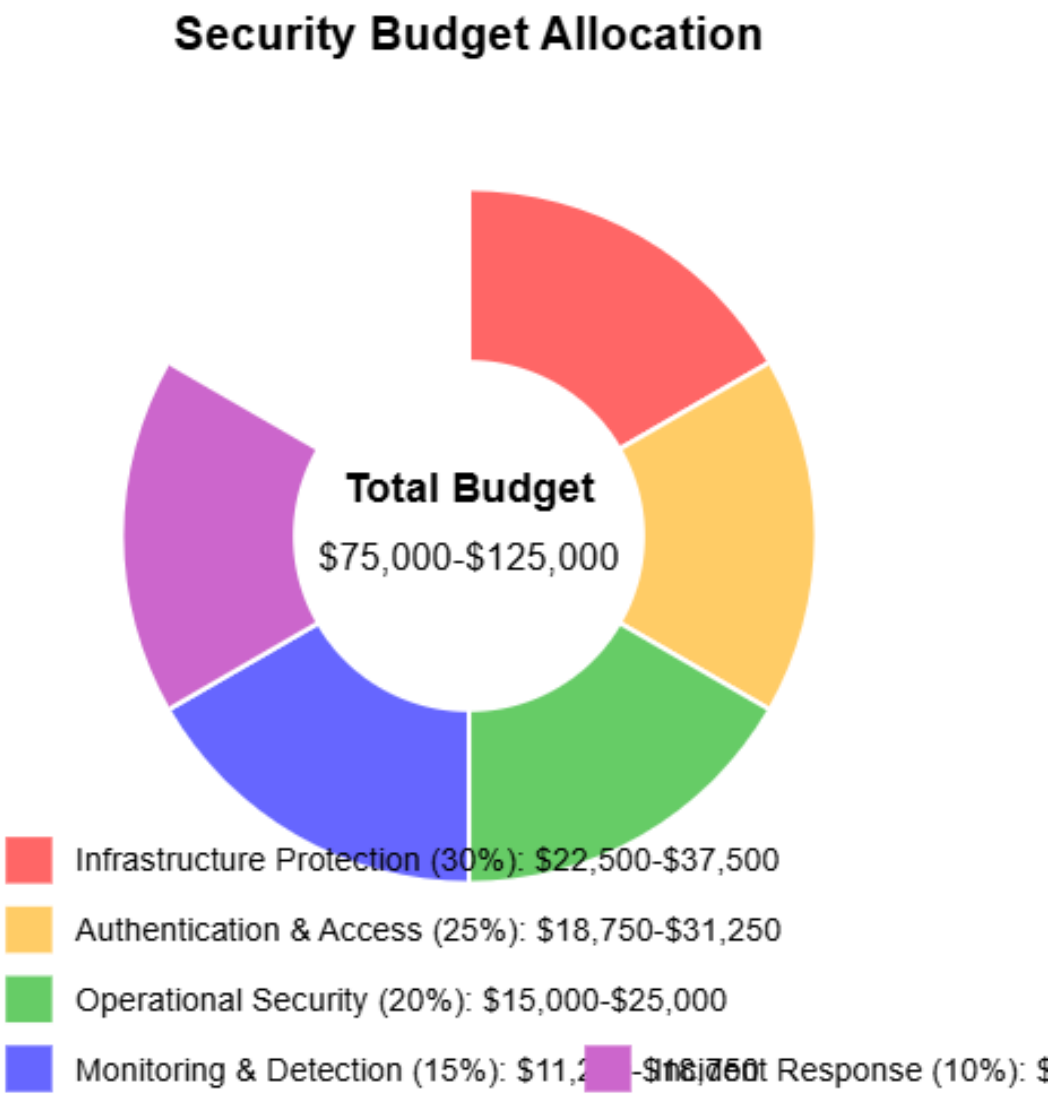

Figure 3.1: Security Budget Allocation by Category

Chapter 4

Specific Subnet Component Recommendations

This chapter provides tailored recommendations for each component of the IT subnet infrastructure, addressing the unique risks and requirements of each system type.

