Advancing the Secure Supply Chain: A RUCKUS Executive Summary

Company overview

Founded in 2002, RUCKUS Networks has continually delivered innovative technology that redefines what's possible in wireless network performance. We build and deliver purpose-driven networks that perform in the tough, unique environments of the industries we serve. Leveraging network assurance and enterprise-wide automation driven by AI and machine learning, we empower our customers to deliver exceptional experiences for every employee, guest, customer, student, and resident who counts on those networks to connect to their digital lives.

Why supply chain risk management

In today's interconnected world where organizations rely heavily on global supply chains, providing security and integrity of those supply chains has become increasingly critical. Recent shocks to global supply chains brought on by the COVID pandemic and geopolitical events have reinforced the vital importance of supply chain risk management.

Successful companies must be constantly diligent in assessing and mitigating both internal and external risks. Such examples include:

- Supplier risk—Supplier quality, component/material authenticity issues, and delivery delays can pose a significant risk to the supply chain.
- Geopolitical risk—Political instability, changes in trade policies, or regional conflicts can lead to lengthy disruptions from global partners.
- Cybersecurity risk—As greater portions of the supply chain become digital, they become increasingly vulnerable to cyberattacks.
- Natural disasters—Unforeseen natural events (earthquakes, floods, pandemics, etc.) can impact the supply chain on a regional or global scale.
- Logistical risks—This includes issues related to the transportation of goods (travel delays, warehousing problems, customs delays, etc.).
- Market risks—Price fluctuations and changes in consumer preferences can have a significant impact on the supply chain.
- Regulatory risks—Changes in regulations or non-compliance with regulations can lead to fines, reputational damage, and disruption of operations.

The ability of an organization to prepare and respond to these supply chain risks allows it to thrive during periods of uncertainty.

Supply chain risk management industry best practices

The National Institute of Standards and Technology (NIST) Special Publication 800-161r1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations" provides comprehensive guidelines for managing risks in the supply chain. These guidelines apply equally to physical and cyber supply chains, providing organizations with a structured approach to:

- **Identify risks:** By understanding the critical components and services within their supply chain, organizations can pinpoint potential vulnerabilities and threats.
- **Assess risks:** Organizations can evaluate the likelihood and impact of identified risks, allowing them to prioritize their mitigation efforts.

- **Manage risk responses:** The guidelines offer best practices and controls to address the identified risks, creating a more secure supply chain.
- **Monitor and control:** Constant surveillance of supply chain activities allows organizations to detect risks and address them using predefined response plans.

This framework encourages the integration of real-time threat intelligence into supply chain risk management. This proactive approach enables organizations to detect emerging threats by continuously monitoring for new vulnerabilities and potential attacks and implement rapid responses to these threats to minimize potential disruptions and damage.

The NIST SP 800 161r1 publication outlines the following control families to assess implementation of supply chain risk management (SCRM) control (more information on these families can be found in the Appendix):

C-SCRM security control families			
• Access control • Awareness and training • Audit and accountability • Assessment, authorization, and monitoring • Configuration management	• Contingency planning • Identification and authentication • Incident response • Maintenance • Media protection	• Physical and environmental protection • Planning • Program management • Personnel security • Personally identifiable information	• Risk assessment • System and services acquisition • System and communications protection • System and information integrity • Supply chain risk management

Supply chain risk management at RUCKUS

SCRM is of critical importance to RUCKUS to protect our interests and those of our customers and partners. We've based our supply chain assurance methods and practices using the framework outlined in the NIST SP 800 161 r1 standards as a guide for developing our supply chain risk management plan. This is a comprehensive and iterative process that relies on effective communications across the organization and suppliers to create a feedback loop for continuous improvement.

Risk management

Assessing and managing risk involves the ongoing identification, analysis, evaluation and control of potential threats that could disrupt operations. RUCKUS has clearly defined methods for regular risk assessments which are performed by multiple internal teams along with contracted third parties when applicable. Risk assessments are conducted on both the physical and cyber level and apply to system resources used by employees, contractors, vendors, and third parties.

- **Physical SCRM**—RUCKUS has strict requirements that are used for assessing risk at offices and manufacturing sites that include establishing and maintaining ISO 9001 certification. Risk assessments of these facilities are done on a regular basis to address physical access, validation and audit processes, and protection of confidential information.
- **Cyber SCRM**—Since cybersecurity threats, including data breaches and ransomware attacks, have become increasingly common, RUCKUS's IT security and risk management teams continuously monitor data systems and perform regular security audits to minimize vulnerabilities. Access controls and data encryption are used to help ensure that only authorized individuals have access to sensitive systems and data.

Supplier relationships and accountability

Managing supplier relationships and establishing accountability are critical components of effective supply chain risk management. RUCKUS incorporates security requirements into contractual agreements and service-level agreements (SLAs) with suppliers to certify that security policies and standards are clearly understood and complied with. This also provides a legal framework to hold suppliers accountable for security lapses, incentivizing them to maintain robust security measures. Once

contractual agreements are signed, thorough supplier risk assessments are completed on a regular basis to maintain a high level of security throughout the supplier relationship and continuous compliance.

Supplier evaluation is a critical aspect of SCRM that involves the systematic assessment of suppliers to see that they meet RUCKUS quality, reliability, and compliance standards. The supplier risk assessment process is initiated whenever a new supplier is being evaluated, or when an existing supplier has a change in business process.

