Mitigating cyber supply chain risks in cyber physical systems organizational landscape

Mitigating Cyber Supply Chain Risks in Cyber Physical Systems Organizational Landscape

Abel Yeboah-Ofori
School of Arch, Computing & Engineering
University of East London
u0118547@uel.ac.uk

Daniel Opoku-Akyeia
Faculty of IT Business
Ghana Technology University College
d.opoku-akyea@gtuc.edu.gh

Abstract: **Cyber supply chain (CSC) provide an organization with the ability to align its business processes, information flows and data structures with other organization. However, the increase interdependencies have brought about inherent, threats, risks, attacks and vulnerabilities that adversaries may be able to exploit when not properly mitigated. Additionally, every cyberattack on each organization increases the probability of the risk cascading to others. The CSC risk has increased exponentially due to uncertainties surrounding cyberattacks and the cyber threat landscape. Recent CSC threats have been disruptive and impacting on the smooth flow of delivery of products and services. CSC risk has been observed as one of the areas that impact greatly and causes budget overruns. The aim of this paper is to mitigate CSC risks in an organizational landscape. In particular, the paper identifies supply inbound and outbound chain threat landscape using a risk breakdown structure. Further, we assess the risk to gather cyber threat intelligence. Furthermore, we use the probability distribution method to determine the CSC risks and analyze the risk probabilities and likelihood of risk cascading impact. Our results show that CSC risk can be neutralized using probability distribution methods to detect and mitigate the risks and their impact levels.**

Keywords: *Cyber Supply Chain; Risk Mitigation; Threat Landscape; Cyber Physical System; Risk Management*

I. INTRODUCTION

Supply chains systems are increasingly operating immensely in the last decade in a more connected global environment [1]. So are the risks and vulnerabilities. According to ITPRO, 50% cyberattacks now uses island hooping to target their victims infiltrating the smaller companies to gain access to the large organizations.. Financial, retail and manufacturing business is in the firing line of this increasing popular cyberattack method [2]. Cyber supplier inbound and outbound Chain risks and threats have increased exponentially as organizations integrate their services and products on the CSC system. Many organizations and banks outsource their sensitive customer data, financial information, business strategy and organizational structures to third party companies and vendors for storage, processing, analysis, delivery and aggregation for business decisions. The primary objective of cyber supply chain risk mitigation is to identify, assess and mitigate products and services that may contain potentially malicious functionality, are counterfeited or are vulnerable due to poor manufacturing and development practices within the cyber supply chain [3]. CSC attack could be initiated through a network, embedded malicious soft, vulnerable website or through spear phishing. It has become inevitable to carry out a risk assessment to gather threat intelligence of threat actors motives, intents, attack vectors, vulnerable spots and adversary goal require to mitigate the cyber risks. The inbound suppliers include the external organization that has remote access to the CSC system and provides electric power transmission, [4] the banks that provide the electronic products and payments as well as third party vendors that purchase the electricity directly and then sell it to consumers. For instance, in an inbound supply chain environment, the adversary could target CMS systems through a third party supply chain system with the bank [5]. Here, the bank receives bill payment through online banking services on behalf of the organization then transfer the funds into the organization's accounts directly. The organization can experience attacks on the physical and network infrastructures that support the application processes. The adversaries goal is to use inland hopping attack to penetrate the supply chain system, gain access to the valuable information stored through a third party and potentially commit large scale cyberattacks. Therefore, security requirements engineering approach can provide a comprehensive and structured elicitation and understanding of cybersecurity requirements, attack vector, threat analysis and intelligence models in supply chain environment.

The aim of this paper is to mitigate cyber supply chain risks by identifying attacks, threats and vulnerable spots within the cyber supply inbound and outbound chains and third party organization landscape. The contribution of this paper is in threefold: (1) identifying the supplier inbound and outbound chains threat landscape that may pose a risk on the system, (2) use probability distribution method to analyze the probability of the threats cascading and (3) finally develop mitigating techniques to control the risks.

