Sample Supply Chain Risk Management (SCRM) Plan

Introduction

ABC Telecom recognizes the critical importance of supply chain risk management (SCRM) in ensuring the security, integrity, and resilience of its operations. This SCRM plan is based on guidance from NISTIR 8276, "Key Practices in Cyber Supply Chain Risk Management," and NIST SP 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." The plan outlines a proactive approach to identifying, assessing, mitigating, and monitoring risks across our supply chain.

Purpose

The purpose of this plan is to integrate cybersecurity risk management into ABC Telecom's procurement, vendor management, and operations processes to safeguard critical assets and services from potential supply chain threats.

Scope

This plan applies to all ABC Telecom business units, departments, and third-party suppliers involved in the design, manufacture, distribution, and management of hardware, software, and services. The plan covers:

- Information and communication technologies (ICT) supply chain
- Procurement and vendor management
- Cybersecurity risk related to products, services, and software

Key SCRM Objectives

1. **Ensure Continuity and Resilience**: Ensure operational continuity through robust supply chain risk mitigation strategies.
2. **Cybersecurity Integration**: Embed cybersecurity throughout the supply chain lifecycle.
3. **Transparency and Accountability**: Enhance visibility into the supply chain to ensure trust, accountability, and compliance.

Key Practices Based on NISTIR 8276

1. **Identify Critical Assets and Suppliers**
   - **Objective**: Identify and prioritize critical assets and the suppliers that provide these assets.
   - **Implementation**: Conduct a comprehensive asset inventory that categorizes critical hardware, software, and services. Identify key suppliers that provide these assets and evaluate their criticality to operations.
2. **Develop Supplier Risk Profiles**
   - **Objective**: Assess and categorize supplier risks based on their potential to impact ABC Telecom.
   - **Implementation**: Use a tiered risk assessment model, identifying suppliers based on their cybersecurity posture, regulatory compliance, and the criticality of the products/services they provide. Assign risk profiles based on factors like geographic risk, financial health, and reliance on third-party vendors.
3. **Engage in Risk-Aware Procurement**
   - **Objective**: Integrate cybersecurity risk assessments into the procurement process.
   - **Implementation**: Establish cybersecurity-specific criteria for selecting vendors and partners. Ensure contracts include clauses that require vendors to follow secure development, incident reporting, and compliance with cybersecurity regulations.
4. **Continuous Monitoring and Threat Intelligence Sharing**
   - **Objective**: Continuously monitor the supply chain for emerging threats and vulnerabilities.
   - **Implementation**: Collaborate with industry peers, government agencies, and information-sharing organizations (e.g., ISACs) to stay informed about current threats and supply chain risks. Implement monitoring mechanisms for real-time visibility into supplier activities and any breaches.
5. **Establish a Response and Recovery Plan**
   - **Objective**: Develop incident response and recovery capabilities tailored to supply chain threats.
   - **Implementation**: Ensure response plans address supplier-related incidents and include clear communication channels with critical suppliers during an incident. Test recovery procedures regularly and conduct post-incident reviews to strengthen supply chain defenses.

NIST SP 800-161 Integration

The SCRM plan aligns with the guidance provided in NIST SP 800-161 to ensure a secure and resilient supply chain for federal and non-federal entities. Key focus areas include:

1. **Risk Identification**
   - **Threat Modeling**: Apply threat modeling techniques to identify potential cyber risks within the supply chain. This includes evaluating vendor software and hardware for backdoors, unpatched vulnerabilities, and potential data leaks.
   - **Supplier Risk Assessments**: Leverage NIST's risk assessment frameworks to evaluate suppliers' cybersecurity capabilities, using both qualitative and quantitative metrics.
2. **Risk Response**
   - **Mitigation Strategies**: Develop and implement specific strategies to mitigate identified risks. For example, require suppliers to follow secure software development practices or mandate regular audits of their cybersecurity controls.
   - **Risk Transfer**: In cases where certain risks cannot be completely mitigated, utilize cyber insurance or legal agreements to transfer or share risks with suppliers.
3. **Security Controls Implementation**
   - **Supply Chain Mapping**: Develop a detailed map of all suppliers and their associated products and services. Understand each tier in the supply chain and assess potential security weaknesses at each stage.
   - **Security Standards Compliance**: Ensure that suppliers comply with relevant cybersecurity standards such as ISO 27001, SOC 2, and NIST SP 800-53.
4. **Third-Party Vendor Management**
   - **Supplier Audits**: Conduct regular audits of critical suppliers to ensure compliance with ABC Telecom's cybersecurity requirements. Establish a vendor performance review process to assess ongoing risk and compliance.
   - **Vendor Cyber Hygiene Requirements**: Require vendors to implement and maintain strong cybersecurity hygiene practices. This includes regular patch management, access control enforcement, and employee security training.
5. **Incident Handling and Reporting**
   - **Communication Protocols**: Establish clear communication protocols for when an incident occurs that involves a supplier. Ensure timely reporting of incidents and breaches by suppliers.
   - **Collaborative Response**: Work closely with suppliers to manage the response to a cyber event, ensuring alignment on containment, mitigation, and recovery efforts.

Metrics and Monitoring

ABC Telecom will implement continuous monitoring tools and establish key performance indicators (KPIs) to measure the effectiveness of the SCRM program. KPIs may include:

- Number of third-party incidents per year
- Time taken to remediate supplier-related incidents
- Supplier compliance rates with security requirements
- Frequency of supplier audits and security reviews

Training and Awareness

To ensure successful implementation, all relevant employees and stakeholders will receive training on supply chain risk management practices. Training will cover:

- Understanding supply chain risks
- Incident reporting procedures
- Cybersecurity standards and compliance expectations for suppliers

Conclusion

ABC Telecom's SCRM plan aims to protect our operations and customers by effectively managing cybersecurity risks in the supply chain. This proactive approach, aligned with NIST guidance, will enable us to build a resilient supply chain while meeting regulatory and security requirements. Regular updates to the plan will ensure its relevance in a rapidly changing threat landscape.