A SEMINAR WORK

ON

NIST SP 800-161R1 CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS

BY

JIWUEZE BRIGHT CHUKWUEBUKA
(M.Sc. Cyber security, winter semester 22/23)

ABSTRACT

In this paper presentation, we are going to discuss in detail a risk management standard known as “Nist sp 800-161r1 cybersecurity supply chain risk management practices for systems and organizations”. We will introduce what the standard is all about using some definitions, discuss about its scope and purpose, elaborate the controls, and other interesting aspect of the standard, we compare it to other standards, then discuss on how and when to use it as well as strength and weakness of the standard and finally round it up with a practical example on how to implement the standard.

INTRODUCTION

SUPPLY CHAIN: This refers to the linked set of resources and processes between and among multiple levels of an enterprise, each of which is an acquirer that begins with the sourcing of products and services and extends through the product and service life cycle, it can also be the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product.

A supply chain encompasses everything from the delivery of source materials from the supplier to the manufacturer through to its eventual delivery to the end user.

CYBERSECURITY SUPPLY CHAIN RISK: This can be the potential harm or compromise that may arise from suppliers, their supply chains, their products, and services, this could be because of exposures, threats, and vulnerabilities associated with the products and services, it could also be an insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cyber supply chain.

To demonstrate this concept: suppose Company A decides to undertake a digital transformation project. Their marketing department engages a third-party service provider (supplier 1) to assist with the transformation. This service provider leverages a cloud-based customer platform (supplier 2) that is delivered as a service. As part of the transformation, all Company A's customer details are migrated into this cloud service. Unfortunately, the service provider (supplier 1) fails to secure the administrative accounts they are using to configure the cloud platform (supplier 2), and a malicious actor gains access using their accounts and extracts files containing Company A's customer details. The service provider (supplier 1) remains unaware that their administrative accounts have been compromised until Company A's marketing department is approached by a malicious cyber actor who demands a ransom to delete the customer data, or they will release it publicly.

A real-world example is the SolarWinds attack in USA: a supply chain attack that affected about 18,000 SolarWinds customers which include federal agencies, courts, well known IT companies, private sector companies, state, and local governments across many countries. These hackers hacked the SolarWinds system and infected their product called "Orion software", this software was in turn used by the SolarWinds customers without knowing that it has been infected by a malware, this held the affected agencies and companies ransom in the hand of this perpetrators.

CYBER SECURITY SUPPLY CAIN RISK MANAGEMENT(C-SCRM): The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.
One of the frameworks for this job is the Nist sp 800-161r1 cybersecurity supply chain risk management practices for systems and organizations.

SCOPE AND PURPOSE OF THE STANDARD

This standard encompasses a wide array of stakeholder groups that include information security and privacy, system developers and implementers, acquisition, procurement, legal, and HR. C-SCRM covers activities that span the entire system development life cycle (SDLC), from initiation to disposal.
This standard is also used in organizations and companies to mitigate and reduce risk throughout the supply chain, including the development of appropriate response, strategies, policies, procedures, and processes. The standard serves as guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain.
This standard is applicable to be used by the following individuals and entities.

- Individuals with system and information security, privacy, or risk management and oversight responsibilities, including authorizing officials (AOs), chief information officers, chief information security officers, and senior officials for privacy;
- Individuals with system development responsibilities, including mission or business owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials;
- Individuals with project management-related responsibilities, including certified project managers and/or integrated project team (IPT) members;
- Individuals with acquisition and procurement-related responsibilities, including acquisition officials and contracting officers;
- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;
- Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;
- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts.

• It also provides guidance for cloud service providers.

THE STRUCTURE AND CONTROLS OF THE STANDARD

This means the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

The C-SCRM controls are organized into the 20 control families of [NIST SP 800-53, Rev. 5]

This controls are applied to the following levels of acquiring product and services

- Acquirers
- Suppliers
- Developers and manufactures
- System integrators
- External system service providers
- Other ICT/OT related service providers

The Cyber security supply chain risk management are grouped into 20 control families and under each control has some sub control. To this project, we will give brief explanation of the interesting part, which is the major controls, enterprises should require their prime contractors to implement this controls and flow down this requirement to relevant sub- tier contractors.

These control families are as follows.

