International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 43-57
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Cybercrime and Risks for Cyber Physical Systems

2019

[1]Abel Yeboah-Ofori
School of Architecture, Computing & Eng.
University of East London
United Kingdom
u0118547@uel.ac.uk

[2]Dr. Jamal-Deen Abdulai
Dept. of Computer Science
University of Ghana
Ghana
jabdulai@ug.edu.gh

[3]Dr. Ferdinand Katsriku
Dept. of Computer Science
University of Ghana
Ghana
fkatsriku@ug.edu.gh

ABSTRACT

Cyber Physical Systems (CPS) is the integration of computation and physical systems that make a complete system such as the network, software, embedded systems, and physical components. Major industries such as industrial plants, transport, national grid, and communication systems depend heavily on CPS for financial and economic growth. However, these components may have inherent threats and vulnerabilities on them that may run the risk of being attacked, manipulated or exploited by cyber attackers and commit cybercrimes. Cybercriminals in their quest to bring down these systems may cause disruption of services either for fame, data theft, revenge, political motive, economic war, cyber terrorism, and cyberwar. Therefore, identifying the risks has become imperative in mitigating the cybercrimes. This paper seeks to identify cybercrimes and risks that are associated with a smart grid business application system to determine the motives and intents of the cybercriminal. The paper identified four goals to mitigate the risks: as business value, organizational requirements, threat agent and impact vectors. We used the Analytical Hierarchy Process (AHP) to determine the importance of the goals that contribute to identifying cybercrime and risks in CPS. For the results, a case study is used to identify the threat and vulnerable spots and the prioritized goals are then used to assess the risks using a semi-quantitative approach to determine the net threat level. The results indicate that using the AHP approach to identify cybercrime and risk on CPS provides specific risk mitigation goals.

KEYWORDS: Cyber Physical System, Cybercrime, Risk Mitigation, Smart Grid, Cyber Security, Analytical Hierarchical Process.

1 INTRODUCTION

CPS infrastructures and applications have brought economic, business and societal impact benefits nationally and globally in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. CPS is the integration and configuration of computation, network and physical processing systems that are embedded together and uses computers, sensors, actuators, and network monitors to control processes [1]. CPS technology integrates the dynamics of analysis and design, modeling, abstractions of physical processes with those of the software, hardware and network topologies and provides a (smart grid) system infrastructure. Cybercrimes are the actual crimes committed using computers and the internet to manipulate, delete, alter, redirect or compromise and the exploitations that are carried out including advanced persistent threats. They are more of the consequences and effects of cyber attacks and they include data theft, industrial espionage, intellectual property theft, ID theft, and DoS. Cyberattack is the physical attacks that are initiated against the CPS through remote penetration, brute force, spear phishing, and hacking and SQL injection attacks. The attack media include Remote Access Trojan (RAT), rootkit, botnet, cross-site scripting, session hijacking, IP spoofing, redirect script, spyware, ransomware, and others. Cyber attacks are carried out through many different forms of threat agent such as Trojans, viruses, botnets, spyware, and worms which are instrumental in facilitating certain cybercrimes. Cybercrime can be initiated from anywhere in the world on Network Control Systems (NCS) and Supervisory Control and Data Acquisition (SCADA) systems [2]. CPS are autonomous systems that make a decision in real time using agents and requires real-time availability of information.

CPS implementation has inherent challenges and vulnerabilities embedded in them due to the evolving organizational processes and the changing threat landscapes.

This has led to many problems such as poor requirements capturing, software errors, and misconfiguration and lack of risk assessments. These implementation challenges and vulnerabilities may run the risk of being exploited by cybercriminals in their quest to bring down the systems and cause disruption of services for fame, revenge, political motive, economic war, cyber espionage, cyber terrorism, and cyberwar. There have been recent cybercrimes such as Stuxnet attack [2] and Duqu malware [3]. Ukraine Power plant [4], Ransomware attacks on UK NHS [5] [6], Saudi Aramco power plant attack [7]. These cybercrimes have impacted greatly on the organizational business process and had had a socio-economic impact on these nation states. These perpetrators can cause zero-day attacks, evil maid attack, Denial of service attack, resonance attacks, and spyware, ransomware, spoofing, rootkit, and botnet attacks. Most organization integrates their systems with SMEs, suppliers, and distributors for business processes and service deliveries on a supply chain environment. However, most of the systems that these systems are not properly secured.