Organizational resilience

RUCKUS adheres to best practices outlined in NIST SP 800-161r1 for incident response and recovery, so that disruptions are managed swiftly and normal operations are restored as quickly as possible. These include:

- Incident response plans consisting of comprehensive documentation that outlines the procedures to follow for both physical and cyber supply chain disruptions, as well as clearly defined roles and responsibilities of team members involved in incident response.
- Regular training programs on response procedures and simulation drills to test the effectiveness of incident response plans.
- Internal and external communication protocols to see that stakeholders are well informed and expectations are managed.
- Business continuity planning which outlines strategies for maintaining critical operations during and after an incident (including data backup and recovery plan procedures).
- Post-incident reporting including root cause analysis, which can help prevent recurrence and improve future incident response efforts.

Promoting a culture of security

At RUCKUS, security is not viewed as the responsibility solely of the IT department. It is a shared responsibility between departments and is integrated into all business practices. This starts with strong leadership engagement and is shared by employees, contractors, suppliers, and partners. RUCKUS fosters a culture of security by:

- Promoting collaboration between different departments such as IT, HR, procurement, legal, etc., to address supply chain risks holistically.
- Encouraging security best practices, such as protecting sensitive data including personally identifiable information (PII).
- Regularly investing in initiatives that focus on supply chain security, such as system upgrades and modernization efforts to enhance SCRM effectiveness.
- Providing comprehensive security awareness training programs to all employees and contractors as part of new-hire onboarding and annual refresher courses.
- Communicating new SCRM developments, including a quarterly newsletter that contains topics such as new malware circulating the internet, examples of recent phishing attempts, and upcoming changes to security policy.

Managing an effective supply chain has many benefits, including operational efficiency, cost controls, cost savings, sustainability, and improved customer satisfaction. RUCKUS has a proven track record of successfully managing supply chain risk through the establishment of risk management practices, maintaining strong supplier relationships, and promoting organizational resilience. As supply chains evolve and face new challenges, RUCKUS will continue to apply a robust risk management strategy to deliver success for its partners and customers.

Appendix

RUCKUS has developed a comprehensive approach to supply chain risk management, which considers the NIST SP 800 161 r1 security control families outlined in the below table.

SCRM security control families	Description
Access control	Access to systems and components should be limited to authorized users with a clearly defined business justification. Such access must be managed and monitored to prevent the release or modification of sensitive information.
Awareness and training	Training dedicated to supply chain awareness and security risks should be provided to individuals at all levels within the organization. Suppliers and other external partners should also be required to complete supply chain-related training as appropriate.
Audit and accountability	System audit records must be properly maintained to enable the monitoring, analysis and reporting of inappropriate information system activity. Individual system users must be uniquely traceable so that unauthorized users can be held accountable for their actions.
Assessment, authorization and monitoring	Supply chain security controls should be regularly assessed and monitored to confirm effectiveness. Verification of supplier's conformance to secure supply chain requirements must be included in the periodic assessments.
Configuration management	Configuration management tracks the changes to systems, components and documentation within the supply chain. Maintaining configuration management control is critical for organizations to monitor what changes were made and who made them.
Contingency planning	Supply chain contingency planning helps create a suitable level of resilience and recoverability for the organization. This includes developing and implementing plans for emergency response, backup operations, and post-disaster recovery.
Identification and authentication	Identification and authentication allow organizations to trace individuals, processes and systems that make up the supply chain network. Proper authentication methods must be applied across enterprise information systems before allowing access to employees, contractors, vendors and third parties.
Incident response	Incident management involves the monitoring and detection of security events, the execution of proper responses, and the documentation and reporting of those events.
Maintenance	Organizations must perform regular maintenance of information systems as part of supply chain risk management. Maintenance plans should be documented and updated regularly, and maintenance-related activities should be communicated at all levels of the company.
Media protection	Both physical and digital media related to an organization's supply chain must be safeguarded using media protection controls. Media that contains sensitive information should be limited to authorized users and properly sanitized prior to disposal.
Physical and environmental protection	Controls should be put in place to protect assets such as warehouses, manufacturing plants, and supporting infrastructure from physical and environmental risks.
Planning	Security policies, plans and procedures should be put in place to see that SCRM controls stay current with industry, regulatory and customer requirements.
Program management	Program management processes should be applied throughout the supply chain to initiate, track, and control all activities.

SCRM security control families	Description
Personnel security	Individuals who are in positions of responsibility within the supply chain should be properly vetted to confirm they meet the necessary security criteria. Employees, suppliers and third parties should undergo periodic reviews to certify that they remain in compliance.
Personally identifiable information	Personally identifiable information (PII) must be protected and handled with great care to protect the overall confidentiality and integrity of highly sensitive and privileged information.
Risk assessment	Risk assessments should be completed on a regular basis to determine system vulnerabilities. The results of these assessments should include level of risk criticality, likelihood of risk occurrence, and remediation plan.
System and services acquisition	Controls should be in place to address system development lifecycle processes which take supply chain risk and information security into consideration. This includes allocation of sufficient resources for system upgrades and modernization efforts along with the implementation of security measures on services acquired outside the organization.
System and communications protection	Communication infrastructure must be monitored and protected to safeguard information security at both external and key internal boundaries of the company network.
System and information integrity	Adequate system and information integrity controls are crucial to protect organizations from cyberattacks and other malicious threats. Security alerts and advisories should be monitored continuously and acted upon when necessary.
Supply chain risk management	Overall SCRM plans should include the implementations, requirements, constraints, and implications at an enterprise and system level. These plans should be documented and integrated into existing system security plans.

About Ruckus Networks

Ruckus Networks builds and delivers purpose-driven networks that perform in the demanding environments of the industries we serve. Together with our network of trusted go-to-market partners, we empower our customers to deliver exceptional experiences to the guests, students, residents, citizens and employees who count on them.

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

CO-119361-EN (10/24)