1. **FAMILY: ACCESS CONTROL**

Systems and components that traverse the supply chain are subject to access by a variety of individuals and enterprises, including suppliers, developers, system integrators, external system, service providers, and other ICT/OT-related service providers. Such access should be defined and managed to ensure that it does not inadvertently result in the unauthorized release.

2. **FAMILY: AWARENESS AND TRAINING**

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3. **FAMILY: AUDIT AND ACCOUNTABILITY**

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

4. FAMILY: ASSESSMENT, AUTHORISATION AND MONITORING

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

5. FAMILY: CONFIGURATION MANAGEMENT

Configuration Management helps track changes made throughout the SDLC to systems, components, and documentation within the information systems and networks.

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

6. CONTINGENCY PLANNING

Cybersecurity supply chain contingency planning includes planning for alternative suppliers of system components, alternative suppliers of systems and services, alternative delivery routes for critical system components, and denial-of-service attacks on the supply chain. Such contingency plans help ensure that existing service providers have an effective continuity of operations plan, especially when the provider is delivering services in support of a critical mission function.

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7. IDENTIFICATION AND AUTHENTICATION

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

8. **FAMILY: INCIDENCE RESPONSE**

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

9. **FAMILY: MAINTENANCE**

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

10. **FAMILY: MEDIA PROTECTION**

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information-on-information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

11. **FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION**

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

12. **FAMILY: PLANNING**

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behaviour for individuals accessing the information systems.

13. **FAMILY: PROGRAM MANAGEMENT**

All program management controls should be applied in a C-SCRM context. Within federal agencies. The senior information security officer (e.g., CISO) and senior agency official responsible for acquisition (e.g., Chief Acquisition Officer [CAO] or Senior Procurement Executive [SPE]) have key responsibilities for C-SCRM and the overall cross-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, such as the CIO, the head of facilities/physical security, and the risk executive (function).

14. **FAMILY: PERSONNEL SECURITY**

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

15.FAMILY: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

Personally identifiable information processing and transparency is a new control family developed specifically to address PII processing and transparency concerns. The enterprise should keep in mind that some suppliers have comprehensive security and privacy practices and systems that may go above and beyond the enterprise's requirements. The enterprises should work with suppliers to understand the extent of their privacy practices and how they meet the enterprise's needs.

16.FAMILY: RISK ASSESSMENT

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operating of organizational information systems and the associated processing, storage, or transmission of organizational information. Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain.

17.FAMILY: SYSTEM AND SERVICES ACQUISITION

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

18.FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems SC-1 POLICY AND PROCEDURES System and communications protection policies and procedures should address cybersecurity risks

19.FAMILY: SYSTEM AND INFORMATION INTEGRITY

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

20.FAMILY: SUPPLY CHAIN RISK MANAGEMENT

Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures. In general, an enterprise should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier or their provided services or products.

COMPARISON WITH OTHER STANDARDS

Previously, I have performed some tasks with four other standards, they are.

COBIT: A framework created by ISACA to bridge the crucial gap between technical issues, business risks and control requirements. to ensure quality, control, and reliability of information systems.

ITIL: A framework for effectively managing IT services throughout the entire service lifecycle. The ITIL framework offers guidance and best practices for managing the five stages of the IT service lifecycle: service strategy, service design, service transition, service operation and continual service improvement.

IT-Grundschutz: is intended to help companies and organizations to identify and implement necessary security measures in a structured manner. The aim of the specified procedure is to achieve an appropriate and sufficient medium level of protection for IT systems.

ISO 27001 is the international standard that describes best practices for an ISMS (information security management system). The ISO 27001 Standard takes a risk-based approach to information security. This requires organizations to identify information security risks and select appropriate controls to tackle them.

These standards explained above are mostly precise about identifying and treatment of risks associated with IT systems, ITIL have some of the features of Nist sp 800-161r1.

Nist sp 800-161r1 cybersecurity supply chain risk management practices for systems and organizations is more of not just protection of the IT systems, but it is directly involved in the risk associated with different stages of production, which includes all risks associated with both direct contractors and sub- tier contractors, This standard covers the security of all individuals and systems involved in supply chain, from all stages of production, delivery to implementation of ICT/OT products.