4.1 Payroll & Web Server Recommendations

Server Infrastructure Recommendations

1. **High-Availability Implementation**
   - Deploy redundant failover servers for both payroll and web systems ($10,000-$15,000)
   - Implement automated failover with minimal RTO (¡ 15 minutes)
   - Configure database replication with near-zero RPO for critical data
   - Establish regular failover testing schedule (monthly)
2. **Enhanced Security Measures**
   - Implement application firewalls for web services ($5,000-$8,000)
   - Deploy database activity monitoring with encryption for sensitive data
   - Enforce strong authentication (MFA) for all administrative access
   - Establish regular vulnerability scanning schedule (weekly)
3. **Robust Backup Strategy**
   - Implement 3-2-1 backup strategy with multiple recovery points
   - Configure automated backup verification and testing (weekly)
   - Establish off-site, air-gapped copies of critical financial data
   - Document comprehensive recovery procedures with clear roles

4.1.1 Detailed Technical Controls

- **Server Hardening:**
  - Remove unnecessary services and default accounts
  - Implement application whitelisting on server systems
  - Configure log forwarding to centralized SIEM solution

  - Establish file integrity monitoring for critical system files

- **Database Security:**
  - Implement column-level encryption for sensitive payroll data
  - Configure database firewalls with query analysis
  - Establish comprehensive auditing for all privileged operations
  - Deploy automated vulnerability scanning specific to DBMS

- **Web Application Security:**
  - Implement Web Application Firewall (WAF) with OWASP rule sets
  - Conduct regular application code reviews and penetration testing
  - Deploy Content Security Policy (CSP) and other security headers
  - Configure TLS 1.3 with forward secrecy and certificate monitoring

4.2 Employee Workstation Recommendations

Endpoint Security Recommendations

1. **Endpoint Protection Platform**
   - Deploy next-generation antivirus with behavioral analysis ($3,000+ annually)
   - Implement application control and device usage policies
   - Configure Data Loss Prevention (DLP) for sensitive information
   - Establish centralized monitoring and alerting
2. **Authentication & Access Controls**
   - Enforce MFA for all system and application access ($2,000 one-time setup)
   - Implement strong password policies with management solution
   - Configure automatic screen locking and session timeouts
   - Establish least-privilege access model for all user accounts
3. **User Awareness & Training**
   - Conduct regular phishing simulation exercises ($1,500 annually)
   - Provide role-based security training for different departments
   - Establish clear reporting procedures for suspicious activities
   - Develop security champions program across departments

4.2.1 Detailed Technical Controls

- **Endpoint Hardening:**
  - Disable unnecessary operating system features and services
  - Configure host-based firewalls with application control

  - Implement drive encryption for all endpoint devices
  - Establish automated configuration management and drift detection

- **Remote Work Security:**
  - Deploy secure VPN solution with MFA and split tunneling
  - Implement conditional access policies based on device health
  - Configure secure remote desktop protocols with encryption
  - Establish mobile device management for company-owned devices

- **Data Protection:**
  - Implement document and email classification system
  - Configure DLP policies for various data types and channels
  - Deploy secure file sharing solution with access controls
  - Establish regular data handling training for all employees

4.3 Printer & Network Peripheral Recommendations

Network Peripheral Recommendations

1. **Printer Security Enhancements**
   - Change all default credentials on network printers ($0 cost)
   - Implement firmware update procedures and tracking ($1,000 annually)
   - Configure secure printing with user authentication
   - Disable unused services and protocols (FTP, Telnet)
2. **Network Segmentation**
   - Segregate printers onto a separate VLAN ($500 setup cost)
   - Implement ACLs to restrict printer communication
   - Configure network monitoring for printer traffic analysis
   - Establish secure printing protocols (IPP over HTTPS)
3. **Data Protection Measures**
   - Enable disk wiping for printer/copier internal storage
   - Configure document logging and auditing capabilities
   - Implement pull printing to prevent document abandonment
   - Establish regular security reviews of printer configurations

4.3.1 Detailed Technical Controls

- **Printer Hardening:**
  - Disable unused physical ports (USB, SD card)

  - Configure strong encryption for stored data
  - Implement secure boot and firmware validation
  - Establish centralized printer management console

- **Print Server Security:**
  - Harden print server operating system
  - Configure secure communication between clients and print server
  - Implement printer driver whitelisting
  - Establish comprehensive logging of print jobs

- **Document Security:**

- **Document Security:**
  - Configure document watermarking for sensitive materials
  - Implement print job encryption from endpoint to printer
  - Deploy DLP integration with multifunction devices
  - Establish user training for handling printed confidential information

Chapter 5

Risk Matrix & Prioritization

Based on the comprehensive analysis of threats, vulnerabilities, and potential impacts, this chapter provides a structured approach to prioritizing risk mitigation efforts.

