Cyber security threat modeling for supply chain organizational environments

future internet

MDPI

Article

Cyber Security Threat Modeling for Supply Chain Organizational Environments

Abel Yeboah-Ofori and Shareeful Islam *

School of Architecture Computing & Engineering, University of East London, London E16 2RD, UK; u0118547@uel.ac.uk

* Correspondence: shareeful@uel.ac.uk; Tel.: +44-208-223-7273

Received: 26 December 2018; Accepted: 21 February 2019; Published: 5 March 2019

Abstract: Cyber security in a supply chain (SC) provides an organization the secure network facilities to meet its overall business objectives. The integration of technologies has improved business processes, increased production speed, and reduced distribution costs. However, the increased interdependencies among various supply chain stakeholders have brought many challenges including lack of third party audit mechanisms and cascading cyber threats. This has led to attacks such as the manipulation of the design specifications, alterations, and manipulation during distribution. The aim of this paper is to investigate and understand supply chain threats. In particular, the paper contributes towards modeling and analyzing CSC attacks and cyber threat reporting among supply chain stakeholders. We consider concepts such as goal, actor, attack, TTP, and threat actor relevant to the supply chain, threat model, and requirements domain, and modeled the attack using the widely known STIX threat model. The proposed model was analyzed using a running example of a smart grid case study and an algorithm to model the attack. A discrete probability method for calculating the conditional probabilities was used to determine the attack propagation and cascading effects, and the results showed that our approach effectively analyzed the threats. We have recommended a list of CSC controls to improve the overall security of the studied organization.

Keywords: cyber supply chain; cyber security; attack modeling; smart grid; threat intelligence; threat actor

1. Introduction

A supply chain (SC) is a collection of different organizations that align their business processes, goals, objectives, and some components of their systems to third party organizations, suppliers, consumers and partners [1,2]. Cyber physical systems (CPS) are the integration of computation and physical process that make a complete system, such as physical components, network systems, embedded computers, software, and the linking together of devices and sensors for information sharing [3]. The emergence of CPS, electronic transactions, third party vendors, and banking services have evolved over time and brought many changes to how the organizations and industries operate. CPS supply chains have also brought many challenges, such as lack of specific organizational threat intelligence gatherings, failure to audit third party vendors, lack of security controls, and lack of (cyber supply chain CSC)risk management. Cyber attacks could impact other supply chain partner systems due to many reasons such as software errors, vulnerabilities in any SC partner [4]. Examples include the Saudi Aramco electric-grid cyber attack in 2017, and the Ukraine power grid attack in 2015 [5]. These indicate that supply chain attacks are on the rise and require an attack model and threat analysis to gather threat intelligence [6]. There are existing attack models, such as MITRE's kill chain model [6] that describe the actions an adversary could take to compromise and operate within an organization's overall communication network. Attack trees [7] provide a formal and methodical way of describing

the security of systems based on varying attacks. They use multilevel children within the attack tree, with a single root node that uses different ways to achieve its goal using leaf nodes and Building Security in Maturity Model (BSIMM) [8]. These works are important and contribute to the cyber threat modeling knowledge domain. However, there is a limited focus on supply chain perspective, and specifically on threats relating to inbound and outbound chain contexts that need adequate analyses to ensure CSC security.

The main contributions of this paper are threefold. Firstly, we modeled and analyzed the cyber threats of supply chains organizational context. We integrated concepts from threat intelligence, such as threat, attack vector, TTP, and control, with concepts from the goal modeling languages, including actor, goal, and requirement, and from supply chain context including inbound and outbound. Secondly, we considered widely used industry practices such as the internet security control [9] and STIX threat model [10] to analyze the threats in the supply chain context. Finally, we used a running example from a smart grid system to analyze the proposed approach and demonstrate the applicability of the work. The results showed that we had identified probable CSC threats, risks, and attacks, such as penetration and manipulation that could impact the studied organizational goal. We ascertained the CSC attack vector, and modeled attack patterns and gathered threat intelligence that provided an understanding of adversaries' motives, capabilities, actions, and intent. We have recommended security controls to mitigate the CSC threats.

The rest of the paper is structured as follows: Section 2 presents an overview of related works in the CSC security environment and the existing threat models, while Section 3 considers the need for CSC threat modeling and presents the concepts for a proposed meta-model as well as a threat modeling process and attack algorithms. Section 4 present the analytical and predictive research approach used to implement the threat modeling theorem and evaluates it by following a running example of a case study to model CSC attacks. Section 5 provides a discussion of the several observations identified in the study. Finally, Section 6 presents a conclusion of the study and proposes future works.

2. Related Work

This section provides an overview of the related works on CSC security and smart grid attacks. Supply chain security in CPS smart grid domains is widely integrated with other organizations and requires extensive research.

2.1. CSC Security Environment

Supply chain security are mechanisms that are put in place to control, manage, and enhance the supply chain system to ensure business continuity, protect products, and provide information assurance. Forty-six cybersecurity attack incidents were reported in the energy sector in 2015, most of which targeted the IT systems of utilities and vendors [11,12]. Woods and Bochman (2018) provides an investigation of the operational practices of CSC and risk across the energy, electricity, gas, and nuclear sectors [4]. The research focused on energy sector flaws due to software vulnerabilities such as counterfeit, maliciously tainted, or unintentionally tainted software components that were built into products during design or implementation phase. Here, the components are authorized, authentic, and have passed validation. Wand and Lu (2013) presented a compressive survey of cybersecurity issues for smart grids [13]. The authors specifically focused on reviewing and discussing security requirements, network vulnerabilities and attack countermeasures, secure communications protocols, and architectures in the smart grid. Sun et al. (2018) proposed a state of the art survey for the most relevant cyber security studies in power systems [14]. The authors reviewed cyber security test beds for research that demonstrated cyber security risks and constructed solutions to enhance the security of smart grid technologies and industry practices and standards. However, the study did not review CSC from a vendor perspective. Hymayed et al. (2017) identified smart grid vulnerabilities in TCP/IP communication protocols due to protocol mis-configuration [3]. The authors' supply chain risk encompassed IT and Operational Technology (OT) suppliers and buyers as well as non-IT and

non-OT partners. However, auditing from inbound and outbound supply chains was not discussed from a specific organizational context.

2.2. Threat Modeling

MITRE's Adversary Attack, Techniques & Common Knowledge (ATT&CK) is an adversary model and framework for describing the actions an adversary could take to compromise and operate within an organizations network. MITRE's Cyber Attack Lifecycle consists of seven phases, namely: recon, weaponize, deliver, exploit, control, execute, and maintain. MITRE's 11 tactic categories within ATT&CK for organizations were derived from the latter stages of exploit, control, execute, and maintain [6]. Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive dictionary and classification taxonomy of known attacks that could be used by analysts, developers, testers, and educators to advance community understanding and enhance defense. CAPEC ID438, ID439, and ID3000 [15] list three key vulnerable spots through which adversaries can exploit CSC, and these include modification during manufacturing, manipulations during distributions, and various domain attacks. Within these are various compromises that could be initiated using malware or SQL injection attacks. Common Weakness Enumeration (CWE) (2014) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, and open manner. CWE identifies weaknesses that are exploitable in software, which the attacker can make function in a way that was never intended. The approach allows an organization to prioritize the CWEs most relevant to the organization's business mission, goals, and objectives [12]. Structured Threat Information eXpression (STIX) uses adversary Tactics, Techniques, and Procedures (TTP), cyber attack campaign, incidents, courses of action, exploitation targets, threat actors, and other methods to provide a common mechanism for adding structured cyber threat intelligence information across a range of use cases for improving consistency, efficiency, interoperability, and overall situational awareness [10]. The OWASP Top 10 Most Critical Web Application Security Risks identifies the various web application security weakness, attacks, threat agent, attack vectors, and impacts on organizations [16]. An integrated cyber security risk management approach considering all aspects of critical infrastructure including vulnerabilities and attack scenarios is proposed by [17]. The Diamond model is an intrusion analyses model that describes how an adversary attacks a victim based on two key motivations. The model consists of four components, namely: adversary, infrastructure, capability, and victim. It has associated features, such as timestamp, phases, results, directions, methodology, and resources. In the event of an attack, the model uses the timestamp to identify the phases [18]. Gai et al. (2017) proposed a maximum attack strategy method of spoofing and jamming on the cognitive radio network, using optimal power distribution in wireless smart grid networks. The method was effective for causing the DoS attack on radio frequencies [19]. The authors further proposed a novel homomorphism encryption approach to tackle both insider and outsider threats that can fully support blended arithmetic operations over cipher texts [20]. A dynamic privacy protection model was proposed by [21] to address threats relating to wireless communication. The aim of the model was to ensure data privacy within a scale of communication without using conventional encryption methods. The Attack graph—or graph tree—are conceptual diagrams used to analyze how a target can be attacked. The tree-like structure has multilevel children with a single root used to detect vulnerabilities in the network for analyzing an effective defense [22].

3. Threat Modeling for Supply Chain Contexts

This section presents the concepts for the proposed approach. Our work contributes towards identifying and analyzing cyber threats for the CSC domain.

