Supply Chain Cybersecurity

This playbook outlines steps to manage and secure a company's supply chain against cyber threats. It is intended to protect sensitive information and infrastructure from potential breaches.

Step 1: **Assessment**

Evaluate your current supply chain for potential cyber vulnerabilities. This may involve mapping out the supply chain, identifying key assets, and categorizing suppliers based on their access to sensitive data or systems.

Step 2: **Standards**

Develop a set of cybersecurity standards and requirements that all suppliers must adhere to. These standards should be based on best practices and be appropriate for the level of risk each supplier represents.

Step 3: **Verification**

Require all suppliers to provide evidence that they meet your cybersecurity standards. This could involve third-party audits, certifications, or self-assessments.

Step 4: **Contracts**

Update contracts with suppliers to include clauses that enforce the cybersecurity standards. Ensure that there are clear penalties for non-compliance and terms that allow for regular security reviews.

Step 5: **Monitoring**

Implement monitoring tools and processes to continually assess the cyber health of suppliers. This could include regular scans, alerts, and updates to ensure ongoing compliance with cybersecurity standards.

Step 6: **Incident Response**

Develop a coordinated incident response plan that includes suppliers. This plan should outline roles, responsibilities, and communication strategies in the event of a cyber attack or breach.

Step 7: **Training**

Provide training and resources to suppliers to help them understand the importance of cybersecurity and how to maintain the standards required.

Step 8: **Continuous Improvement**

Regularly review and update the supply chain cybersecurity framework. Assess the effectiveness of controls, incorporate new threats and vulnerabilities into the model, and refine processes to improve security over time.

General Notes

Compliance

Ensure that the cybersecurity requirements for suppliers are also in compliance with relevant laws and regulations.

Collaboration

Promote collaboration between your company's cybersecurity team and suppliers to foster a culture of security and to address any issues proactively.