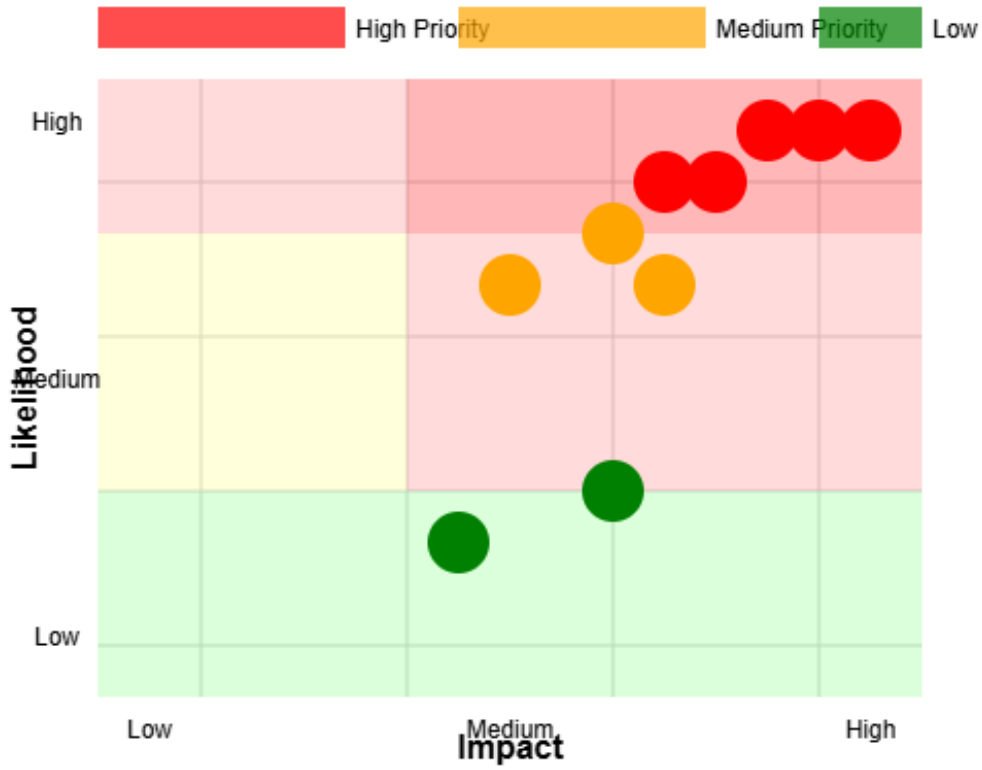

Figure 5.1: Risk Matrix for IT Subnet

5.1 High Priority Risks (Address within 0-3 months)

Priority 1 Mitigation Actions

1. **Ransomware protection** (Risk Score: 20)
   - Implementation of robust endpoint protection
   - Email filtering and attachment scanning
   - Regular backup verification procedures
2. **Security awareness program** (Risk Score: 20)
   - Comprehensive training for all employees
   - Phishing simulation exercises
   - Clear reporting procedures for security incidents
3. **System patching automation** (Risk Score: 20)
   - Centralized patch management system
   - Regular vulnerability scanning
   - Defined patching schedule with emergency procedures
4. **Firewall rule enhancement** (Risk Score: 16)
   - Audit and cleanup of existing rules
   - Implementation of least-privilege access
   - Regular rule review procedures
5. **Multi-factor authentication** (Risk Score: 16)
   - Deployment across all critical systems
   - Integration with single sign-on where possible
   - User training and support

5.2 Medium Priority Risks (Address within 3-6 months)

Priority 2 Mitigation Actions

1. **Backup implementation** (Risk Score: 15)
   - Implementation of 3-2-1 backup strategy
   - Regular testing of restore procedures
   - Offline backup storage solutions
2. **SQL injection prevention** (Risk Score: 15)
   - Web application security review
   - Implementation of input validation
   - Database access restriction
3. **Password management** (Risk Score: 15)
   - Enterprise password management solution
   - Strong password policy enforcement
   - Regular password audits
4. **DDoS protection** (Risk Score: 12)
   - Cloud-based DDoS mitigation service
   - Traffic pattern monitoring
   - Incident response procedures
5. **Monitoring implementation** (Risk Score: 12)
   - Centralized logging solution
   - Alerting for suspicious activities
   - Regular log review procedures