3.1. The Need for Cyber Supply Chain Threat Modeling

Modeling cyber attacks in an SC environment is a proactive way of creating an understanding and awareness of an adversary's modes of operations and TTPs. Supply chain security ensures

business continuity for an organization as it is able to channel its business activities, such as processes, information, people, and resources of the products and services, to external suppliers, distributors, and individual customers. Increased interdependencies have brought about CSC threats, risks, attacks, and vulnerabilities that adversaries could exploit. Therefore, modeling and analyzing these threats can provide secure protection for a controlled supply chain system. The following are factors that are influencing supply chain threats:

- Evolution of the cyber supply chain threat landscape;
- Integration of supply chain stakeholders on the cyber threat model;
- Inability to determine cascading threat impacts on inbound and outbound supply chains;
- Evolving threat landscapes affecting the supply chain organisation context

3.2. Conceptual View

As stated previously, we considered concepts from the supply chain, threat modeling, and goal modeling domains. These concepts and their properties provided us with an in-depth understanding of the threat actor's intent, motives, and methods, which was needed to model attacks, analyze, and derive threat intelligence.

Goal: A goal represents the strategic aim of an organization. Goals are realized by different factors based on organizational objectives and business processes. Yu (1995) posits that a goal represents a condition in the world that an actor would like to achieve [2]. To achieve a goal, an organization must identify the various actors that will ensure the goal is attained or aborted. We considered both organizational and security goals. An organizational goal is the objectives carried out to meet the overall organizational strategy and vision, while security goals are control systems put in place to prevent threats, risks, attacks, and compromises. Security goals emphasize more of the threat actor's goal, in which the aim is to attack or abort the main organizational goal. The security goal is to ensure confidentiality, integrity, and availability for the overall supply chain systems, and its surrounding context [17].

Actor: An actor describes an entity that has goals and intentions within the system or within the organizational setting [2,23]. The actors are the employees, suppliers, and distributors, as well as those with the potential to cause a threat to the supply chain system (which could be different from the threat actor). Legitimate actors or system users are categorized as organization employees, or users with permission to access or use the supply chain system. Actors can be recognized either by their password, process, identity, or privileges. Suppliers are the various organizations on the supply chain system, including distributors, third party vendors, and suppliers.

A threat actor (adversary or attacker) is characterized as a malicious actor representing a cyber attack threat, with presumed intent and historically observed behavior [10]. For this study, we defined a threat actor as an entity that can breach or compromise the supply chain system, such as a person, user account, or process. Threat actors can be categorized as either intentional or unintentional, and internal or external. The threat actor is linked to the attack, vulnerability, and TTP in a many-to-many relationship. We identified threat actors through their capabilities, such as their intent, type of password used, observed patterns, behavior, history, and motives.

Vulnerability: vulnerabilities are flaws or weakness that can be exploited by a threat actor or a threat agent. In an SC system, a vulnerable can be identified from various sources, including the software, network, website, user, process, application, and configuration, or from a third party vendor. The adversary could insert a hard-coded password as the default administrative setup into the COTS software and that could be a vulnerability when it is not changed after purchase.

Attack: An attack is any deliberate action or assault on the supply chain system with intent to compromise its processes, procedures, and delivery of electronic products, information flows, and services. A supply chain compromise attack is the manipulation of product delivery mechanisms prior

to receipt by a final consumer [15]. Attack properties include type, pattern, perquisites, and vectors. Attack pattern is an abstract mechanism for describing how a type of observed attack is executed [24].

Tactics, Techniques, and Procedures (TTP) is a representation of the behavior or modes of operations of the adversary or threat actor [10]. TTP leverages specific adversary capabilities, behaviors, and exploits it can use on victims. TTP could be used to gather cyber threat information about the attack pattern, resources deployed, and exploits exhibited. TTP is relevant for identifying threat actors, campaigns to provide CSC threat intelligence on adversary's motives, intended effects, and impact on an organization. For instance:

- *Tactics* describe how threat actors operate during the various attack campaigns. This includes how the adversary carries out reconnaissance for initial intelligence gathering, how the information is gathered, and how the initial compromises were conducted. For instance, tactics may be to send a spear phishing email to a group on the supply chain.
- *Techniques* are the strategies used by the adversary to facilitate the initial compromises such as tools, skills, and capabilities deployed. This includes how the adversary establishes control, maneuvers within the supply chain system infrastructures, and exfiltrates data, as well as how to obfuscate through the system. The adversary conceals the email contents in such a way that is not obvious to detect.
- *Procedures* are the set of tactics and techniques put together to perform an attack. Procedures may vary depending on the threat actor goal, purpose, and nature of the attack. A procedure includes carrying out reconnaissance on the victim's systems to identify vulnerable spots, gather information, access rights, and control mechanisms to determine what could be exploited.

Inbound and outbound supply threats: The inbound and outbound supply chains are the organizational systems that integrate with third party companies, suppliers, and distributors to achieve the organizational goal [24]. The inbound suppliers include the external organization and third party vendors who have remote access to the CSC system and who provide electric power transmission [25,26]. The threat actor could penetrate the inbound supplier's system and manipulate data, or alter the organizations that provide the electronic products and payment services. The third party vendors purchase the electric power directly and resell it to the consumer. The outbound supply chain environment is the organization that provides distributed electric power to other organizations, individuals, and third party vendors. The threat actor could initiate malware or SQL injection attacks during distribution, causing a misconfiguration of the supply chain system.

CSC requirement: Requirements are the constraints and expectations needed to ensure that the system supports the stakeholders and business needs. The requirement concept includes properties such as organizational requirements, business requirements, systems requirements, user requirements, and operational requirements [10,23]. The organizational requirements contain concepts that specify the overall organizational environment and how the software will integrate with the security constraints to achieve the goal.

Risks: Risk is the potential negative impact from an attack. The probabilities of attacks being initiated from the vendor systems are high, as they represent a single point of failure. Supply chain risk is the potential for an adversary to sabotage the supply chain, maliciously introduce unwanted functions, or subvert the design, product, or integrity of the system [17,27]. CSC risk can be categorized as IT, non-IT, management, or government. IT risks are technical and operational, while non-IT risks represent organizations, products and services, environmental factors, and natural disasters. Supply chain risks are cascading risks, as an attack on one party may affect others as the organizations that are involved in the integration and process chains also increase [28].

Controls: Controls are security strategies and measures that are formulated and implemented to ensure that the organizational goal and objectives are achieved, and that risks are mitigated with minimal threat or no threat at all. CSC security controls are managerial, operational, and technical safeguards or countermeasures employed within an organizational information system to protect

the confidentiality, integrity, and availability of the systems and their information [29]. Due to the invincible nature of cyber attacks, the organization should establish a collaborative mechanism with all stakeholders on the supply chain to protect and secure the supply chain systems.

Cyber incident reports: Incident report systems provide CSC attack victims the platform to report attacks and threats that have occurred, including their impact and the degree of severity. The purpose is to gather and analyze threat information that can assist organizations and stakeholders to achieve their security goals. Properties for cyber incident reports include type, date, source, and impact. They could serve as notification platforms and disseminators of threat information for training and awareness among third party collaborators, software developers, and security experts.

Threat information sharing: Cyber threat information sharing is a platform that provides the information necessary to assist an organization in identifying, assessing, monitoring, and responding to cyber threats [30]. There are rules that govern and protect information sharing, such as information sensitivity and privacy, sharing designations, and tracking procedures [30,31].

The meta-model shown in Figure 1 depicts the concepts and their relationships. A threat actor may want to attack the system and exploit vulnerable spots using TTP methods to manipulate the CSC system. CSC requirements are used to ensure the security goal, and constraints are achieved to meet the organizational goal. The attack entity is linked to the threat actor, TTP, risks, and threat, as the properties determine the nature of attacks and probable threats. The CSC requirements, risk, controls, and cyber incident report could have an effect on the organizational goal as well as the inbound and outbound supply chains. This interrelationship provides evidence of the degree of threat or cascading effect of how a particular risk could impact the CSC. The likelihood of an attack becoming a probable threat is determined by the threat intelligence gathered.