II. RELATED WORKS

CSC has improved business processes, enhance transparency, speed in productivity and increase accuracy, as well as monitoring and control. However, CSC risks in the supply inbound and outbound chain has been increasing especially with the advent of cyberattacks and it is affecting the smooth flow of resources even in the most robust supply chains systems. [6], proposed a mitigating risk of a cyberattack on a smart grid system by discussing the fragmented landscape of studies into the risk of cyber attacks on a smart meter, system engineering and fault tolerance. [7], proposed cybercrime risks on CPS that used subjective judgment and Analytical hierarchal

978-1-7281-7417-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSIoT47925.2019.00020

process (AHP) to determine risks. NIST [8] proposed a CSCRM guideline that identifies, assesses, selects and implement risk management processes and mitigation controls through an organization to help manage ICT supply chain risks from adoptive tier 1 through to implementation tier 4. NCSC [8] proposes a supply chain risk guidance with a series of 12 principles, designed to help establish effective control and oversight of your supply chain by identifying what needs protecting, knowledge of supplier's system, and security risk posed by the supply chain. [10], proposed a cybersecurity threat modelling for supply chain organizational environment, by analyzing CSC attacks and cyber threat reporting among supply chain stakeholders. [11], proposed the application of logical and systematic methods of establishing the context of identifying, analyzing, evaluating, treating risk associated with any activity, process, function and product. [12], provide guidelines for establishing a systematic approach for risk management necessary to identify organizational security requirements for information security. [13], proposed an intuitive scheme for the categorization of cybersecurity risk assessment methods for SCADA systems by analyzing the twenty-four risk assessment method. [14], proposed a risk assessment in CPS from an office environment by identifying physical security and information and clarifying risk from a user perspective. NIST 800-30 [15] proposed a risk assessment approach to support enterprise-wide risk management required to mitigate purposeful attacks, environmental disruptions, human or machine errors, and structural failures. [17], proposed a probabilistic threat propagation for network security by present a method for detecting malicious and infected nodes on both monitored networks and the external internet**.** [18], proposed an intuitive scheme for categorizing cybersecurity risk assessment method for SCADA systems after reviewing 24 risk assessment methods applied in the context of SCADA systems.

III. APPROACH

This section adopts the Cyber Supply Risk Management approach required to be carried out through the lifecycle of the organizational CSC. An organization should be able to identify its assets, goal, specific requirements and threat actors. [11] [18], posits that risk assessment is the most error-prone step in risk management process due to the uncertainties in estimating the magnitude of potential financial loss and the probability that the loss will occur. By quantitatively assessing vulnerabilities and proposed a method for evaluating security enhancement. To Mitigate CSC risks, we consider a potential cyberattack could affect an organizational supply chain and determine the vulnerabilities, threat landscape, and the associated risks that are likely to impact the organization. For the study we adopt the CSCRM process below:

- Risk awareness and preparation
- Risk identification
- Risk assessment: Analysis and Evaluation
- Risk response: Risk transfer, risk sharing, risk reduction & risk avoidance
- Risk communication
- Risk monitoring and control

A. Risk Mitigation Approach

For the study, we adopted the probability distribution methods and to mitigate the CSC risks. The rationale for choosing probability distribution methods and the financial portfolio criteria model is that, CSC risks can be quantified based on how threats propagate on the supply inbound and outbound chains and its cascading impacts for cyber threat intelligence.

B. Probability Distribution Function on CSC Attack Propagation

Probability distribution function (PDF) looks at the different probability outcomes or possible values for the random variables. We use probability distribution method to determine the outcome of an attack propagation on the CSC system to determine a product was modified during production, manipulated during distribution or manipulated during delivery after a cyber attack has been initiated.

$$\sum_{x}^{n} P(x) = 1 \qquad (1)$$

Cyber threat intelligence gathering and risk identification provide the organization knowledge of the vulnerabilities and threats to the organizational goal and basis to understanding the organization security situational awareness, a rationale to invest in security and the cost of alternatives.

IV. CYBER SUPPLY CHAIN RISK MITIGATION PROCESS (CSCRM)

This section considers, CSCRM approach as discusses in section 3, and implement the process of identifying organizational goal, assets, and requirements. IEC/ISO31000 proposes an architecture that incorporates the relations between risk management principles, framework and the processes by establishing concepts that explicitly address uncertainties, linking that to the organization framework mandate and establishing the processes [1]. Further, we Identification of vulnerable spots, attacks and probable risks. Furthermore, we identify mitigation goals as follows:

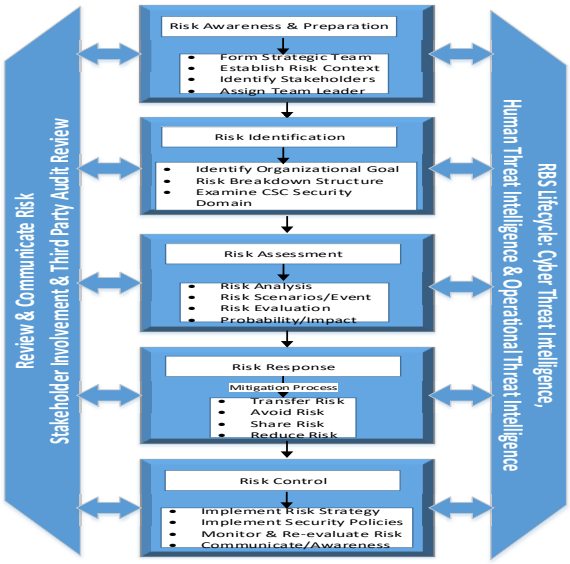

Figure 1. Cyber Supply Chain Risk Mitigation Process

A. Risk Awareness and Preparation

Risk awareness and preparation is the initial stage where the team organization accepts the fact that there are potential CSC risks to be considered from a strategic, tactical and operational perspective.

Activity 1: Establish the CSC Risk Context: A security strategic team is formed to oversee the CSC risk management process including representatives from all stakeholders to leverage communication, knowledge and cross functional information sharing. The rationale is to establish the context within which the risk charter, plan and motivation are structured and responsibilities are assigned. The role of the team is to identify all assets, various organizational and third party vendor goals, known attacks, known-unknown, and unknown-unknown to provide awareness and understanding of the CSC domain and the threat landscape. This allows the organization to proactively develop a strategy, determine the approach required and allocation of adequate resources for the process. The goal is to recognize and manage internal events and external threats that may affect the likelihood of a business continuity process and impact on the organizational goal by asking the following:

- What can go wrong (risk event): known-unknown
- How to minimize the risk event's impact: unknown-known
- What can be done before an event occurs: unknown-known
- What to do when an event occurs: Mitigation

B. Risk Identification

The risk identification process includes identifying and listing all organizational assets and all possible attacks on the supply chain system that could be deemed as a risk. An important aspect of risk identification is the cyber threat intelligence, human threat intelligence and physical threat intelligence gatherings of threat actors, attack vectors, vulnerable spots and adversary goal require to mitigate the cyber risks. We follow the activities below:

C. CSC Systems Assets and Infrastructure

The Smart grid systems assets and the infrastructures consist of network architecture, wireless communication network, mesh topology and communication protocols that that supports the distributed control systems and SCADA systems. It has a power generation, transmission and distribution platforms that are connected to the main command and control systems. The smart grid uses Intelligence Electronic Devices (IED), Bus, router, switches and public facing IP address systems to connect to the supply inbound and outbound chains. The smart grid systems have firewalls connect to the CSC vendor system and substation access spots. For further reading in Smart grid. Refer [10]. We identify areas the threat actors could exploit as in figure 2.

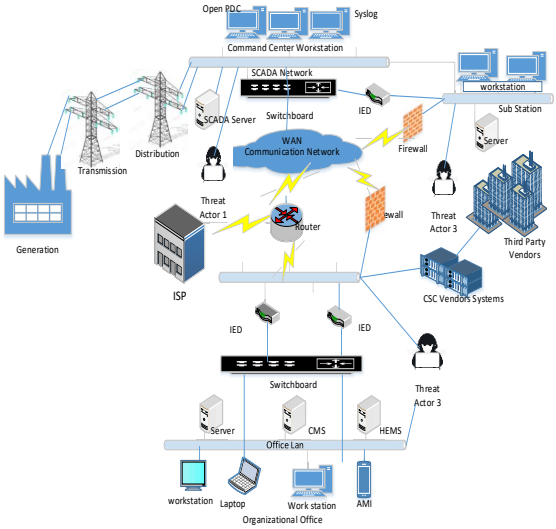

Figure 2. CSC Smart Grid Systems Assets and Infrastructure

Activities 1: Identify Organizational Goal: Involves bringing together the team and stakeholders to brainstorm and use other problem identification techniques to provide detailed identification of the organizational goal, each critical assets, supply inbound and outbound chains infrastructures, CSC requirements, processes, for examining and documenting the associated risk and vulnerabilities.

Activity 2: Risk Breakdown Structure (RBS). Risk Breakdown Structure (RBS) is a technique used by the team to capture and profile all the assets, infrastructures, goals, internal and external threats and vulnerabilities. The rationale is to capture all the possible risks that could

potentially affect the CSC in spite of its effect and impact level.