HOW AND WHEN TO USE THIS STANDARD

This standard is used throughout the chain of supply, from production stage to the implementation of the product, it also accesses and mitigate the risk associated with all individuals and systems in the supply chain, both at all levels of the enterprise itself, the contractors and sub- tier contractors.

To use this standard, firstly, determine risk by developing a ***threat scenario.*** A Threat Scenario is a set of discrete threat events associated with a specific threat source or multiple threat sources, partially ordered in time. Developing and analysing threat scenarios can help enterprises have a more comprehensive understanding of the various types of threat events that can occur and lay the groundwork for analysing the likelihood and impact that a specific event or events would have on an enterprise. With a threat scenario defined, the enterprise can complete a risk assessment to understand how likely the scenario is and what would happen (i.e., the impact) as a result. Ultimately, the analysed components of a threat scenario are used to reach a risk determination that represents the conclusion of an enterprise’s level of exposure to cybersecurity risks throughout the supply chain. Once a risk determination has been made, the enterprise will determine a path for responding to the risk using the ***Risk Exposure Framework***. Within the Risk Exposure Framework, enterprises will document the threat scenario, the risk analysis, the identified risk response strategy, and any associated C-SCRM controls.

STEPS IN RISK EXPOSURE FRAMEWORK AND RISK TREATMENT

1. Create a Plan for Developing and Analysing Threat Scenarios
2. Characterize the Environment
3. Develop and Select Threat Events for Analysis

4. Conduct an Analysis Using the Risk Exposure Framework
5. Determine C-SCRM Applicable Controls
6. Evaluate/Feedback.

STRENGTH AND WEAKNESS OF THE STANDARD

This standard update guidance on identifying, assessing, and responding to cybersecurity risks throughout the supply chain at all levels of an organization. It offers key practices for organizations to adopt as they develop their capability to manage cybersecurity risks within and across their supply chains. It also encourages organizations to consider the vulnerabilities not only of a finished product they are considering using, but also of its individual components — which may have been developed elsewhere — and the journey those components took to reach their destination. It shapes and influences laws, policies, procedures, and practices involve in research, development, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and management of ICT/OT products and services by acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

The major weakness of the standard is its limitation to risks associated with supply chain, assessing risk within all procedures that involves in acquiring and implementing ICT/OT products and services, it doesn’t provide the complete security controls to ensure the general information and system security of an enterprise/organization, especially to big companies, it majorly protect an enterprise from threats and vulnerable that may come in through third-party vendors, contractors, sub-tier contractors and their products and services. The controls did not cover the threats and vulnerabilities that may arise from other business processes.

PRACTICAL APPLICATION EXAMPLE OF THE STANDARD

TELECOMMUNICATIONS COUNTERFEITS

Background:

A large enterprise, ABC Company, has developed a system that is maintained by contract with an external integration company. The system requires a common telecommunications element that is no longer available from the original equipment manufacturer (OEM). The OEM has offered a newer product as a replacement, which would require modifications to the system at a cost of approximately $1 million. If the element is not upgraded, the agency and system integrator would have to rely on secondary market suppliers for replacements.

ABC Company has decided to perform a threat scenario analysis to determine whether to modify the system to accept the new product or accept the risk of continuing to use a product that seems to counterfeit.

Environment:

The environment is characterized as follows:

- The system is expected to last 10 more years without any major upgrades or modifications and has a 99.9 % uptime requirement.
- Over 1,000 of the $200 elements are used throughout the system, and approximately 10 % are replaced every year due to regular wear-and-tear, malfunctions, or other reasons.
- The element is continuously monitored for functionality, and efficient procedures exist to reroute traffic and replace the element should it unexpectedly fail.
- Outages resulting from the unexpected failure of the element are rare, localized, and last only a few minutes. More frequently, when an element fails, the system's functionality is severely reduced for approximately one to four hours while the problem is diagnosed and fixed or the element replaced.
- Products such as the element in question have been a common target for counterfeiting.
- The integrator has policies that restrict the purchase of counterfeit goods and a procedure to follow if a counterfeit is discovered
- The integrator and acquiring agency have limited testing procedures to ensure functionality of the element before acceptance