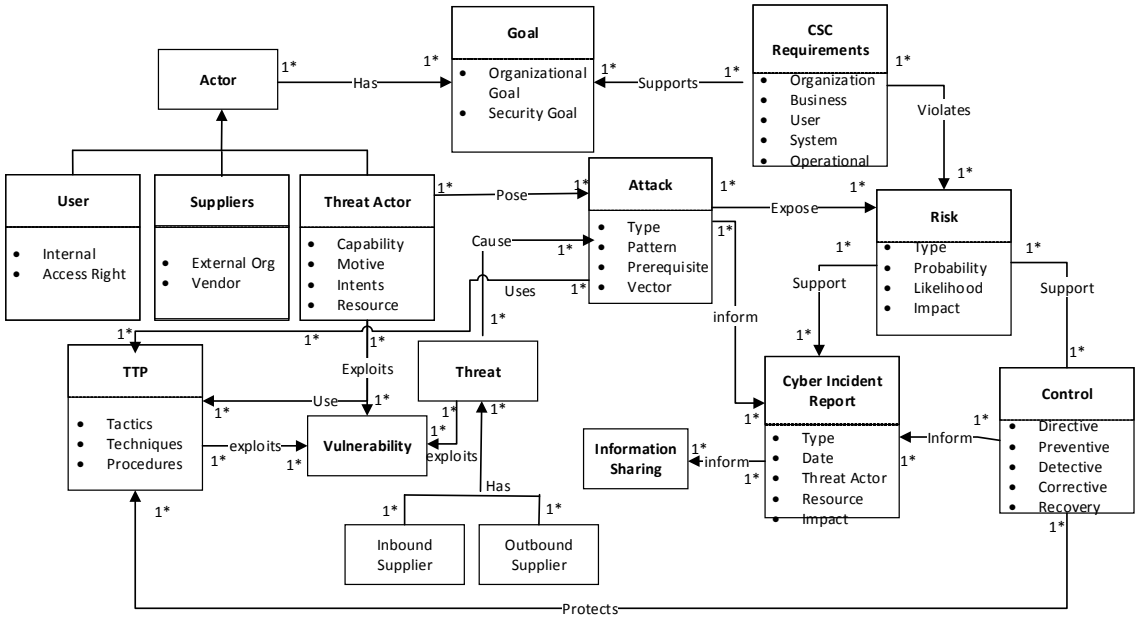

Figure 1. The meta-model.

3.3. Threat Modeling Process

The underlying process involves a systematic approach to identify the organization's supply chain system, internal infrastructures, business processes, attack context, and relevant controls. The process consists of four main phases, as shown in Figure 2.

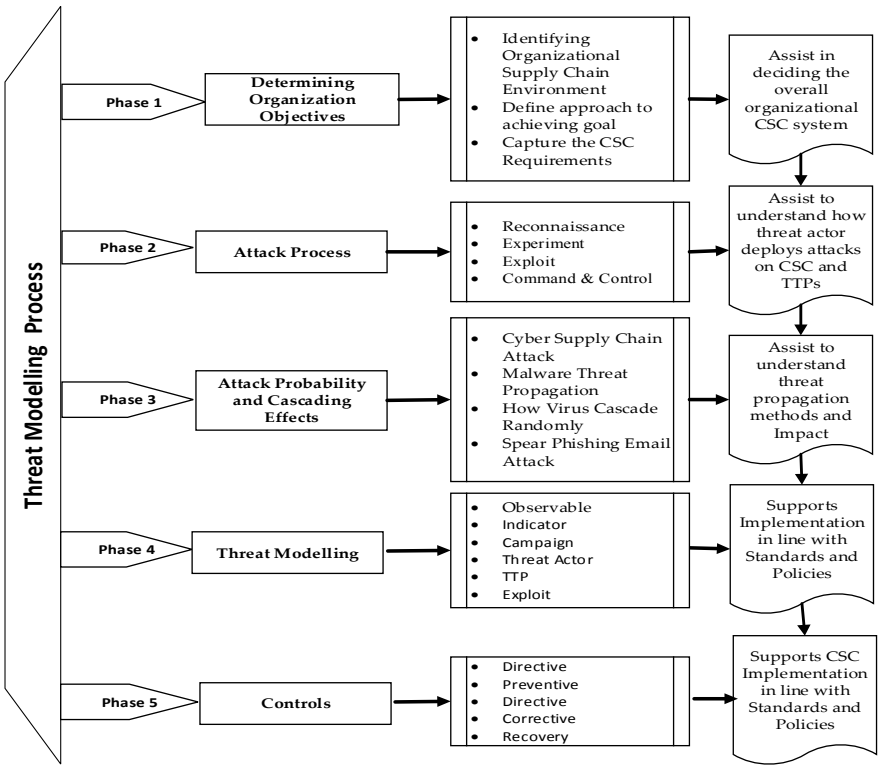

Figure 2. CSC threat modeling process.

Phase 1: Determining organization objectives

The aim of this phase is to identify the overall organizational CSC environment including goals and requirements. It includes three activities which are briefly mention below:

- ***Activity 1: Identifying the organizational supply chain environment*** This activity identifies CSC systems and the external organization, suppliers, distributors, and third party vendors on the inbound and outbound supply chains. The purpose is to identify the vendor's software, hardware, and network design process and policies. This informs strategic management whether the organizational goals are achievable, repeatable, and measurable.
- ***Activity 2. Define the approach to achieving the goal*** This activity identifies necessary actions required to achieve the organizational goals. The organizational goal is to provide safe and reliable service to consumers, while the security goal is to ensure that the supply chain system is secure, reliable, for the overall to achieve business continuity and information assurance.
- ***Activity 3. Capture the CSC requirements*** This activity involves capturing the overall CSC requirement on the inbound and outbound supply chains to ensure the security goal and constraints. The requirements ensure proper integration and interfacing with vendors. Here, the systems development life cycle (SDLC) concepts are used to capture the requirements.

Phase 2. Attack Process

The attack process identifies the activities of a threat actor and the TTP used to deploy the attack. The phase involves complex activities as all the stakeholders may have different system components, requirements, processes, and infrastructures. The attack pattern may be determined based on each stakeholder's business goal, objectives, and the size of the business. The activities include:

Activity 1. Attack Steps

In this phase the threat actor explores the organizational system, and the supply inbound and outbound chains, as shown in Figure 3. The attack steps are as follows:

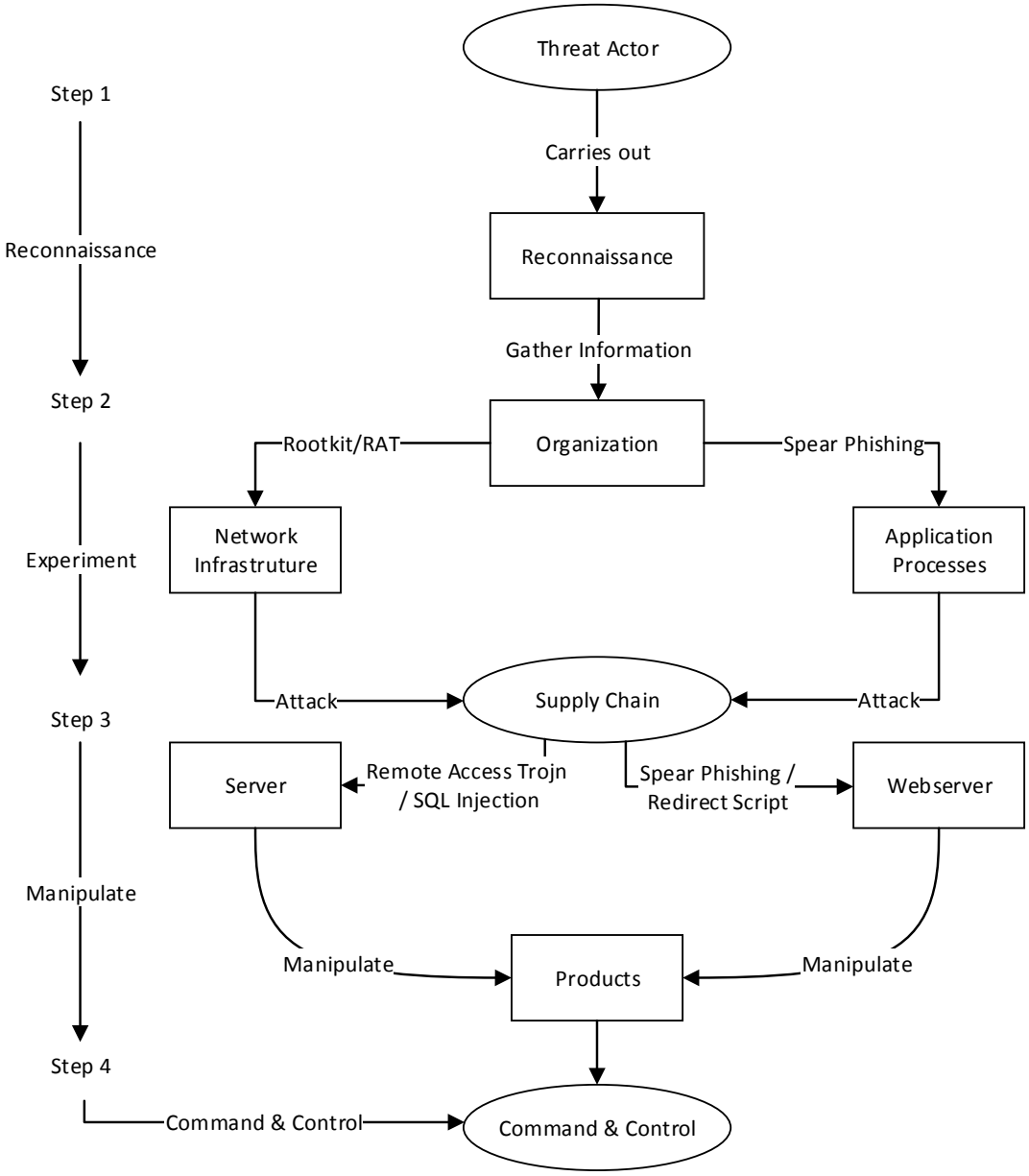

Figure 3. Adversary attack steps.