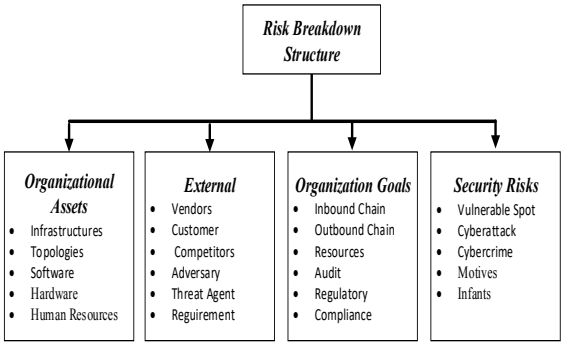

Figure 3. Risk Breakdown Structure

Activities 3: Examined CSC Security Domain: The CSC security domain is examined and investigated after the macro risks are captured, to identify possible attacks such as malware, spyware, and ransomware attack that could be initiated on the supply chain and the source of attacks.

1. Identify specific risks by using: brainstorming, threat intelligence, reviewing of RBS listed, checklist of situational awareness, subjective and expert opinions of the various attack.
2. Identify risks by auditing the third party organizations, classify them based on their service provisions and levels of integration of the various supply chain network system.

The process of identifying, investigating, research and reviewing the CSC network security systems, the existing infrastructures and that of the stakeholder systems provide cyber threat intelligence and situational awareness of potential risks.

D. Risk Assessment

The purpose of risk assessment is to provide evidence-based cyber threat intelligence and analysis to make informed decisions on how to treat a particular risk, how to select between options and the cost of alternatives. Risk assessment considers the likelihood of a risk after identifying and reviewing all probable threats and vulnerabilities that could cause a negative impact. The probability and impact of the risks are examined and quantified in two dimensions using probability and impact factors. The probability of the risk of becoming a reality has to be assessed using techniques such as an expert subjective judgment or discrete probability variables to determine the likelihood and impact. Risk assessment combines two techniques risk analysis and evaluation to determine the probability and likelihood of impact.

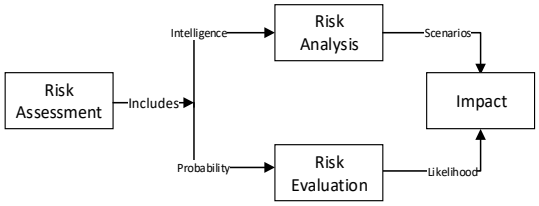

Figure 4. Risk Assessment Process

Activity 1: Risk analysis involves using threat intelligence to identify possible sources of risk such as attack pattern, attack vectors, TTPs, adversary motives and intent. It also uses threat intelligence to identify threats or events that could have a harmful impact on an organizational goal such as product manipulation during production or manipulation during delivery or inserting spyware in a software that is bought off the shelf.

Activity 2: Risk Scenario/Event: A scenario is used that combines three ideas to explain the concept of risk: we select an event (cyberattack), and then combines its probability of occurrence with its potential impact and cascading effects. Further, it estimates the risk by asking the following:

- What is the probability that this event will actually occur in the future? For instance a Ransomware or Remote Access Trojan attack.
- What would be the impact if it actually occurred? For instance, we use low, medium, high and extremely high probability to determine the likelihood.

Due to the integrated nature of CSC, a high-risk event would have both a high probability of occurring and a big negative impact should it occur. The concept of cyber risk is always future-oriented and considers the impact the attack could have in the future and what to do when an event of a cyber attack.

E. Probability Distribution Methods

For the study, we adopted the probability distribution methods to mitigate CSC risks. The rationale for choosing probability distribution methods is that, CSC risks can be quantified based on how threats propagate on the supply inbound and outbound chains and its cascading impacts for cyber threat intelligence. Refer to our previous work in [10] for the attack analysis.

F. Risk Scenario

An organizational supply chain system incorporates other supplier, distributors and third-party vendors on the inbound and outbound chains. The security risk team has identified a malware attack on the CSC system. The team has decided to identify, assess and evaluate the severity of impact and probability of the cascading effects of the risk event. We carry out a risk assessment on all the risk access

spots using a scenario. We assume that not all risk is considered the same as some may be high risk than others. Risk is assessed according to its probability of the event and the impact factor. We categorize the severity and impact as by using a numerical scale of 1 (Low) to 5 (Very High) to determine the relative risks on the vulnerable spots where 1-10 = Very Low, 11-20 = Low, 21-40 = Moderate. 41-70 = High and 71-100 = Very High.