5.3 Lower Priority Risks (Address within 6-12 months)

Priority 3 Mitigation Actions

1. **Advanced persistent threat protection** (Risk Score: 10)
   - Enhanced network monitoring
   - Behavioral analysis tools
   - Threat intelligence integration
2. **Physical security enhancements** (Risk Score: 8)
   - Access control system upgrades
   - Video surveillance improvements
   - Environmental monitoring systems
3. **API security** (Risk Score: 9)
   - API gateway implementation
   - Rate limiting and throttling
   - Authentication and authorization review
4. **Change management procedures** (Risk Score: 9)
   - Formal change approval process
   - Configuration management database
   - Post-implementation reviews

Chapter 6

Implementation Roadmap

This chapter provides a detailed, phased approach to implementing the recommended security enhancements, ensuring a manageable and prioritized deployment strategy.

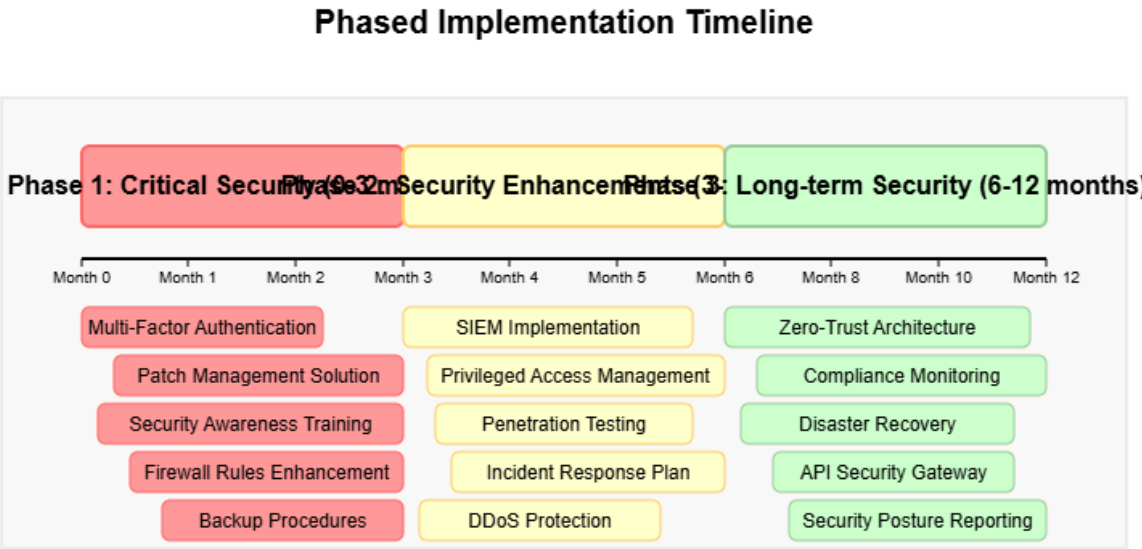

Figure 6.1: Phased Implementation Timeline Overview

6.1 Phase 1: Critical Security Controls (0-3 months)

Phase 1 Implementation

1. **Deploy Multi-Factor Authentication** across all critical systems
   - Week 1-2: Select MFA solution and develop deployment plan
   - Week 3-6: Pilot deployment for IT staff and administrators
   - Week 7-12: Organization-wide deployment with user training
   - **Key Deliverable:** 100% MFA coverage for critical systems
2. **Implement automated patch management solution**
   - Week 1-4: Solution selection and server deployment
   - Week 5-8: Agent deployment and testing
   - Week 9-12: Full implementation and policy development
   - **Key Deliverable:** Automated patch compliance reporting with 98% target
3. **Conduct initial security awareness training**
   - Week 1-2: Content development and platform selection
   - Week 3-4: Executive and IT staff training sessions
   - Week 5-12: Department-by-department training rollout
   - **Key Deliverable:** 100% employee completion of foundational security training
4. **Enhance firewall rules and segmentation**
   - Week 1-3: Audit existing rules and identify gaps
   - Week 4-6: Develop enhanced ruleset and segmentation plan
   - Week 7-12: Implement changes during maintenance windows
   - **Key Deliverable:** Network segmentation with critical systems isolated
5. **Establish backup procedures with off-site storage**
   - Week 1-4: Solution selection and initial implementation
   - Week 5-8: Test backup and recovery procedures
   - Week 9-12: Documentation and process integration
   - **Key Deliverable:** 3-2-1 backup strategy with verified recovery capability

