Security Roadmap

Organization: Susan Mills LLC

Document Purpose

This Security Roadmap outlines the strategic, phased approach Susan Mills LLC will take to implement a formal cybersecurity program. The roadmap translates the findings from Stage 1 (Business Impact Assessment, Risk Assessment, and Gap Analysis) and Phase 2 planning activities into a clear, justified, and time-bound implementation plan. Its primary purpose is to ensure that new security controls are deployed in a controlled manner that reduces business risk, avoids scope creep, and delivers measurable improvements to the firm's security posture.

This roadmap is intended for use by the business owner, employees, the external IT consultant, and any future stakeholders involved in the governance of the cybersecurity program.

Organizational Context

Susan Mills LLC is a small accounting firm with five employees operating in a hybrid work environment. Employees use Windows laptops and access a mix of local and cloud-based applications that process sensitive financial and tax data for small business clients.

Key Risk Drivers Identified in Stage 1

- **Lack of centralized device management**: Employees have full administrative control over company laptops.
- **Weak identity and access controls**: No enforced MFA or centralized identity lifecycle management.
- **Limited visibility and monitoring**: No consistent way to assess device security posture or user authentication risk.
- **Hybrid workforce exposure**: Devices routinely operate outside the trusted office network.
- **Client data sensitivity**: High confidentiality requirements due to financial and tax records.

The Risk Assessment concluded that the likelihood of account compromise, data leakage, and regulatory exposure was **medium to high**, while the potential business impact was **high**, including reputational damage, loss of client trust, and potential legal or regulatory penalties.

Roadmap Overview

The Security Roadmap follows a three-phase, top-down approach:

- **Phase 1: Foundations** – Establish core identity, device, and network security infrastructure.
- **Phase 2: Standardization** – Enforce consistent security controls across all users and devices.

- **Phase 3: Optimization** – Fine-tune controls, improve visibility, and reduce residual risk.

Each phase builds on the previous one, ensuring that foundational controls are in place before more granular optimizations are attempted.

Phase 1: Foundations

Objective

Establish centralized identity, device management, and secure network access as the foundation of the cybersecurity program.

Projects and Controls

1. **Microsoft Entra ID Deployment**
2. Centralized cloud-based identity provider
3. Creation of managed user accounts for all employees
4. **Multi-Factor Authentication (MFA)**
5. Microsoft Authenticator app required for all user logins
6. **Microsoft Intune Configuration**
7. Enrollment of all company-owned Windows laptops
8. Establishment of baseline device compliance policies
9. **802.1X Network Authentication**
10. Deployment of secure Wi-Fi authentication using RADIUS
11. Integration of RADIUS with Entra ID for credential-based access

Why These Controls Are Needed

- Addresses the highest-risk gap identified: unmanaged identities and devices
- Reduces the likelihood of credential theft leading to unauthorized access
- Prevents unmanaged or compromised devices from accessing internal resources

Scope

- **Users**: All five employees
- **Devices**: All company-owned Windows laptops
- **Systems**: Microsoft 365, cloud applications, and internal Wi-Fi network

Responsibilities

- **Business Owner (Susan Mills)**: Executive sponsor and approval authority
- **IT Consultant**: Technical implementation and configuration
- **Employees**: Device enrollment and MFA adoption

Major Requirements

- Microsoft 365 Business Premium (or equivalent) licensing
- Employee training on MFA and device enrollment
- RADIUS-capable network equipment

Timeline

- Estimated duration: 4–6 weeks

Business Improvements

- Centralized control of identities and devices
- Immediate reduction in account compromise risk
- Clear ownership and visibility over company assets

Phase 2: Standardization

Objective

Ensure consistent application of security controls across all users, devices, and access scenarios.

Projects and Controls

1. **Conditional Access Policies**
2. Enforce MFA based on user risk, device compliance, and location
3. Block access from non-compliant or unmanaged devices
4. **Standardized Device Configuration Policies**
5. Enforced OS updates and security patches
6. Standardized antivirus and endpoint protection settings
7. **Least Privilege Enforcement**
8. Removal of local administrator rights from standard users
9. Use of role-based access where elevated privileges are required

Why These Controls Are Needed

- Reduces inconsistent security practices across employees
- Limits the damage caused by compromised accounts or malware
- Aligns security enforcement with real-world risk conditions

Scope

- **Users**: All employees
- **Devices**: All Intune-enrolled laptops
- **Access Scenarios**: Office network, home networks, and cloud services

Responsibilities

- **IT Consultant**: Policy design and rollout
- **Business Owner**: Approval of access rules that impact workflows
- **Employees**: Adoption of standardized workflows

Major Requirements

- Well-defined access requirements for each role
- User communication and change management
- Testing period to avoid business disruption

Timeline

- Estimated duration: 4 weeks following Phase 1

Business Improvements

- Predictable and enforceable security posture
- Reduced attack surface across devices
- Improved compliance with client confidentiality expectations

---

Phase 3: Optimization

Objective

Refine security controls, improve monitoring, and reduce residual risk through targeted adjustments.

Projects and Controls

1. **Advanced Conditional Access Tuning**
2. Fine-grained rules based on sign-in risk
3. Session controls for sensitive applications
4. **Network Access Optimization**

5. MAC address controls where appropriate
6. Port security and logging on network equipment
7. **Security Monitoring and Review Processes**
8. Regular review of sign-in logs and device compliance reports
9. Periodic access reviews for users and devices

Why These Controls Are Needed

- Addresses edge cases not covered by baseline policies
- Improves detection of suspicious behavior
- Ensures the security program remains effective over time

Scope

- **Systems**: Entra ID, Intune, network infrastructure
- **Users**: All employees, with emphasis on higher-risk access scenarios

Responsibilities

- **IT Consultant**: Initial tuning and documentation
- **Business Owner**: Ongoing oversight and review cadence

Major Requirements

- Defined metrics for success (e.g., failed logins, non-compliant devices)
- Scheduled review meetings

Timeline

- Estimated duration: 2–3 weeks, then ongoing

Business Improvements

- Reduced false positives and user friction
- Better visibility into security risks
- Long-term sustainability of the cybersecurity program

Risk Mapping Summary

Identified Risk	Likelihood	Impact	Mitigating Controls
Credential theft	High	High	MFA, Conditional Access
Unmanaged devices	Medium	High	Intune enrollment, compliance policies

Identified Risk	Likelihood	Impact	Mitigating Controls
Unauthorized network access	Medium	Medium	802.1X with RADIUS
Data breach	Medium	High	Identity controls, device compliance

This mapping demonstrates how each major control directly reduces one or more high-priority risks identified in Stage 1.

Conclusion

This Security Roadmap provides Susan Mills LLC with a clear, phased path from an ad hoc security posture to a managed, risk-based cybersecurity program. By prioritizing foundational identity and device controls, standardizing enforcement, and then optimizing over time, the firm can significantly reduce its exposure to cyber threats while maintaining operational efficiency. The roadmap also provides the justification needed to explain costs and changes to stakeholders in clear business risk terms, ensuring long-term support and success.