Table 1. Probability and Risk Indicators

Vulnerable Spots	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Firewall	)rganizational Goal	No	70	High	Wrong Firewall
IDS/IPS	Requirements	No	60	High	Configuration
Vendor	Service Provision	No	80	High	Audit
Network	Model Topology	No	60	Medium	Sub-netting
IP	Identify Users	No	55	Medium	Segmentation
Database	)ata Center Storage	No	75	High	Sanitizations
Software	Off The Shelf	No	75	High	ƨeprogram/Update
Website	Third Party Host	No	90	High	SSL/TLS

ble 2. verity Matrix

Vulnerability	Likelihood	mpact	Detection Difficulty	Cause of Risk
Firewall	5	70>	5	Failure to Invest in an incorrect firewall
IDS/IPS	4	60>	4	Lack of expertise
Vendor	5	80>	5	Lack of third party auditing
Network	4	60>	4	Poor Network segmentation
IP	4	55>	4	Not Reviewing IP Addressing System
Database	4	75>	4	Using Data centers without auditing
Software	5	75>	5	Poor test: software bought off the shelf
Website	5	90>	5	Using hosted websites with others

The risk severity matrix in the table 2 provides us with a basis to prioritize which risk to address. Risks with impact level from 70> are considered as a high priority and receive immediate attention. Those risks with 40> are considered high risk and must be addressed if possible in line with the very high risks as their impact could affect the supply chain integration. For instance using a public facing IP address system on a hosted website makes the CSC system very highly vulnerable to an attacker could use island hopping attacks to penetrate the website, gain access to the network and manipulate the software to cause product alteration or manipulate delivery channel.

G. Risk Evaluation

We classify the probable risks using probability distribution techniques below as discussed in section 3 to evaluate the risks as in the following order.

Table 3. Risk Classification

Cause of Risk	Risk Classification	Risk Assessment
Failure to Invest correct firewall	High Impact, High Probability	Neutralize the risk by purchasing the correct firewall based on organizational goal and requirement
Lack of expertise	High Impact, Low Probability	Neutralize risk by competent and qualified the competent security staff.
Lack of Third Party Auditing	High Probability, Low Impact	The risk can be mitigated with regular internal and external auditing.
Poor Network Segmentation	Low Probability, High Impact	The network can be segmented and Firewall/IPS placed between them so that any remote attack on each network may not impact the other.
Not Reviewing IP Address System	Low Probability, Low Impact	The risk can be neutralized by using IP Analyzers and other penetration testing tools to identify vulnerable spots
Using Data centres without auditing	Low Probability, High Impact	Mitigate risk by auditing data centres and sanitize the database as an an attack may expose customer data, cause Data theft, ID theft risk to all those connected to the CSC
Poor test: software bought off the shelf	High Impact, Low Probability	Neutralize the risk by testing the software and third party software before customization and installation to the supply chain
Using hosted websites with other	High Impact, High Probability	The organization uses the public facing IP address system for the supply inbound and outbound chains is dangerous and must be mitigated.

V. PROBABILITY OF CYBER SUPPLY CHAIN ATTACK PROPAGATION

This section determines the probability of attack propagation as discussed in section 3. We use a discrete random variable method as a random variable that can take on any value from a discrete set of values as specified. For the study, we use six different types of attacks variables to set

possible finite values of CSC risks, where the values in the set are numbered from 123456. We use the internal or external threat as our inference since the likelihood of risk of an attack could take on any of these two forms. The probability distribution method determines the outcome of a risk of an attack propagation on the CSC system initiated from anywhere. The six types of attacks include internal attack, external cyber attack, modified during production, manipulated during distribution, manipulated during delivery, or manipulated during installation after a cyber attack has been initiated. The rationale is that we can enumerate all the risk values from 1–6 in the set of its possible value and sum over up all these possibilities and the likelihood of occurrence.