Step 1. Reconnaissance: The adversary carries out research online and uses other social engineering methods to gather information such as:

- What infrastructure is the organization using: topology, IPs, software, or configurations;
- Profile of the organization, business applications, third party vendors, and other organizations;
- Is the supply chain a corporate and public network system (e.g., virtual private network VPN);
- What type of attack can be initiated (e.g., malware, redirect script, injection, and phishing)? For instance, the adversary could use passive attack tools such as Nmap or Kali Linux.

Step 2. Experiment: The adversary uses various attack methods (TTP) and tools to penetrate and gain control of the victim's systems to try and explore vulnerable spots. For instance:

- The adversary creates an executable malware remotely;
- The adversary inserts a remote access Trojan (RAT), and the malware is installed and executed when a user downloads or opens it through a spear phishing email.

Step 3. Exploit: At this stage, the threat actor gains control of the systems and determines the attack goal. The threat actor penetrates the workstations of the internal users, gains access into the system resources and the supply chain environment, and manipulates the organization's products.

Step 4. Command and control: The adversary uses remote access and Advance Persistent Threat (APT) techniques to establish control of the CSC system, at which point they are able to monitor business processes and activities, and to manipulate the system, exfiltrate information, and obfuscate.

Phase 3. Attack probability and cascading effects

The probability of a cyber attack on a CSC can be initiated in many ways. A threat actor requires full control of a compromised system in order to be able to remotely control malware propagation.

Activity 1. Cyber supply chain attack propagation

Cyber attack propagation changes as the supply chain application processes and operational technologies change. Therefore, it could prove difficult to use any purely quantitative method to formulate attack scenarios at this moment. Since the scenarios are specific to an organizational context, we considered subjective judgments to determine the estimated probability of a successful supply chain attack by using different attack scenarios. The variables that influenced the probability of a malware propagation attack were as follows:

- **Penetration**: We assumed that the threat actor could penetrate the vulnerable spots on the inbound and outbound chain in all the scenarios.
- **Manipulation**: This stage is where the threat actor gains access into the supply chain system and can manipulate data. Threat actor motives and intents were determined by the manipulation.
- **Severity of attack:** The severity of an attack is determined by the extent to which a threat has propagated to the supply chain system. The severity of the attack and the cascading effect are used to determine the the required controls to mitigate the attacks. We categorized the attacks as low, medium, or high in all the scenarios we considered, as there were penetrations available to the threat actor that corresponded to the level of propagation on the targeted supply chain system.

We considered Common Vulnerability Scoring System (CVSS) [32] concepts to determine the severity of attacks as low, medium or high malware propagation. The level of penetration and the severity of the attack determines the probability of a successful random distribution. The propagation was determined using a discrete probability scale of 0–100%. The degree of severity of each manipulation was calculated in percentages as low ($\leq$15%), medium (16 to 59%), or high (above 60%).

Let,

P: Penetration

M: Manipulation

P_a: Probability of attack

AT: Number of attacks

S: Scenario

n: total numbers of scenarios

S_i: attack frequency

Pg: level of propagation

Sa: severity of attack or impact level

Pacc = (access/scenario)

P(scenario) = $1/n$, where n: number of scenarios.

a_i = P(access/scenario), where i: index

We determined the level of penetration and the extent of manipulation by the percentage score used (Table 5). The formulae for calculating the conditional probabilities were as follows:

$$P_{acc} = \sum_{i=1}^{n} P\begin{pmatrix} a \\ s \end{pmatrix}. \mathrm{P}(S_i) \quad (1)$$

Table 5 provide a list of attacks on the vulnerable spots that attackers can penetrate, the extent of manipulation and the percentage of each attack probability. Thus, we calculated the estimated expected value for the probability of attack success as:

$$P_{acc} = \frac{1}{n} \sum_{i=1}^{n} a_i \tag{2}$$

The goal of the threat actor is twofold: penetration and manipulation. We assumed there were 8 vulnerable spots and 10 targeted devices (AT1–AT10) on the CSC system (Figure 4). The threat actor's motive is to acquire a higher level return value by penetrating the command center workstation, and to maintain command and control using advanced persistent threat methods. Our objective was to determine the likelihood of an attack, its level of propagation and the cascading effects. Inputs contained a group of scenarios. We simulated attack scenarios using propagation methods. The initialization worked by repeatedly scanning input probabilities to determine the most and least values, then put them together to fill the vulnerability column. Inputs consisted of the following parameters: For each attack manner using a level of propagation Pg of Si, we considered penetration (P) and the attack (AT) to determine the propagation. The output results will produce a cascading effect on the CSC systems. For further clarification, we used concepts from [19] for the penetration and manipulation attacks. Table 5 illustrates the method and a recursive formula to create the cascading effects.

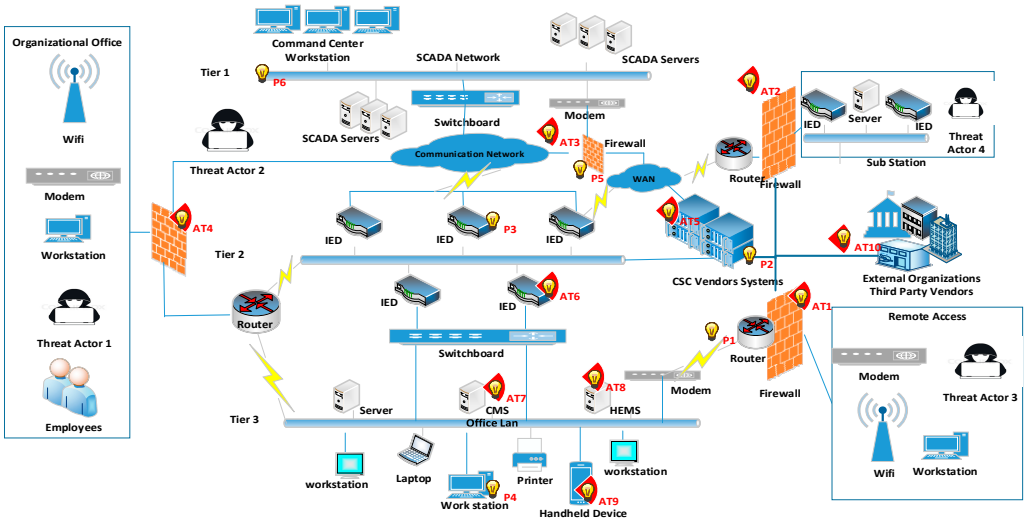

Figure 4. Structure of smart grid CSC and potential security threats.

Activity 2. Malware threat propagation

In a software compromised attack, we identified whether the attack was through manipulation during distribution or during manufacturing. We used TTP to determine the actual sources of malware and whether the course of the attack on the organization CSC was initiated through malware installed or a malware-executed program. Malware installed virus is one way that malicious code can be inserted into the computer.

Algorithm 1 Cascading Effect Algorithm

Input: Propagation Attack Scenarios
Output: Penetration Effects
Initialization

1. Multiply each probability P_a by n.
2. Create array Scenarios and Probability, each of size n
3. For m = 1 to n − 1:
    1. Find the probability P satisfying Pacc $\leq$ 1
    2. Find a probability P (with i $\neq$ s) satisfying Pacc $\geq$ 1
    3. Set Probability [i] = P_i
    4. Set Scenario [i] = S_i
    5. Remove P from list of initial probabilities
    6. Set $P_a = P_a - (1 - p_i)$
4. Let ***i*** be the last probability remaining, which must have a weighted S_a + 1.
5. Set Probability [i] = 1.
6. If, else /"**Cascading Effect**"/ 1: P_a <—— S_i 2: for S_i, i>1 do 3: for P * Pa * Si do 4: for M in S_i do 5: if AT = P_a*P+M*S_i = >1 then 6: Pg + S_1 = Sa 7: end if 8: end for 9: applying algorithm 1 10: end for 11: End for 12: Return Table (Contains the attack methods)

Generation

1. Generate a scenario from an n-sided attack; call the side ***i***.
2. Propagate attack that comes up with a probability **P[*i*]**.
3. If the scenario comes up "P" return ***i***.
4. Otherwise, return scenario [***i***].

Pseudocode

Start,

1. *Multiply each probability by the number of scenarios*
2. *Create array of scenarios and probability, for each of the number of scenarios*
3. *For manipulation equals 1 to number of scenarios equal 1:*
4. *Find the probability P satisfying access divided the scenario that is less or equal 1.*
5. *Find the probability P (with index less or equal to scenario) satisfying access divided scenario that is more or equal 1*
6. *Set probability index*
7. *Set scenario to index*
8. *Set probability of attack to equal minus 1. /"Remove probability from list of initial probabilities"/*
9. *Let index be the last with weighted index severity of attack or impact level.*
10. *If else /"Cascading Effects"/*
11. *Let Probability of attack (Pa) be more than attack frequency (S_i)*
12. *For attack frequency, if index is more than 1, do (indicate)*
13. *Multiply the number of penetration P, probability of attack and attack frequency*
14. *For manipulation in number of attack frequency, do (indicate)*
15. *If the number of attacks is equal to probability of attacks, multiplied by penetration, plus manipulation, times attack frequency, are greater than 1?*
16. *Then calculate*
17. *Level of propagation and attack frequency is equal to severity of attack or impact level*

End

Activity 3. Probability distribution and manipulation for random attacks

The probability of penetrating a web server on a supply chain system can be very challenging. The TTP that the threat actor deploys is basically to create a real message that prevents the spam filters from detecting it and that could generate wrong probabilities. The probability formula for malware executable emails using spear phishing is:

$$P = \frac{P_s^c(1 - r^-)}{\mathrm{v}} \tag{3}$$

Let:

P: probability

P_s: probability of a malware spear phishing penetrating the mail server

C: the number of clicks on the malware

r^-: the average detection rate of an antivirus program installed on third party vendor system

$1 - r^-$: probability of the malware avoiding detection

V: total number of views of a malicious message

We used Scenario 3 in Section 5 to calculate the probability distribution.

