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 processes that involves in acquiring of product and services, this begins with the sourcing of products and services and extends through the implementation of the product, it can also be the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product.
Among this include delivery of source materials from the supplier to the manufacturer and to its eventual delivery to the end user.

CYBERSECURITY SUPPLY CHAIN RISK: This can be the potential threat or vulnerability that may arise from suppliers, their supply chains, their products, and services, this could be because of inadequate security measure or security awareness that could give rise to insertion of counterfeits and malicious software and hardware in a system, it results to poor manufacturing and development practices in the cyber supply chain.

To demonstrate this concept: let's say Company X decides to undertake a customer relationship management (CRM) project. Their marketing department engages a third-party service provider (supplier A) to assist with the project. This service provider leverages a cloud-based platform to manage their database (supplier B). in this scenario, all Company X's customer details are migrated into the database which is been managed by supplier B. Unfortunately, the service provider (supplier A) fails to secure the administrative accounts that linked to the cloud platform (supplier B), and a malicious actor gain access using their accounts and extract files containing Company X's customer details. The service provider (supplier A) would be unaware of this vulnerability and data breach until Company X'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's 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 CHAIN RISK MANAGEMENT(S-SCRM): This is the process of identifying and mitigating the risks associated with supply chain. 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 is used in enterprises and establishments to mitigate and lower the risks throughout a supply chain, this is achieved by developing appropriate policies, procedures, and processes to manage the supply chain.
This standard is applicable to be used by the following individuals and entities.

- Individuals responsible for system and information security, e.g. chief information officers, chief information security officers, and senior officials for privacy.
- Individuals responsible for system development, e.g. program managers, system engineers, hardware and software developers, system integrators, and acquisition or procurement officials.
- Individuals that have responsibilities associated with project management, e.g. project managers and project team members.
- Individuals responsible for security and privacy implementation and operations responsibilities, e.g. business owners, system owners and system administrators.
- Individuals responsible for security and privacy assessment, including auditors, Inspectors General and system evaluators.
- Cloud service providers.

THE STRUCTURE AND CONTROLS OF THE STANDARD

This means the management, operational, and technical controls 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.

Enterprises should require their prime contractors to implement this controls and flow down this requirement to relevant sub- tier contractors.

According to
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
The control families and their descriptions are as follows.

1. **FAMILY: ACCESS CONTROL**

Systems and components that achieves the supply chain should be subjected and accessible to only variety of individuals and enterprises, including suppliers, developers, system integrators, external system, service providers, and other ICT/OT-related service providers. Granting access should be defined and managed to ensure that the system is not tampered by unauthorised individuals.

2. **FAMILY: AWARENESS AND TRAINING**

Organizations must ensure that people involved in organizational information systems are aware of the security risks associated with their activities, also, of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems, 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 retain information about system audit to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, also, ensure that the actions of individual information system users can be uniquely traced to those users so they would be held accountable for their actions.

4. **FAMILY: ASSESSMENT, AUTHORISATION AND MONITORING**

Organizations must periodically assess the security controls in organizational information systems to determine if the controls are effective in their application, then, develop and implement plans to correct deficiencies and eliminate vulnerabilities in organizational information systems.

5. **FAMILY: CONFIGURATION MANAGEMENT**

Organizations must establish and maintain baseline configurations and inventories of organizational information systems throughout the respective system development life cycles, also, establish and enforce security configuration settings for information technology products used in organizational information systems.

6. **CONTINGENCY PLANNING**

Organisations must plan for alternative suppliers of system components, alternative suppliers of products 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.

7. **IDENTIFICATION AND AUTHENTICATION**

Organizations must be able to identify users of their information systems, processes acting on behalf of users, this could be identified through device authentication or verification of the identity of those users, processes, or devices. This authentication or verification must be a prerequisite to allowing access to organizational information systems.

8. **FAMILY: INCIDENCE RESPONSE**

Organizations must employ an operational incident handling capability for organizational information systems that includes adequate, detection, containment, analysis, recovery, and user response activities, also, track, document, and report incidents to appropriate organizational officials and authorities.

9. **FAMILY: MAINTENANCE**

Organizations must perform constant and timely maintenance on organizational information systems as well as providing effective controls on the tools, techniques, mechanisms, and personnels used to conduct information system maintenance.

10. **FAMILY: MEDIA PROTECTION**

Organizations must be able to protect their information system media, both paper and digital, they ought to limit access to information inside the information system media to authorized users and information system media ought to be sanitized or destroyed before disposal or release for reuse.

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

Organizations must limit physical access to information systems, equipment, also access should be limited to the respective operating environments, only authorised users should access them. Information systems should be protected against environmental hazards, also, appropriate environmental controls should be provided in facilities containing information systems.

12. **FAMILY: PLANNING**

Organizations must develop and implement security plans for organizational information systems, 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. All persons that play key security roles in organisations must be involved in Cyber security supply chain risk management.