We assign the risks (X) as the discrete random variable (Threats) and assume its probability distribution function P(x) by assigning a probability that X is equal to each of its possible values as specified. For instance, if we identify six different risks on a supply chain system, we can assign a probability of 1/6 to each of the six risks. In the cyber threat landscape where we use discrete random variables, the probability of threat distribution could be referred to as a probability mass function P(x). We define the value of P(x) with a subscript as the probability that a random variable X (Risks) equals the given number x (Threats), i.e. $P_x(x)$ = Pr(X=x). In a cyber attack environment, a valid probability function P(x) must be non-negative for each possible risk value x. Further, the random threat variable is given a number of values in the set of possible values with a probability of at least one attack, so we require that P(x) must sum to one especially as part of the CSC systems requirements capturing:

$$P(x) \geq 0 \text{ for all } x \qquad (2)$$

Where the summation is implicitly applied to all possible values of X (Risks). For instance, in an event of a cyberattack, the probability of any of the six risks occurring is calculated as:

$$P(x) = \begin{cases} \frac{1}{6} & if x \ \{1,2,3,4,5,6\} \\ 0 & Otherwise \end{cases} \qquad (3)$$

Due to the uncertainties in the event of an attack, we could assume that the relative likelihood of an attack can be initiated externally or internally. Therefore, let X (Risk) be the sum of any of the six attack variable outcomes listed in section 5. Then X could take on any value in the set {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} in a random variable. Thus, P(x) is calculated as:

$$P(x) = \begin{cases} \frac{1}{36} & if x \in \{1,12\} \\ \frac{2}{36} = \frac{1}{18} & if x \in \{3,11\} \\ \frac{3}{36} = \frac{1}{12} & if x \in \{4,10\} \\ \frac{4}{36} = \frac{1}{9} & if x \in \{5,9\} \\ \frac{5}{36} & if x \in \{6,8\} \\ \frac{3}{36} = \frac{1}{6} & if x = 7 \\ 0 & otherwise \end{cases} \qquad (4)$$

A. Constructing a Probability Distribution

We construct a discrete probability distribution for random variable X by defining as the number of attacks and risk of manipulations that could be deployed on the CSC after an internal or external cyber attack. We ask the following question and uses the determinants as below to determine the motives and intent of the adversary: What is the probability of a risk on the CSC after initiating an attack? Assuming:

X = Risk = A risk could be internal or external
P = Probability
C = External Cyberattack
A = Internal Attack
P = Modified During Production
S = Manipulated During Supply
D = Manipulated During Delivery
I = Manipulated During Installation

Probability Distribution looks at the different probability outcomes or possible values for the random variables. We plot the outcomes to determine how the distribution is spread out among those possible outcomes.

Table 4. Probability of Initiating an Attack

PD	AI
PD	SD
SD	DI
SD	DI

Probability Distribution for the Random Variables

- P(X=0) = 1/8 = CPD
- P(X=1) = 3/8 = CSD, CAI, CDI
- P(X=2) = 3/8 = ASD, PSD, PDI
- P(X=1) = 1/8 = APD

VI. RESULTS

This section discusses the results of probabilities of the cyberattack propagation and its impact on the CSC system.

A. Probability Distribution Analysis

From the probability distribution table 1, our analysis reveals eight different probabilities of risk on the CSC system could be compromised with various manipulation schemes.

- CPD: The adversary could initiate cyberattack, then cause manipulation during production and then manipulation during delivery. The motive and intent of the adversary are to penetrate the CSC system, manipulate the product by inserting malware in the code at the software development stage that will trigger at the during the delivery channels and divert the products to wrong sources. These could cause Intellectual property theft, Industrial espionage, command & control and DoS attacks and impact the organizational goal and assets.
- CSD, CAI, CDI: Indicates that adversaries could cause an internal or cyber attack on the supply chain, cause manipulate

during supply and installation. The adversary's motives and intent of the attack are more geared towards industrial espionage and advance persistent threat using remote access Trojan or rootkit attack where the adversary targets user with UBS drives, insert a virus on it, to initiate the attack.

- ASD, PSD, PDI: Indicates that the adversary could cause an internal attack, then manipulate the product during supply and manipulation during installation. The motive and intent of the adversary are to insert spyware into the product in order that when a user installs the product and runs it, the virus propagates to other on the network and also provides the adversary access to the network for further manipulations.
- APD: The adversary could attack internally, then cause manipulate during production and manipulation during delivery. The motive and intent of the adversary are to gain access to customer personal details, credit card details, and any information relevant to be able to exploit the customers.

VII. RISK MITIGATION

We follow the following risk mitigation process to determine how to respond to the various cyberattacks.