Phase 4. Threat modeling using STIX

In this phase, we used the STIX visualization (STIXviz) tool to model the attack process. The STIX tool uses eight constructs such as adversary attack, cyber attack campaign, incidents, exploit targets, threat actors and TTP to generate a structured cyber threat model [14]. However, for our model, we adopted some of the constructs to model the activities, such as observable, indicators, campaign, threat actor, and TTP, to describe the interrelations and actions an attack may take to penetrate and manipulate the CSC system.

Activity 1. Observable: These are the base constructs that are used to determine the measurable events pertinent to the operations of computers and the network. [7] These includes technical and non-technical. We identified all the CSC infrastructures as listed in Phase 1: Activity 1. These included the network systems, Supervisory Control and Data Acquisition (SCADA), Remote Terminal Unit (RTU), Communication devices, and many more.

Activity 2. Indicators: Indicators are parameters that express the nature of the attack and whether it is imminent, in progress, or has already occurred [24]. We used CSC threat activities, adversary behaviors, risky events, or state of the incident to determine what could serve as an indicator.

Activity 3. Campaign: The campaign explains the instances of the threat actor pursuing intent, as observed through sets of incidents and TTP. The intended effect of the threat actor penetrating a supply chain and manipulating the distribution and delivery channels could be a malware attack that is being delivered through spear phishing, or rootkit installation attack, as explained in Phase 3.

Activity 4. Threat Actor: The threat actor construct identifies the attacker based on the campaign activities. Threat Actors are characterized as malicious actors representing a threat including presumed intent and historically observed behaviors [31].

Activity 5. TTP: TTPs consist of the specific threat actor behaviors exhibited in an attack. The campaign, indicators, and threat actor activities determine the TTP that are deployed on the supply chain system as explained in activity 2, 3 and 4. TTP leverages on resources such as tools, capabilities, and personnel to penetrate and manipulate system.

Activity 6. Exploit target: Exploit targets are the vulnerable spots on the supply chain infrastructures such as software, network system, or configurations that are targets for exploitation by the TTP of a threat actor.

Phase 5. Controls: To incorporate controls into a supply chain system, we used knowledge of actual attacks that have occurred in the past. To ensure proper security controls, the organization must form a strategic team to identify, investigate, review, and evaluate the supply chain system processes and applications. We identified the following controls:

- **Directive controls** are more strategic, where risks are identified and assigned to specific inbound and outbound supply chain requirements.
- **Preventive controls** are policies implemented on associated risk probabilities that are intended to preclude actions violating policy or increasing third party risk. This includes supply chain risk assessments and audits.
- **Detective controls** use attack indicators to identify practices, processes, and tools that identify and possibly react to security violations. These include firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) configurations.
- **Corrective controls** involve measures such as courses of actions and CSC risk management designed to react to detections of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- **Recovery controls** are mechanisms put in place to restore a system to its original state once an incident has occurred and resulted in compromising integrity or availability. These include countermeasures, backups, segmentation, and incidence response strategy.

4. Evaluation

In this section, we follow a running example of a smart grid case study to model CSC attacks that are able to determine the applicability of the threat model empirically. We confirmed the viability of the resources, the questionnaires used to generate the study context, and the methods used to gather the data. We investigated the case study and analyze the data gathered to determine the results.

4.1. Data Gathering

For the study, we adopted the analytical and predictive research approach to implement and evaluate the approach. The rationale for the adoption of analytical research is to look for causal relationships amongst the data we collected and attempt to measure them using probability distribution methods. Then, based on qualitative and quantitative analysis, the predictive method was applied to determine whether a specific phenomenon was likely to appear in a similar situation [33]. Considering the invincible nature of cyber attacks and the cascading effects that the attacks could have on a CSC system, we adopt both qualitative and quantitative approaches in our research methods. Both primary and secondary data were collected. We had meetings and discussions with senior management about the purpose and scope of the study, then we had a follow-up meeting and interviews with middle managers who had expertise inside and outside of the organization under study. Data from the secondary source were collected from the organization's websites and other online resources.

4.2. Running Example of a Case Study

The Electricity Corporation of Ghana (ECG) distributes electric power to the southern part of Ghana. ECG provides electricity to about 3.1 million domestic and business customers. ECG core business processes include distribution, setting up a new connection, network operations, maintenance, metering, and billing. It ensures the electric power chain distribution of Ghana with over 70% market share and the largest power distributor in Ghana [34]. ECG is responsible for the distribution of power in the six administrative southern regions in Ghana. The ECG organizational goal is to provide safe and reliable high-quality electric service to consumers in the regions by improving system reliability, improving customer service delivery, reducing system losses, improving operational efficiency, and improving organizational culture. The ECG distribution network system infrastructure must be able to accommodate new connections and support the distribution of electric power to homes, businesses, and third party companies. Recently, the government introduced a rural electrification program requiring the ECG to include new connections. However, the ECG had difficulty meeting the fast developing customer base, the increasing demand on its network operations, maintenance, metering,

and billing systems. It became imperative that ECG deploy a system to speed up fault identification and restoration, cyber security, reliability, and tolerance.

4.3. Smart Grid Electric Power Infrastructure

To meet the challenges above, the ECG recently commissioned and installed an all-automated SCADA system that was required for the modification of its existing network. The electricity distribution network infrastructure uses mesh topologies and SCADA systems as the main infrastructure supporting the CPS smart grid system.

4.3.1. Application Infrastructures and Core Business Systems

The application infrastructures and the network communications system provide business operation, processes, communication protocols, and support the distributed control systems (DCS) and SCADA system. The third party vendor uses Microsoft operating system software and a browser that connects their systems to the ECG server remotely using public service IPs for the prepaid services. The ECG's core business is electric power distribution, and the organizational network infrastructure and business systems are categorized in Table 1.

Table 1. Electricity Corporation of Ghana (ECG) core businesses systems.

Network Infrastructure	Application Systems	People/User	Controls
Smart Grid Architecture	Content Management System/CRM	Staff	Security/Audit
Mesh Topology	HEMS	Suppliers	Best Practices & Guidelines
SCADA Systems	Mobile Devices/Advanced Metering Integration	Vendors	ISO 27001-2 ISMS
UHF Radio	Prepaid	Distributors	
Sub Station	Postpaid System		Policies

4.3.2. Electric Power Distribution Challenges

The ECG electric distribution system has suffered lots of setbacks over the past decade, including voltage surges, software errors, and network interruptions. These challenges are some of the factors that have led to the introduction of prepaid meters or smart meters in Ghana. Prepaid metering or smart metering is the means of paying for electricity before its consumption. However, this has also introduced software errors into the system in recent times, such as prepaid card errors and prepaid meter tampering.

4.3.3. The ECG Supply Chain Organizational Environment

There are seven public institutions involved in the Ghana power sector [33], as well as about two public–private sectors. There are third party organizations contracted by the ECG that supply the digital meters the vending machines. The prepaid system operates via a public–private partnership that is all integrated into the supply chain.

4.4. Study Goal

The goal of this paper is to investigate and understand the cyber security threat in the SC environment of the study context. In particular, we aim to model threats, and to analyze the threats and the associated risks and cascading effects. The hypothesis below will determine the extent of the compromises.

Hypothesis 1: *To what extent, can the threat actor penetrate the ECG CSC system on the inbound and outbound supply chains?*

Hypothesis 2: *To what extent can the threat actor manipulate the data on the supply chain system and the delivery mechanisms?*

4.5. The Process

We used the processes and conceptual approaches in Table 2 to support our study.

Table 2. Mapping the case study with the meta-model concept.