14.FAMILY: PERSONNEL SECURITY

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

15.FAMILY: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

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 at intervals assess the risk that could occur in organizational operations, 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 always be performed at the enterprise. The system-level risk assessment should include both the supply chain infrastructure and the information system/components that is been used in supply chain.

17.FAMILY: SYSTEM AND SERVICES ACQUISITION

Organizations must allocate enough resources to strongly protect information systems of the organisation, employ system development life cycle processes that understands information security considerations, employ software usage and installation restrictions, lastly, ensure that third-party providers incorporate good security measures to secure their information, applications, and/or services.

18.FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

Organizations must monitor, protect, and control organizational communications. These are those information transmitted or received by organizational information systems. Organizations must also employ architectural designs, system engineering principles, and software development techniques that promote effective information security within organizational information systems.

19.FAMILY: SYSTEM AND INFORMATION INTEGRITY

Organizations must always identify, report, and correct errors associated with information and information systems in a timely manner, they must provide protection from malwares at appropriate locations within the information systems in the organization. Information system security alerts and advisories must be properly monitored, and appropriate response action must be always taken.

20.FAMILY: SUPPLY CHAIN RISK MANAGEMENT

Enterprise should review and concur on the development of C-SCRM policies and procedures, also, provide guidance to system owners for developing product using C-SCRM guidelines. Generally, an enterprise should consider any information relevance to the security, confidentiality, integrity, resilience, quality, trustworthiness, or authenticity of the supplier and their product and services.

COMPARISON WITH OTHER STANDARDS

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

COBIT: A standard developed by ISACA to take care of the gap between technical issues, business risks and control requirements. to make sure that information systems retain their quality, control, and reliability.

IT-Grundschutz: is developed to assist enterprises and establishments to identify and implement appropriate security measures in an organized manner. The main aim of the standard is to ensure an appropriate and sufficient level of security for IT systems.

ISO 27001: The international standard that explains the procedure for an ISMS (information security management system). This Standard takes a risk-based approach to information security. Here, organizations need to identify information security risks and select the best controls to tackle them.

These standards explained above, though, the have similarities with the standard we are discussing in this project work, but their limitations revolve round the establishment which they are been implemented and use.

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 supply chain, third party vendors, service and product acquisition 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.

STRENGTH AND WEAKNESS OF THE STANDARD

This standard is strongly involved in guiding, identifying, assessing and treatment of cybersecurity risks throughout the supply chain at all levels of products and services acquisition. It offers key controls for organizations to adopt as they develop their strength to manage cybersecurity risks within and across their supply chains. It also encourages enterprises to consider not only the vulnerabilities associated with a finished product, but also be careful of the journey those finished product took to reach their destination. It shapes and influences laws, policies, procedures when acquiring ICT/OT products and services by acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

This standard have less weakness in the field of cyber security because it is strictly involved in both enterprises risk assessment and mitigation, also it goes down to risk associated with product and service acquisition as well as the vulnerabilities associated with the journey of a finished ICT/OT products and services before implementation. It majorly protects an enterprise from threats and vulnerable that may come in through third-party vendors, contractors, sub-tier contractors and their products and services.

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 implement this standard, firstly, determine risk by developing a ***threat scenario.*** Identifying the threat scenario simply means identifying a specific threat source or multiple threat sources in the supply chain. Developing and analysing threat scenarios can assist organizations to have a more in-depth knowledge of the various types of threat events that can occur and lay the groundwork for analysing the likelihood and impact that a particular event or events would have on an organization, their contractors and sub-tier contractors. After defining a threat scenario, the organization can undergo a risk assessment procedure to understand how likely the scenario is and what would happen as a result. consequently, the analysed components of a threat scenario are used for risk determination, this represents in conclusion the enterprise's level of exposure to cybersecurity risks all through the supply chain. Once a risk determination has been done, the enterprise will determine a procedure for responding to the risk using the ***Risk Exposure Framework***. Within this contest, enterprises ought to document the threat scenario, the risk analysis, the identified risk response strategy, and any best C-SCRM controls associated with the identified risk.

STEPS IN RISK EXPOSURE FRAMEWORK AND RISK TREATMENT

According to https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
The steps include,

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.

PRACTICAL APPLICATION EXAMPLE OF THE STANDARD

BOOKKEEPING/FINANCIAL AUDITORS

Background:

A bank named ABC Bank, has system that is maintained by contract with an external service provider who audit their financial records and keep track of the daily transaction of the bank. The external service provider needed a cloud-based service provider to keep and secure those records using a cloud-based platform. The cost of leveraging this cloud service provider and cloud platform is approximately $ 300,000 annually. Without proper storage and backup of data using this cloud-based platform, the audited financial record will only be saved in the local computer of the external auditor or auditing company.

ABC Bank has decided to perform a threat scenario analysis to determine whether to allow the leveraging of the cloud-based service provider for storage and backup of the audited record or only work with the external auditing company.