A. Risk Response

Risk response decides on how to treat the risks and who is responsible for each risk in order to ensure proper mitigation procedures. We consider a number of methods to handle risk. These are factors we consider when mitigating the risk: Transfer the risk, Accept the risk, Avoid the risk, Reduce the risk, Share the risk, or Accept the risk.

B. Risk Mitigation

Acts on threat intelligence gathered and implements control mechanisms, policies, and audit trails to lessen the impact or chance of the risk occurring. This includes making a strategic decision, resources availability, and draw up an agreement with all stakeholders and get it sign-off by all party as well as establishing a cyber risk information-sharing platform.

- **Transfer the risk**: Paying a premium insurance companies to pass the risk to another party Insurance is a means of transferring the financial impact of having a risk occur. Subcontracting can also be done using data centres and Internet service providers. This gives the organization a chance to make a vendor responsible for a particular risk.
- **Avoid the risk:** Includes implementing CTI, security measures, budget allocation, configurations, certifying systems, carrying out penetration testing, regular updates, regular backups, audit stakeholder organization and third party vendors, contingency planning and controls to eliminate the CSC risk.
- **Sharing the risk** - Allocating supply chain system resources to different organization and segmenting the system to different parties in order to share risk. This process ensures that risks threat information is share
- **Reduce the risk**: By creating awareness, training and educating users, employ experts, establish, formal communication mechanisms, Implement monitoring and controls strategies, and auditing third party vendors regularly.
- **Accept the risk:** These are unknown-known and unknown-unknown risks that are inevitable to avoid such as zero-day attacks, earthquake, power failure, system failure. Contingency planning is used to mitigate such risks. They are uncertain risks in that the effort to do anything is not worthwhile or nothing can be done at present. In such a situation, the CSC system is reviewed from time to time during the course of inbound and outbound activities.

C. Risk Monitoring & Control

As discussed in section 4. the process of monitoring and controlling all the risks identified and categorized in the risk register. It includes establishing and executing the risk response strategy, monitoring events that are considered as high probability, contingency planning and monitoring new risks. Due to the uncertainties and fuzziness surrounding the cyberattacks on the supply inbound and outbound chains, CSC risks identified, assessed and managed have to be monitored regularly. This is to ensure that any change in the risk status and the risk register are updated on a regular basis for information assurance and situational awareness purposes. The process involves:

- The risk management team must systematically track and evaluate the performance of risk management strategies in line with the risk register and audit trails.
- Organize ad-hoc and regular risk reviews meeting to identify changes in the cyber threat landscape, outstanding software updates, risk probability and impact trends, update risk register, remove outdated risks, and identify new risks. For, instance OWASP Top 10 threats provides current risks and threat updates.

The risk monitoring and control process includes:

- Prioritize high probability risks and monitor CSC audit trail of threat and vulnerabilities for contingency planning purposes.
- Run regular reports from Firewalls and IDS/IPD and monitor network penetration activities and anomalies.
- Run reports on from the IP Analyzer tool and monitor for any intrusion activities and anomalies.
- Implement regular and ad-hoc supply inbound and outbound chain audit on third party vendors
- Sanitize the database system and monitor user transactions.
- Implement stakeholder configuration management system that incorporates all supplier and distributors.

D. Risk Communication

Risk Communication includes organizing training and works, implementing policies and processes and procedures that orient the staff towards an understanding of the risks, threats and vulnerabilities that may exist. The rationale is to create awareness, understanding, and expose users to the potential dangers and the impact it may have on the product, business process, reputation, and jobs in the event of an attack.

E. Comparing Results with Other Works

There are existing related works on cyber supply chain risk management and cyber physical system. Comparatively we reviewed risk management methods used to mitigate threats in Section 2 [6, 13, 18]. Ref [6], proposed a mitigating risk of a cyberattack on a smart grid system by discussing the fragmented landscape of studies into the risk of cyber attacks on a smart meter, system engineering and fault tolerance. Ref [13], proposed an intuitive scheme for the categorization of cybersecurity risk assessment methods for SCADA systems by analyzing the twenty-four risk assessment method. Ref [18], proposed an intuitive scheme for categorizing cybersecurity risk assessment method for SCADA systems after reviewing 24 risk assessment methods applied in the context of SCADA systems. However, our work looked at mitigating cyber supply chain risks from inbound and outbound chains on the smart grid. Our work looked at identifying the CSC risk using risk breakdown structures. Then analysis the risk using probability distribution methods to determine risk propagation and cascading effects.