Threat Scenario Analysis:
When one of the elements in the system needs to be replaced, an engineer will install a counterfeit, quickly test to ensure that it is running properly, and record the change. It could take two years for the counterfeit product to fail, and up to 200 counterfeit elements could be inserted into the system before the first sign of failure. If all the regularly replaced elements are substituted for counterfeits and each counterfeit fails after two years, the cost of the system would increase by $160,000 in 10 years. The requisite maintenance time would also cost the integration company in personnel and other expenses.
When a counterfeit fails, it will take approximately one to four hours to diagnose and replace the element. During this time, productivity is severely reduced. If more than one of the elements fails at the same time, the system could fail entirely. This could cause significant damage to agency operations and violate the 99.9 % uptime requirements set forth in the contract. Moreover, if it becomes determined that the element failed because it was counterfeit, additional costs associated with reporting the counterfeit would be incurred.

Mitigation Strategies:
The following were identified as potential mitigating activities
- Require developers to perform security testing/evaluation at all post-design phases of the SDLC
- Validate that the information system or system component received is genuine and has not been altered
- Incorporate security requirements into the design of information systems (security engineering)
- Employ supplier diversity requirements [PL-8(2)].

Based on these controls, the agency was able to devise a strategy that would include:
- Acceptance testing: The examination of elements to ensure that they are new, genuine, and that all associated licenses are valid. Testing methods include, where appropriate, physical inspection by trained personnel using digital imaging, digital signature verification, serial/part number verification, and sample electrical testing.
- Increasing security requirements in the design of the system by adding redundant elements along more critical paths (as determined by a criticality analysis) to minimize the impact of an element failure.
- Search for alternative vetted suppliers/trusted components.

It was determined that this strategy would cost less than accepting the risk of allowing counterfeits into the system or modifying the system to accept the upgraded element.

Threat Scnenario	Threat Source	Counterfeit telecommunications element introduced into supply chain	
	Vulnerability	Element no longer produced by OEM Purchasing authorities unable or unwilling to identify and purchase only genuine elements	
	Threat Event Description	The threat agent inserts their counterfeit element into a trusted distribution chain. Purchasing authorities buy the counterfeit element. Counterfeit elements are installed into the system.	
	Threat Event Outcome	The element fails more frequently than before, increasing the number of outages.	
Enterprise units, processes, information, assets, or stakeholders affected	Acquisitions Maintenance OEM / supplier relations Mission-essential functions		
Risk	Impact	Moderate: Element failure leads to 1-4-hour system downtime	
	Likelihood	High: Significant motivation by threat actor and high vulnerability due to the agency’s inability to detect counterfeits with 25 % annualized probability of premature component failure	
	Risk Exposure (Impact x Likelihood)	Medium: Significant short-term disruptions that lead downtime to exceed uptime threshold by 0.5 % (e.g., 99.4 % < 99.9 % requirement)	
	Acceptable Level of Risk	Low: System must have less than 10 % annualized probability of missing 99 % uptime thresholds	
Mitigation	Potential Mitigating Strategies and C-SCRM Controls	Increase acceptance testing capabilities, security requirements in the design of systems	Modify the system to accept element upgrade

		and employ supplier diversity requirements.	
	Estimated Cost of Mitigating Strategies	$180,000	$1 million
	Change in Likelihood	Low: 8 % annualized probability of component failure	
	Change in Impact	Low: Element failure causes failover to redundant system component – cost limited to maintenance and replacement	
	Selected Strategies	Agency-level examination and testing Place elements in escrow until they pass defined acceptance testing criteria Increase security engineering Search for multiple suppliers of the element	
	Estimated Residual Risk	Low: 8% annualized probability of component failures leading to system downtime (i.e., less than 99.9 % uptime)	

CONCLUSION AND SUMMARRY

Nist sp 800-161r1 cybersecurity supply chain risk management practices for systems and organizations is a standard that access and mitigate risks at all levels of the supply chain, it also inculcates all risks associated with the enterprise itself, the contractors and sub-tier contractors towards the production of ICT/OT products.

In this paper work, we were able to give a detail description of what supply chain is all about, the risks associated with all levels of supply chain and their mitigation strategies, we also explained the interesting part of the controls used in this standard, we discussed when and how to use the standard, strength and weakness of the standard, we did a comparison of the standard with other standards, lastly, we summarized by given a practical example of how to implement the standard in a supply chain environment.