6.2 Phase 2: Security Enhancements (3-6 months)

Phase 2 Implementation

1. **Deploy SIEM solution for enhanced monitoring**
   - Month 1: Requirements gathering and solution selection
   - Month 2: Initial deployment and configuration
   - Month 3: Alert tuning and integration with existing systems
   - **Key Deliverable:** Centralized security monitoring with customized alerting
2. **Implement privileged access management**
   - Month 1: Solution selection and architecture design
   - Month 2: Initial deployment for administrative accounts
   - Month 3: Complete integration and policy enforcement
   - **Key Deliverable:** Just-in-time privileged access with full auditing
3. **Conduct initial penetration testing**
   - Month 1: Vendor selection and scope definition
   - Month 2: Test execution and preliminary findings
   - Month 3: Remediation planning and implementation
   - **Key Deliverable:** Vulnerability assessment with prioritized remediation plan
4. **Establish formal incident response procedures**
   - Month 1: Procedure development and team formation
   - Month 2: Initial training and tabletop exercises
   - Month 3: Full-scale incident simulation and refinement
   - **Key Deliverable:** Documented IR plan with defined roles and procedures
5. **Implement DDoS protection measures**
   - Month 1: Solution evaluation and selection
   - Month 2: Implementation planning and initial configuration
   - Month 3: Full deployment and testing
   - **Key Deliverable:** Automated DDoS mitigation for public-facing services

6.3 Phase 3: Long-term Security Posture (6-12 months)

Phase 3 Implementation

1. **Implement zero-trust architecture components**
   - Month 1-2: Architecture design and planning
   - Month 3-4: Initial component deployment
   - Month 5-6: Policy development and enforcement
   - **Key Deliverable:** Micro-segmentation with least-privilege access
2. **Establish continuous compliance monitoring**
   - Month 1-2: Compliance requirements mapping
   - Month 3-4: Monitoring tool selection and implementation
   - Month 5-6: Reporting and remediation process establishment
   - **Key Deliverable:** Automated compliance dashboard with remediation workflow
3. **Develop comprehensive disaster recovery solution**
   - Month 1-2: Solution design and infrastructure requirements
   - Month 3-4: Initial implementation and configuration
   - Month 5-6: Testing and documentation
   - **Key Deliverable:** Tested DR plan with RPO/RTO metrics achieved
4. **Implement API security gateway**
   - Month 1-2: API inventory and risk assessment
   - Month 3-4: Gateway selection and deployment
   - Month 5-6: Policy enforcement and monitoring integration
   - **Key Deliverable:** Centralized API control with security monitoring
5. **Establish regular security posture reporting**
   - Month 1-2: Metrics identification and data collection methods
   - Month 3-4: Dashboard development and initial reporting
   - Month 5-6: Process integration and automation
   - **Key Deliverable:** Executive-level security posture reporting

Chapter 7

Return on Investment Analysis

This chapter evaluates the financial justification for the proposed security investments, analyzing both quantitative and qualitative benefits of risk reduction.

7.1 Cost-Benefit Analysis

Table 7.1: Security Investment Cost-Benefit Analysis

Risk Category	Potential Loss	Mitigation Cost	ROI Ratio
Ransomware Attack	$100,000-$250,000	$15,000-$25,000	5:1 to 10:1
Data Breach	$150,000-$350,000	$25,000-$40,000	4:1 to 8:1
Business Disruption	$5,000-$15,000 per day	$20,000-$30,000	3:1 to 7:1
Regulatory Penalties	$50,000-$100,000	$15,000-$30,000	2:1 to 5:1
Total	**$305,000-$715,000**	**$75,000-$125,000**	**3:1 to 7:1**

7.1.1 Financial Impact Analysis

The proposed security investments of $75,000-$125,000 represent a significant commitment but offer compelling ROI when compared to potential losses:

- **Ransomware Impact:** A single successful ransomware attack can cost the organization $100,000-$250,000 when accounting for ransom payment, business disruption, recovery efforts, and reputation damage.
- **Data Breach Costs:** The average cost of a data breach involving sensitive information is estimated at $150,000-$350,000, including investigation, notification, legal expenses, and customer retention efforts.
- **Operational Disruption:** Server outages can cost $5,000-$15,000 per day in lost productivity and business opportunities, with recovery times potentially extending to 3-7 days without proper preparations.
- **Compliance Penalties:** Regulatory fines for inadequate security measures can reach $50,000-$100,000 depending on the nature of the violation and applicable regulations.