Concepts	Properties	Descriptions
Goal	Organizational goal	Distribute electric power to customers Generate utility bills, Receive payments Provide vendors remote access to CSC Secure systems
	Security goal	
Actors	Users Suppliers	Employees: internal and external Suppliers Distributors
	Threat actor	A person, user account, or processes that can be identified by the intent, motives, and capabilities of an attacker
Requirements	Organizational requirement,	Specify high level organizational environment overall and integrate with the security constraints to achieve the organizational goal
	user categories, ID, stakeholders, description, acceptance criteria	
Supply Chain System	Inbound	Organizations Financial institutions Third party vendors Individual consumers Services providers
	Outbound	Organizations Stakeholders Power transmission company Sub-stations
Vulnerability	Router, firewall, wifi Remote services: remote login, remote command execution	CSC Source and destination, Timestamp,
	Dynamic, host configuration protocol, (DHCP) server logs	Domain name, TCP/UDP port number, media, MAC address IP Address
Attack	Attack goal	Compromise system of:
	Attack pattern	Malware, spyware, injection
	Attack prerequisites	Information on vulnerabilities
	Attack vectors	Mechanisms to deploy attack
	TTPs	Tactic, Technique, & Procedure
Threat	Indicators	Determines vulnerabilities, flaws, and loopholes that can be exploited by a threat actor or a threat agent Specific observable patterns SCS threat activities Adversary behaviors Risky events State of an incident

Phase 1. Attacks on ECG smart grid infrastructure

We consider a smart grid communication path and security application using concepts from the IEC 61850 Smart Grid Interoperability Guide [35] and NIST Smart Grid Interoperability Standards [36] with its three-tiered hierarchical structure interconnected with intelligent electronic devices (IED). Tier 1 covers the transmission and distributions domains, using high-bandwidth communication media such as WiMAX and Fiber on a wireless area network (WAN). The IED monitors and control the electric power transmission to the distribution system using the pharos monitoring unit (PMU) for measuring instantaneous bus voltage, line current, and frequency. The command center integrates with the SCADA system servers and uses a switchboard to establish communication with the IED units [13]. Tier 2 provides a gateway for the Wireless Area Network (WAN) technologies and communication

utilities to have access to the customers' premises for the advanced meter infrastructure (AMI) and demand response applications. It uses a collection of Intelligence Electronic Devices (IED) units to collect the various Phasor Measuring Units (PMUs). Tier 3 integrates the local area network with the customer management systems (CMS) and uses the IED to communicate with the smart meter, which aggregates sensor information from various home appliance devices. We present the attack modeling concepts and steps in Figure 4.

Activity 1. Determine attacks on the CSC

A Threat Actor may be an internal employer or may come from an external source. Several attacks can be initiated on the CSC by the threat actor. As indicated in Figure 4, (P) represents Penetration and (AT) represents Attack.

Tier 1: smart grid integrates with SCADA system servers and uses a switchboard to establish WAN communication with the IED units.
Tier 2: uses IEDs to connect with AMI and demand response applications.
Tier 3: uses LAN to integrate with the CMS and uses the IED to communicate.

The threat actor uses various attack vectors to gather knowledge about the smart grid system topology, configurations, protocols, and operational parameters. Table 3 represents a breakdown of how the threat actors penetrate the systems. We use:

- Penetration (P) to represent how the adversary attacks the system (P1–P6);
- Attack (AT) to represent the devices that were under attack (AT1–AT10);
- Steps (ST) to represent the steps the threat actor followed to attack (ST1–ST4).

Table 3. Smart grid SCS and potential security threats.

Attack Vector Type		CSC System Target	Position	Steps
Penetrating	External	CSC WAN/firewall	P1	ST1
		CSC vendor remote access	P2	ST2
		IED-supported communication	P3	ST3
		Workstation, CMS, HEMS	P4	ST4
	Internal	Command center firewall	P5	ST4
		Organizational LAN firewall		AT4
		Command center SCADA	P6	ST4
Attacking	Devices under cyber attack	Firewall	AT1–AT4	
		CSC vendors	AT5	
		IEDs	AT6	
		CMS	AT7	
		HEMS	AT8	
		Handheld devices	AT9	
		Vendor devices	AT 10	

Activity 2: Determine attack vectors

Here we discuss the attack vectors from Table 3, and follow the attack step in Section 4, to explain the attack vectors using the case study.

- P1. Threat actor penetrates the system from a remote source through the firewall refer Step 1.
- P2. Threat actor gains remote access through Vendor Systems refer Step 2.
- P3. Threat actor exploits the IED that supports the communication systems refer Step 3.
- P4. Threat actor manipulates the workstations, server, and handheld devices refer Step 4.
- P5. Threat actor penetrates the command center firewall refer Step 4.
- P6. Threat actor gains access into the command center and takes controls of the SCADA servers, manipulating, exfiltrating, and obfuscating.

- AT1. The internal threat actor uses social engineering, ID theft, and administrative privileges to gain access through the LAN firewall to manipulate the system refer Step 4.

Activity 3: Detect devices under cyber attack

- AT1–AT4. Indicates that the firewall devices affected are under cyber attack.
- AT5. CSC vendor systems are under attack.
- AT6. IEDs are under attacks.
- AT7. CMS server is under attack.

AT8. No funding body have any role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results".

- (HEMS) server is under attack.
- AT9. Handheld devices are under attack.
- A10. Vendor devices are under attack.

Phase 2: Attack scenarios

An attack scenario is used to determine the vulnerable spots and where penetrations occurred between the variables, as listed in Table 4.

Table 4. Probability and threat indicators.

Scenario	Vulnerable Spots	Penetration	Manipulation%	Probability	Threat Indicators
1	Firewall	Y	70	High	Wrong Firewall
2	IDS/IPS	Y	60	High	Configuration
3	Vendor	Y	80	High	Audit
4	Network	Y	40	Medium	Sub-netting
5	IP	Y	55	Medium	Segmentation
6	Database	Y	75	High	Sanitizations
7	Software	Y	75	High	Reprogram
8	Website	Y	90	High	SSL/TLS

Scenario 1. Remote attack on the CSC system

The organization security team found that an adversary had intruded in the CSC system. The threat actor had compromised the workstation of the CMS that interfaced with suppliers, distributors, and third party vendors. The organization's electronic products had been altered for some time. The CMS generated inaccurate customer electricity consumptions, which compromised the amount the customers were paying for their utility bills, their online payments, and third party vendor systems. The organization used two types of payment systems, the prepaid system and postpaid system, that were all integrated into the CMS and HEMS. Using the formula for calculating conditional probabilities and Activity 1 and Table 4, we determined the vulnerable spots, the severities of manipulation in percentages, and threat indicators.

Scenario 2: Spear phishing email attack

A spear phishing email was sent to the organizational web server and it was noticed that the malware had infected 200 staff email addresses, with 160 that had their data corrupted, 27 that were detected by the spam filter, and 205 that were not detected. The number of users that clicked on the attachment was 220. The number of clicks on the malware attached message divided by the total number of viewers of that message represents the probability of opening the infected email. Following the formula in Phase 3 Activity 3, we used discrete probability to calculate the probability of emails that were infected on the supply chain as follows:

$$\mathrm{P} = \frac{PsC(1 - r^{-})}{v}$$

Results:

$$P = Ps{*}C(1-r^{-})/v$$

$$Pa = 200{*}(220-27)/205$$

Therefore, P = 188.29 (the probability of an opened and infected email)

Activity 4. Probability theorem

Probability (P) is the likelihood that an attack or event will happen. For the study, we identified 10 types of attacks that could be initiated on the supply chain system. These attacks were spyware, ransomware, RAT, spear phishing, SQL injection, XSS, DoS, redirect script, cross site request forgery, session hijacking, and hard-coded passwords. To pick an attack such as malware or SQL injection from a scenario of 10 attacks where spyware, ransomware, RAT, and spear phishing attacks were all classified as malware was 1/10.

For a scenario where the second attack is conditional on the first (e.g., manipulation is dependent on penetration), we used the formula:

$$P(A \text{ or } B) = P(A) + P(B) - P(A \text{ and } B)$$

$$P(A + B) = P(A) * P(B/A) \text{ Where } \{B/A \text{ is 'B given A'}\}$$

Bayesian Probability Theorem

We used Bayes' theorem to explain the dependent probability. Bayes' theorem could be used calculate the probability that manipulation would occur and cause a cascading effect on the supply chain based on some pieces of evidence that were present. For a scenario where the second attack is conditional on the first, (manipulation is dependent on penetration) we determined that if, for instance, an organization had 370 manipulations out of 796 penetrations within a given period in a supply chain environment, then in simple terms the probability is 370/796 = 0.046 (<50%). However, suppose we are not sure whether the systems were manipulated or not and the attacks cascaded, we can use the following figures as evidence to generate a probability distribution method to determine the weight of evidence as follows:

- Penetration manipulation (160) and cascading (210);
- No cascading manipulation (236) and cascading (523).

The probability (P_a) that there will be a manipulation (M) after penetration (P) given that it also cascaded is

$$P_a(P \mid M) = P_a(A) * P_a(M \mid P) / P_a(M)$$

where $P_a(M \mid A) / P_a(M)$ is the weight of evidence, calculate:

$$P_a(P) = 370/796 = 0.046; P_a(M \mid P) = 160/37 = 0.432$$

$$P_a(M) = (160 + 236)/796 = 0.317$$

Therefore:

$$P_a(A \mid B) = 0.046 * 0.462/0.317 = 0.062$$

Conversely, the likelihood of a penetration given no manipulation is = 0.038

4.6. Modeling Attack using STIXviz Tool

The STIXviz tool indicates the process flow and schema of how an adversary initiated a malware attack on the ECG electric power products to penetrate and manipulate data. We followed the threat modeling concepts from Sections 4 and 5.1 to model the CSC attacks. The campaign, the indicator, the threat actor, and the TTP are the main icons in Figure 5. Under them are sub-icons that depict the process flows. The campaign explained the TTP and intended effects of the threat actor—that is, the malware delivery and the installed rootkit malware, as explained in Section 4.1. The indicator icon displays the nature of the malicious activities on the supply chain and attributes them to a threat actor. The threat actor icon identifies the attacker based on the campaign activities. The TTP icon uses the campaign, indicators, and threat actor activities to determine the TTPs deployed on the supply chain system.