Environment:

The environment is characterized as follows:

- All data/information about the bank need to be kept in safety and secured environment, in an environment that support disaster recovery, these records must last as long as it remains useful to the bank.
- This audited financial record always need to be made available to the bank at intervals in other to ascertain the level of progress they have made.
- This document when lost will never be retrieved because it is not a document to be manufactured.
- Records like this has always be a common target for perpetrators and theft, this record when gotten or stolen could be used to hold the bank on ransom.
- This audited record, when stored in a local computer alone or when stored as a hardcopy document is a serious disaster, because any of these will expose it to crash, theft and damages.
- The ABC bank has a policy that all their data and information must be saved in a platform that support back up and implement disaster recovery.
- The external auditing service provider does not have what it takes to safeguard the records, that’s the reason for leveraging a cloud-based service provider to assist in security.

Threat Scenario Analysis:
When describing the threat scenario, we talk about the difference between cloud storage and local storage.
Cloud storage means storing digital data in an online space having multiple servers and locations while local storage means storing digital data on physical storage devices, e.g., hard disc drives (HDDs) and external storage devices.

CLOUD STORAGE

- **Security:** Cloud storage is secured than the local storage following the use of algorithms that are encrypted. In cloud storage, only authorized individuals such as the cloud service provider, the auditors and the bank are allowed to have access to the documents in the cloud. This adds an extra layer of security.
- **Accessibility:** The Cloud allows authorized individual to access the document from any location/office, all they need is internet connection and credential to access the document.
- **Recovery:** In case of a failure of hard drive or may be other hardware malfunction, the files will be available to be accessed on the cloud. The cloud provides backup solutions for your local storage on physical drives.
- **Updating:** In cloud storage, any time you make changes to a file, it will be synchronized and updated on all your devices, this makes job easier.

LOCAL STORAGE

- **Speed**: Storing data in local storage is faster than that of cloud.
- **Security**: complete control over the document, who can have access and. have the right to choose the information security protocol you want.
- **Capacity**: Local storage have higher capacity than that of cloud.
- **Survivor**: Local storage does not require internet access.

Judging from the above comparisons, you would agree with me that the major threat scenarios here are,

Disaster recovery: Think about the scenario where the local server dies because of unexpected events, such as fire, flood, damage, breakage, the data dies along with it.

Security: Local servers are prone to theft because it can easily be moved around, but information stored in the cloud have high security to unauthorized access. No one accesses it unless people that have credentials to access it and access to documents stored in cloud can be traced in case of cyber-attack.

Mitigation Strategies:

The following were identified as potential mitigating activities,

- For the fact that bank audited records ought to serve a lifetime purpose, therefore, it requires a high level of backup and recovery to improve the confidentiality, availability, and integrity.
- For the fact that this record is a good target to perpetrators, it should be kept in a well secured environment where access to it can easily be limited and checked.
- Employ the control family that talks about the mitigation of risks associated with data security and disaster recovery.

Based on these controls, the ABC bank and external auditing service provider were able to devise a strategy that would include:

- Acceptance testing: Accepting the risk associated with the record been saved in a local server to save cost.
- Increasing security and disaster recovery requirements by employing a cloud-base service provider
- employ diversity method, check out for other external auditing companies that have other cheaper way of saving data from ransomware attack and would support disaster recovery.

It was determined that contracting a cloud-based service provider or checking out for other auditing companies that have a proper and cheaper environment that supports information security, backup, and disaster recovery, within the supply chain is cheaper than allowing the risk of losing their data if anything should happen to a local server.

Threat Scnenario	Threat Source	ABC Bank Financial audit record to be saved in a local server.
	Vulnerability	Limited security and disaster recovery.
	Threat Event Description	Bookkeeping/daily financial audit record of ABC bank been saved and backed up in a local server owned by an external auditing service provider.
	Threat Event Outcome	Lead to loss of data in case system damage,

		failure, or hardware theft.
Risk	Impact	High: ABC Bank will lose track of their daily financial audit, if the lost data is by theft, it might lead to a ransom demand.
	Likelihood	Medium: The likelihood of occurrence is not too high, it’s a 50% chance, if the external auditing company would be very careful in securing their local server from damage or theft.
	Risk Exposure (Impact x Likelihood)	Medium: While the likelihood of occurrence is under probability, but the impact after occurrence could be a serious loss to ABC Bank
	Acceptable Level of Risk	Low: Such sensitive document should not just be left only in a local server; it should be in a well secured environment that supports disaster recovery.
Mitigation	Potential Mitigating Strategies and C-SCRM Controls	Data flow within the supply chain must be in a secured manner, there should not be an occurrence that would lead to loss of data by theft or damage.
	Estimated Cost of Mitigating Strategies	$300,000 annually, else employer diversity might give rise to getting a cheaper and trusted service provider.
	Likelihood after mitigation	Low: 80% secured and proper disaster recovery plan.

	Impact after mitigation	Low: The impact is low there would be little or less situation that would lead to loss of audit records.
	Selected Strategies	contracting a cloud-base service provider or applying employer diversity.

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.

REFERENSES

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

https://www.oracle.com/in/scm/what-is-supply-chain-management/