7.1.2 Intangible Benefits

Beyond direct financial calculations, the security program delivers significant intangible benefits:

- **Enhanced Reputation:** Demonstrable security practices build customer and partner trust
- **Competitive Advantage:** Security capabilities increasingly factor into business relationships
- **Operational Efficiency:** Improved monitoring and automation reduce manual security efforts
- **Employee Confidence:** Security training and clear procedures improve workforce confidence

7.2 Investment Prioritization Strategy

The implementation roadmap prioritizes investments to maximize return and reduce critical risks first:

1. **Phase 1 Focus:** High-impact, low-cost solutions with immediate risk reduction
    - Multi-factor authentication offers 85% reduction in account compromise risk for relatively low investment
    - Security awareness training provides substantial social engineering protection with minimal expenditure
    - Backup implementation offers critical ransomware protection at modest cost
2. **Phase 2 Focus:** Building on foundational controls with specialized security
    - Privileged access management addresses high-impact administrative account risks
    - SIEM implementation improves detection capabilities across all security domains
    - DDoS protection addresses specific business continuity threats to web systems
3. **Phase 3 Focus:** Long-term security posture enhancement
    - Zero-trust architecture represents strategic security maturity evolution
    - Comprehensive disaster recovery addresses low-frequency, high-impact scenarios
    - Security posture reporting provides governance and continuous improvement framework

Chapter 8

Conclusion and Executive Recommendations

This comprehensive risk assessment has identified significant vulnerabilities within the organization's IT subnet infrastructure. By implementing the proposed mitigation strategies according to the prioritized roadmap, the organization can substantially reduce its risk exposure and enhance its overall security posture.

8.1 Key Findings

1. **Critical Vulnerabilities:** The assessment identified several high-priority vulnerabilities that require immediate attention:
    - Inadequate protection against ransomware and other advanced threats
    - Insufficient backup and recovery capabilities
    - Limited security awareness among personnel
    - Weak authentication mechanisms for critical systems
    - Inadequate network segmentation and firewall configurations
2. **Substantial Risk Exposure:** The organization faces potential financial impact exceeding $250,000 from a single significant security incident, not including reputational damage and operational disruption.
3. **Positive ROI:** The proposed security investments of $75,000-$125,000 (phased over 12 months) represent a prudent allocation with ROI ratios between 3:1 and 7:1 when compared to potential losses.
4. **Achievable Implementation:** The phased approach provides a realistic and manageable path to enhanced security without overwhelming resources or operations.

8.2 Strategic Recommendations

Executive Recommendations

1. **Adopt a Defense-in-Depth Strategy**
   - Implement multiple layers of security controls
   - Focus on both prevention and detection capabilities
   - Address technical, operational, and human factors
2. **Prioritize Based on Risk**
   - Begin with high-impact, low-complexity solutions
   - Address critical vulnerabilities within first 90 days
   - Continuously reassess risk posture as controls are implemented
3. **Develop Security Culture**
   - Invest in comprehensive security awareness training
   - Establish clear security policies and procedures
   - Foster a culture where security is everyone's responsibility
4. **Implement Continuous Monitoring**
   - Deploy robust detection and response capabilities
   - Establish regular security assessments and testing
   - Maintain visibility into emerging threats and vulnerabilities
5. **Prepare for Incidents**
   - Develop and test incident response procedures
   - Ensure business continuity and disaster recovery capabilities
   - Establish clear communication protocols for security events

8.3 Final Remarks

The recommended approach employs defense-in-depth principles, addressing technical, operational, and human factors that contribute to cybersecurity risk. This balanced strategy ensures not only protection against current threats but also establishes a foundation for addressing emerging challenges in the evolving threat landscape.