VIII. CONCLUSION

Cyber supply chain risk mitigation has become a major risk factor due to the integrated nature of the supplier inbound and outbound chains. Further, the uncertainties and fuzziness that surrounds and supply chain risks have become enormous as adversaries are using attacks such as island hopping on third party vendors to attack the main organization. A remote access Trojan attack on a vendor may expose the supplier chain system of the different organization, and the third party vendors. In this paper we have used risk mitigation concepts and risk management methods in supply CSC organizational landscape to identify, assess, analyze, evaluate and respond to CSC risks. To demonstrate the applicability of the method, we have used a risk assessment method and a malware attack scenario to determine the probability of an attack, the likelihood and impact factors as our risk indicators. Further, we have used probability distribution method to determine the probable risks and the probability of cascading to other networks. For instance, we have been able to determine that the adversary could initiate a cyber attack remotely, then cause manipulation during production and then manipulate the delivery channels. Furthermore, we have determined that the motive and intent of the adversary is to penetrate the CSC system, manipulate the product by inserting malware in the code at the software development stage. Finally, we have used a smart grid system as our case study to identify assets, infrastructures and the vulnerable spots that could be exploited. Further study will include cyberattack prediction using machine learning techniques. Secondly, we are working a paper in software reliability in Cyber Physical Systems.

REFERENCES

1. E. Vanpoucke, A. Vereecke, and S. Muylle. “Leveraging the impact of supply chain integration through information technology”, International Journal of Operations & Production Management, Emerald Insight. Vol. 37, 2017. No. 4, pp.510-530. doi.org/10.1108/IJOPM-07-2015-0441.
2. E. K. Thorpe, “50% of Cyber Attacks Now Use Inland Hopping” July 2019.
3. NIST1500-203. Framework for Cyber-Physical Systems. 2017. https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=924021
4. B. Woods, and A. Bochman, “Supply Chain in the Software Era” Atlantic Council: Washington, DC, USA, 2018.
5. National Cyber Security Centre.” Example of Supply Chain Attacks.” GCHQ. 2018.
6. E. B. Rice and AlMajali. “Mitigating the Risk of Cyber Attack on Smart Grid Systems” Conference on Systems Engineering Research. Elsevier. 28. 2014. 575-582. doi: 10.1016/j.procs.2014.03.070.
7. A. Yeboah-Ofori, J. D. Abduli, F. Katsriku. “Cybercrime and Risks for Cyber Physical Systems” International Journal of Cyber Security and Digital Forensics. 2019.
8. D.A Brown, Best Practices in Cyber Supply Chain Risk Management; Intel; 2017. https://www.nist.gov/document-18221.
9. NCSC “Supply Chain Security Guidance: Twelve Principles” National Cyber Security Center. Version 1. 2018
10. A. Yeboah-Ofori, and S. Islam. Cyber Security Threat Modeling for Supply Chain Organizational Environments. Future Internet, 2019. 11, 63, doi: 10.3390/611030063.
11. ISO31000:2009. Risk Management Principles and Guidelines: International Organization for Standardization: Geneva, Switzerland.
12. ISO/IEC 27005: Information Technology Security Risk Management. International Organization for Standardization: Geneva, Switzerland, (2018).
13. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K Stoddart. “A Review of Cyber Security Risk Assessment Methods for SCADA Systems. Elsevier, Computer & Security, 56, 2016, Pg 1-27. doi.org/10.1016/j.cose.2015.09.009.
14. S. Yoneda, S. Tanimoto, T. Konosu. “Risk Assessment in Cyber-Physical Systems in Office Environment” 18th International Conference on Network-Based Information Systems. IEEE. 2015. DOI 10.1109/NBiS.2015.63.
15. NIST 800-30. “Guide for Conducting Risk Assessments” National Institute of Standards and Technology. Version1. 2012.
16. B. R. Rowe and M. P. Gallaher. “Private Sector Cyber Security Investment Strategies: An Empirical Analysis” March 2006
17. K. M. Carter, N. Idika, and W. Streilein. “Probabilistic Threat Propagation for Network Security” IEEE Transaction on Information Forensics and Security, Vol. 9, No. 9. 2014. Pg. 1394-1405. Doi:10.1109/TIFS.2014.2334272.
18. S. C. Patel, J. H. Graham, P. A. S. Ralston. Quantitatively Assessing the vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancement. International Journal of Information Management. Elsevier. 28, 2008, 438-491. doi:10.1016/j.ijinfomgt.2008.01.009.