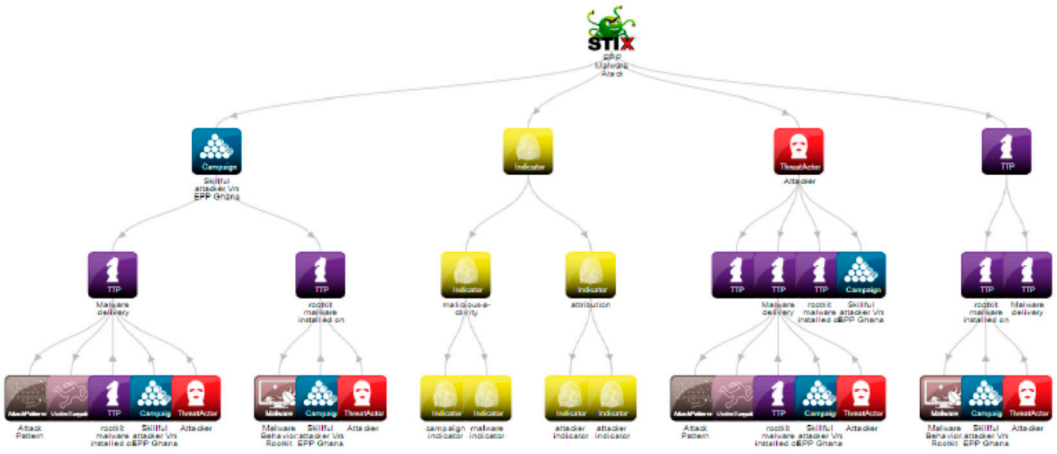

Figure 5. STIXviz tool. Cyber attack modeling and attribution.

4.7. Cyber Supply Chain Controls

To address the questions above in line with organizational objectives, Table 5 provides a lists of security control recommendations.

Table 5. Cyber Supply Chain Controls.

No	Control	Principle	Critical	Security Purpose	Implement	Activity
1	Inventory and Control of Hardware Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access.	Network, laptops, (BYOD) might be out of synch with security updates or might already be compromised.	Attackers can take advantage of hardware installed but not configured and patched with security updates until later.	Utilize active discovery tool to identify devices connected to network and update the hardware asset inventory.	Maintain up-to-date inventory of stored assets or process information and hardware, whether connected to network or not.
2	Inventory and Control of Software Assets	Manage CSC network so that only authorized software is installed. Unauthorized software is found and prevented from installation or execution.	Attackers scan targets sites with vulnerable software that can be remotely exploited and distribute hostile web pages or to third-party sites.	Managing and control of all software plays a critical role in planning, backup, incident response, and recovery.	Utilize inventory tools throughout to automate the documentation of all software on business systems.	Utilize application whitelisting technology on all assets to ensure that only authorized software executes.
3	Continuous Vulnerability Management	Continuously assess and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attacks.	Understanding and managing vulnerabilities must become a continuous activity, requiring significant time, attention, and resources.	Threat actors try to exploit vulnerabilities and attack victim's systems before the organization becomes aware. Due to lack of CSC risk assessment.	Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised.	Utilize an up-to-date compliant vulnerability scanning tool to automatically scan all systems to identify potential vulnerabilities, Deploy automated security updates.
4	Controlled use of Admin Privileges	Not changing hard-coded password default. Impacts on the processes and tools used to track, control, and prevent the correct use, assignment, and configuration of administrative privileges.	Misuse of admin privileges is a primary method for attacks to spread inside a target system.	A privileged user can open a malicious email attachment or website hosting exploited browsers. Second guessing password for an administrative user.	Change default hard-coded password. Ensure all users with administrative account access use a dedicated or secondary account for elevated activities.	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
5	Secure Configuration for Hardware and Software on Mobile Device Laptop and Servers	Implement and manage (track, report, correct) security configuration of assets by using configuration management and change control process.	Developing configuration settings with good security properties is complex. It requires system analysis.	Implement regular security updates on configuration. Ensure vulnerabilities are reported and update to support new operational requirements.	Maintain documented, standard security configuration standards for all authorized operating systems and software.	Utilize Security Content Automation Protocol compliant configuration monitoring system. Verify security configuration. Catalog approved exceptions and alerts in the event of unauthorized changes
6	Maintenance, Monitoring, and Analysis of Audit Logs	Collect and analyze audit logs of events that could help detect, or recover from an attack.	Deficiencies in loggings and analysis allow attacker to hide location and activities.	Keep logging records for audit and compliance purposes. Attackers hide their trails nowadays.	Ensure that local logging has been enabled on all systems and networking devices.	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

5. Discussions

We made several observations from the running example. The study revealed that there were several threats and vulnerabilities that the threat actor could exploit on the electric power smart grid CSC system. These attacks include malware, redirect script, or SQL injection. We discuss the attack vectors used by adversaries as follows:

5.1. Threat Actor Motivation and Intent

The motives and intent of the threat actor may not be known automatically. However, we could use the TTP deployed by the attacker to determine the motive and intention. For instance, design specification establishes the contractual agreement of a final product deliverable after the system requirements have been captured in a software development process. The threat actor could deliberately insert a code to manipulate data, especially in software that is bought off the shelf to prevent the product from achieving the organizational goal. A threat actor may insert a redirect script or exfiltration codes into the actual source during the software development stage to gain access and manipulate the public and private source code repositories. The purpose would be to attack an entity involved in the supply chain lifecycle, such as the organization's website, web server, or database server that connects with a third party financial institution network. With a little knowledge of the software composition, the adversary may cause an APT attack and replace legitimate software with modified versions or counterfeit products. The attacker could use SQL injection attacks to gain access to customers' data and could redirect shipments and deliveries.

The attack could have an impact on several dimensions, such as reputational damage to the organization, loss of customer confidence, loss of customer data, sensitive data exposure, or litigation issues. An example is the malicious alteration of functionalities of the transistors in an integrated circuit, which could cause an electric power consumption reading to oscillate and generate wrong estimates to customers, especially on an industrial scale. This attack could undermine the integrity of the data and software, such as the calculation of charges that determine the total cost of a product at the stage of the distribution channel. The adversary could use a session hijacking attack to take advantage of the insecure default configurations to gain access to the system and change delivery channels. The threat actor could then break the authentication and session management functions, compromise passwords, and gain access to the command center CSC systems especially the demand response, legacy, and billing systems. The cyber physical and cyber digital components of the system could be attacked by adversaries using malware, SQL injection, APT, or command and control attacks on the infrastructure. They could change configurations remotely on the AMI head-end and control meter readings, and send wrong utility measurements, including sending connect and disconnect commands to the electricity services abruptly.

5.2. Attack on the Cyber Physical Components

Cyber physical components are used for the automation of electric power generation, transmission, and distribution processes, and can be attacked due to their close interactions with smart meters and the meter data management system (MDMS) that manages data and the third party vendors. Adversaries can breach the source code by using malware or spyware on the supply chain system and remotely manipulate the CPS smart grid software components that interact with smart meters, organizations, and vendors on the distribution mechanism. Home appliances connected directly to smart meters can be compromised as they interact in a cyber physical environment. Utility companies may use industrial and non-industrial smart meters to control the amount of energy consumed by various organizations, industries, and homes. Further observations show that electric power consumers can now pay their bill using online banking services directly to the utility companies and third party vendors. Here, the customer card details could be stolen using session hijacking attacks as they process

payments online. The attacker logs in and infiltrates other organization networks using the stolen login details after the customer has logged out to gain unauthorized access and cause APT attacks.

5.3. Threat Modeling and Analyses

Threat modeling and analysis looks at the various instances of how threat actors pursuing an intent and exploit it, such as an adversary's motives, opportunities, and the methods deployed by the threat actor. We analyzed the pattern of behaviors as observed through sets of incidents and the TTP used across the organization's supply chain with third parties. We characterized threat actor activities, including presumed intent and historically observed behavior, for the purpose of ascertaining the current threats that could be exploited. The intelligence gathered provides us with an understanding of the adversaries' capabilities, actions, and intents of the organizational supply chain domain. We asking the following questions as we look to investigate further attacks for our analyses and threat intelligence gatherings:

- What attacks have occurred before (malware, SQL injection, session hijacking, XSS);
- How did they occur (causes of action and intrusion sets);
- Who are the threat actors (internal and external staff, adversaries, and threat actors);
- What are the likely occurrences (risk assessments, indicators);
- How can they be detected (penetration tests, vulnerability assessments, threat modeling);
- How can they be recognized (threat intelligence models);
- How can they be mitigated (risk management, controls, policies, regular updates, insurance, and awareness).