By adopting these recommendations, the organization will:

- Significantly reduce the likelihood and impact of security incidents
- Ensure operational resilience and business continuity
- Protect sensitive data and maintain stakeholder trust
- Demonstrate commitment to security best practices

- Build a sustainable security program that evolves with the threat landscape

Security is not a one-time project but an ongoing process that requires continuous attention and improvement. This assessment provides a roadmap for establishing a robust security foundation that can be built upon as the organization's security maturity increases.

Appendix A

Risk Assessment Methodology

A.1 Risk Calculation Formula

The risk scores throughout this assessment were calculated using the following formula:

Risk Calculation Formula

Risk Score = Threat Likelihood × Vulnerability Severity × Asset Value

Where:

- **Threat Likelihood:** Probability of a threat occurring (1-5 scale)
  - 1 = Rare: May occur only in exceptional circumstances
  - 2 = Unlikely: Could occur at some time, but not expected
  - 3 = Possible: Might occur at some time
  - 4 = Likely: Will probably occur in most circumstances
  - 5 = Almost Certain: Expected to occur in most circumstances
- **Vulnerability Severity:** Impact if exploited (1-5 scale)
  - 1 = Negligible: Minimal impact, easily addressed
  - 2 = Minor: Minor impact, straightforward resolution
  - 3 = Moderate: Significant impact requiring resources to address
  - 4 = Major: Major impact affecting operations and requiring substantial resources
  - 5 = Critical: Severe impact threatening organization viability
- **Asset Value:** Importance to operations (1-5 scale)
  - 1 = Low: Non-critical asset with limited operational impact
  - 2 = Moderate-Low: Asset with limited operational impact
  - 3 = Moderate: Important asset affecting operations
  - 4 = Moderate-High: Critical asset with significant operational dependency
  - 5 = High: Mission-critical asset essential to operations

This produces a risk score between 1 and 125, categorized as follows:

- **Low Risk:** 1-25
- **Medium Risk:** 26-75
- **High Risk:** 76-125

A.2 Data Collection Methods

Information for this assessment was gathered through:

- Infrastructure scan and inventory of all subnet components
- Stakeholder interviews with IT staff and department heads
- Technical documentation review of existing systems
- Vulnerability scanning tools applied to representative systems
- Industry benchmark comparisons with similar organizations
- Review of previous incident reports and security logs

A.3 Assessment Scope

The assessment specifically focused on the following components:

- Payroll systems and associated databases
- Web servers and public-facing applications
- Employee workstations (Windows and Mac systems)
- Mobile devices managed by the organization
- Network infrastructure (switches, routers, firewalls)
- Network peripherals (printers, scanners, multifunction devices)
- Data storage and transmission systems

Appendix B

References

1. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, 2018.
2. International Organization for Standardization, "ISO/IEC 27001:2013 - Information Security Management," 2013.
3. SANS Institute, "Critical Security Controls," Version 8, 2021.
4. M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 6th ed. Boston, MA: Cengage Learning, 2018.
5. ISACA, "COBIT 2019 Framework: Introduction and Methodology," 2019.
6. Cloud Security Alliance, "Cloud Controls Matrix v4.0," 2021.
7. D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security*, 4th ed. Burlington, MA: Jones & Bartlett Learning, 2020.
8. MITRE, "ATT&CK Framework," 2021. [Online]. Available: https://attack.mitre.org/
9. NIST Special Publication 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations," 2020.
10. Center for Internet Security, "CIS Controls v8," 2021.

Appendix C

Summary of Mitigation Costs

Table C.1: Summary of Key Mitigation Costs

Mitigation Strategy	**Cost Range**	**Implementation Time**	**ROI**
Multi-Factor Authentication	$2,000-$5,000	2-4 weeks	Very High
Security Awareness Training	$1,500-$3,000/yr	Ongoing (quarterly)	Very High
Automated Patch Management	$4,000-$8,000	1-2 months	High
Enhanced Firewall & IDS Rules	$5,000-$8,000	2-4 weeks	High
Off-Site, Air-Gapped Backups	$3,000-$6,000	1 month	Very High
Network Segmentation	$7,000-$12,000	2-3 months	Medium
SIEM Implementation	$15,000-$25,000	3-6 months	Medium-High
Penetration Testing	$10,000-$15,000/yr	Bi-annual	Medium
Total Estimated Cost	**$75,000-$125,000**	**12 months (phased)**	