5.4. STIX Model

For the STIX model, we used supply chain threat activities, adversary behaviors, risky events, and state of an incident to determine what could serve as a threat indicator. CSC attack incidents and course of actions provided information about the nature of cyber attack indicators and TTPs that can be deployed on the supply chain, especially from the third party vendor's point.

5.5. Comparing Results with Other Works

There is a large body of literature on the subject of cyber supply chain security. Comparing our work with other works, we reviewed proposed attack models that could be used to detect and analyze threats in Section 2 [6,13,14]. [32–34] propose an attack method for spoofing and jamming on the cognitive radio network, algorithms for a novel homomorphism encryption, and a dynamic privacy protection model. However, our work looked at supply chain security from inbound and outbound chains. The paper looked at penetration and manipulation attacks from organizational perspectives. We modeled and analyzed the cyber threat from the supply chain perspective, and used running examples to evaluate the model and proposed controls required to demonstrate the applicability of the work. The results show that we have identified probable CSC threats, risks, and attacks, such as penetration and manipulation, that could impact the organizational goal.

6. Conclusions

Cyber security in supply chain organizational environment has become a major challenge due to the integration and interrelationships of various stakeholder systems that are interconnected to achieve organizational goals. This paper attempts to analyze the security of such systems by considering an attack model using concepts such as goal, actor, attack, TTP, and threat actor that are relevant to the supply chain context along with their interdependencies. To demonstrate the applicability of the model, we used the STIXviz tool to model attacks for gathering threat intelligence within the CPS smart grid network and third party organizational system. The study showed that the adversary's goal is to penetrate the inbound and outbound supply chains and manipulate data. The scenarios provided

us an understanding of the various instances of threat actor's methods of pursuing an intent and exploitation. We have observed the threat actors motives and methods, as well as the cascading effects of the attacks. The results showed that modeling CSC attacks and analyzing pattern of behaviors as observed through the sets of scenarios and the TTP used assisted in understanding the security risks. To ensure CSC controls and proper mitigations, it is required that all stakeholders ensure regular third party auditing and implementation of security policies in line with international standards. We have provided a table with a list of supply chain security controls that can manage and enhance the supply chain system to ensure business continuity, protect products and delivery mechanisms, and provide information assurance. Further study is required in the future to model CSC security threats from power grid sub-station systems and from different attack scenarios. We are also looking to determine cybercrime risks in cyber physical systems. Further study will include a detailed analysis of threats using machine learning techniques.

Author Contributions: A.Y.-O. and S.I. have contributed to the modeling and analyzing of the CSC security threats. A.Y.-O. organized the case study and accomplished the case study. S.I. contributed with reviewing the whole paper.

Funding: This research received no external funding.

Acknowledgments: We would like to thank ECG IT Security management team for sharing the relevant information for the case study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Boyens, J.; Pauslen, C.; Moorthy, R.; Bartol, N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Comput. Sec.* **2015**, *800*, 1. [CrossRef]
2. Yu, E. Modeling Strategic Relationship for Process Reengineering. Ph.D. Thesis, Department of Computer Science, University of Toronto, Toronto, ON, Canada, 1995.
3. Humayed, A.; Lin, J.; Li, F.; Luo, Bo. Cyber-Physical Systems Security—A Survey. Available online: http://ieeexplore.ieee.org/document/7924372/ (accessed on 10 October 2018).
4. Woods, B.; Bochman, A. *Supply Chain in the Software Era*; Atlantic Council: Washington, DC, USA, 2018.
5. Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Available online: https://www.wired.com/2016/03/inside-cunning-unprecedented-hackukraines-power-grid/ (accessed on 18 September 2018).
6. MITRE. Threat Based Defense. Understanding an Attackers Tactics and Techniques Is Key to Successful Cyber Defense. Available online: https://www.mitre.org/capabilities/cybersecurity/threat-based-defense (accessed on 10 October 2018).
7. Phillips, C.; Swiler, L.P. A Graph-based System for Network-vulnerability Analysis. In Proceedings of the 1998 Workshop on New Security Paradigms, Charlottesville, VA, USA, 22–26 September 1998; Association for Computing Machinery (ACM): New York, NY, USA, 1998.
8. BSIMM. Attack Models with BSIMM Framework. Available online: https://www.bsimm.com/framework/intelligence/attack-models/ (accessed on 20 September 2016).
9. CIS Controls. *Basic Organizational Foundational*; Ver. 7; Center for Internet Security: East Green Bush, NY, USA, 2018.
10. STIX: Assets Affected in an Incident. Available online: http://stixproject.github.io/documentation/idioms/affected-assets/ (accessed on 5 May 2018).
11. Idaho National Laboratories. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. Mission Support Centre Analysis. 2016. Available online: https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector (accessed on 25 Febuary 2019).
12. Common Weakness Enumeration (CWE). Common Weakness Enumeration. Supply Chain Risk Management and Due Diligence. Available online: https://cwe.mitre.org/data/index.html (accessed on 10 October 2018).

13. Wang, W.; Lu, Z. Cyber Security in Smart Grid: Survey and Challenges. 2012. Available online: https://research.ece.ncsu.edu/netwis/papers/12WL-COMNET.pdf (accessed on 15 November 2013).
14. Sun, C.; Hahn, A.; Liu, C. Cyber Security of a Power Grid: State of the Art. *Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
15. CAPEC-437: Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack. Available online: https://capec.mitre.org/data/definitions/437.htmlMITRE (accessed on 10 October 2018).
16. Open Web Application Security Project (OWASP). The Ten Most Critical Application Security Risks. Creative Commons Attribution-Share Alike 4.0 International License. 2017. Available online: https://owasp.org (accessed on 10 September 2018).
17. Kure, H.I.; Islam, S.; Razzaque, M.A. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Appl. Sci.* **2018**, *8*, 898. [CrossRef]
18. Caltagirone, S.; Pendergast, A.; Christopher, B. The Diamond Model of Intrusion Analysis; Center for Cyber Intelligence Analysis and Threat Research Hanover Md.: 2013. Available online: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf (accessed on 20 September 2018).
19. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
20. Gai, K.; Qui, M. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. *IEEE Trans. Ind. Inf.* **2018**, *14*, 3590–3598. [CrossRef]
21. Gai, K.; Choo, K.R.; Qiu, M.; Zhu, L. Privacy-Preserving Content-Oriented Wireless Communication in Internet-of-Things. *IEEE Internet Things J.* **2018**, *5*, 3059–3067. [CrossRef]
22. Schneier, B. Attacks Trees. *Dr. Dodds J.* **1999**, *24*, 21–29.
23. Mouratidis, H.; Kalloniatis, C.; Islam, S.; Huget, M.; Gritzalis, S. Aligning Security and Privacy to Support the Development of Secure Information Systems. *J. UCS* **2012**, *18*, 1608–1672.
24. US-Cert. Building Security in Software & Supply Chain Assurance. Available online: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns (accessed on 20 September 2018).
25. Conway, E.; Luu, N.; Shaffer, E. *Best Practices in Cyber Supply Chain Risk Management*; Cisco: San Jose, CA, USA, 2017. Available online: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cyber-supply-chain-risk-management.pdf (accessed on 20 September 2018).
26. Boyens, J. *Integrating Cybersecurity into Supply Chain Risk Management*; RSA; Moscone Center: San Francisco, CA, USA, 2016.
27. Wallace, M. *Mitigating Cyber Risks in IT Supply Chain*; The Global Business Law Review; 2016. Cleveland-Marshal College of Law. Library. Cleveland State University. Available online: https://engagedscholarship.csuohio.edu/gblr/vol6/iss1/2 (accessed on 10 September 2018).
28. Brown, D.A. Best Practices in Cyber Supply Chain Risk Management; Intel; 2017. Available online: https://www.nist.gov/document-18221. (accessed on 20 October 2018).
29. NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems. 2017. Available online: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft-controls-markup.pdf (accessed on 17 September 2018).
30. NIST 800-150. Guide to Cyber Threat Information Sharing. Available online: http://dx.doi.org/10.6028/NIST.SP.800-150. (accessed on 11 October 2018).
31. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX); V1.1, Revision 1; 2014. Available online: https://www.mitre.org/sites/default/files/publications/stix.pdf (accessed on 11 October 2018).
32. Mell, P.; Scarfone, K.; Romanosky, S. *A Complete Guide to the Common Vulnerability Scoring System*; Ver. 2.0; 2007. Available online: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51198. (accessed on 11 October 2018).
33. Brewer, R. *Your PhD Thesis: How to Plan, Draft, Revise and Edit Your Thesis*; Studymates Limited: Abergele, UK, 2017; ISBN 978-1-84285-079-1.
34. Electricity Company of Ghana. ECG. Available online: http://ecgonline.info/ (accessed on 10 September 2018).

35. IEC Standard. *IEC 61850: Communication Networks and Systems in Substations*; IEC: Geneva, Switzerland, 2004.
36. National Institute of Standards and Technology (NIST). *Framework and Road Map for Smart Grid Interoperability Standards*; Release 3.0; NIST: Gaithersburg, MD, USA, 2014.