There are existing works that have looked at cybercrime and CPS risks, threats, vulnerabilities and attacks such as Nicol et al 2016 [8], Cardenas et al 2011 [9], Humayed et al 2017 [10], Wand & Lu 2013 [11], Sun et al 2018 [12], and Anderson et al. 2012 [13]. However, gaps exist such as poor requirements capturing that leads to misconfigurations especially on software that is bought off the shelf. Which also impacts on the network infrastructures that integrates with the cyber digital system. Also, none of the authors considered cybercrime and risk from evolving organizational threat landscape using the Analytical Hierarchical Process (AHP) [14]. This paper seeks to identify cybercrimes and risks that are associated with a smart grid business application system to determine the motives and intents of the cybercriminal. The paper considers business value, organizational requirements, and threat agent and impact vectors as the mitigation goals. The paper looks at the cybercrime and risk for CPS, and not cyber attacks. The main contributions of this paper are threefold: first, we identify threats and attacks that have the potential to cause cybercrime risk. We integrate concepts from CPS risk assessments, frameworks, standards, and controls required to understand the attacker's motives and intents. Secondly, we use the AHP method to determine the net risk levels on the organizational asset and pairwise comparisons for decision making in identifying the risks. We used the Analytical Hierarchy Process (AHP). [14], [15] to determine the importance of the goals. Finally, we used a semi-quantitative approach to determine the net threat level. The reason being that not considering the risk assessment will prevent the organization from achieving the goal. CPS platforms provide organizations the abilities run their businesses goals or objectives with third party systems cybercrime risk may prevent that. A case study is used to evaluate the comparative importance of the goals and equate the results. The results show that using the AHP approach to identify cybercrime and risk on CPS, provides specific risk mitigation goals.

The structure of the paper is as follows: section 1 looks at the background of CPS risk and cybercrime. Section 2 outlines the state of the art, an overview of CPS, attacks, risk, cybercrime. Section 3 looks at the methodology and study approach. Section 4: Implementation of the risk mitigation process and results. Section 5 discusses the risk mitigations goals, relative importance, net results, risk management, and limitations. Section 6 presents the conclusions and future works.

2 RELATED WORKS

This section reviews the papers and related works done for the state of the art that provides concepts to understand the recent trend of cybercrime and risks on CPS smart grid from organization context. For the paper, we define cybercrime, then review the start of the art of CPS attacks, threats, vulnerabilities and risks. Risk and Controls in CPS. Standards and Controls.

2.1 Cybercrimes

Cybercrime is any crime committed using computers, and the internet. Gordon & Ford 2006, [16], Shodhganga 2007 [17], posits that it

is only a cybercrime if the internet places a central role and not an incidental one. However, the Council of Europe defines cybercrime as offenses ranging from criminal activity against data to content and copyright infringement CoE 2001, [18]. Zappa 2014, defines cybercrime as a set of illegal operations that takes place on the internet [19]. UNODC 2013 defines cybercrime as the misuse of information resources and or the impact on them in the informational sphere for illegal purposes [20]. Trojans, Viruses, Bots, Spyware, and Worms, are instrumental in facilitating certain cybercrimes.

2.2 CPS, Infrastructure, Attacks, Threats, Vulnerabilities and Risk

In this section, we look at the overview of CPS and consider the concepts of CPS attacks, threats, vulnerabilities and risk management framework

2.2.1 CPS Smart Grid Infrastructure

CPS is an integration of the computation and physical process that makes a complete system [9]. CPS smart grid uses renewable energy resource distribution in an efficient and reliable way to provide demand and response intelligence [10]. The infrastructure comprises of the application system and network system. The applications integrate Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controls (PLC), Sensors, Actuators and other communication networks for electric power generation, distribution, and transmission [21]. SCADA system uses remote telemetric units (RTUs) and (PLCs) to monitor equipment across various substations, gather data in real time from the various sources and ensure proper control of network servers for business processes including input and output analyses [22]. The network application provides interfaces, interconnectivity and programmable logic required for implementing automation processes for the field devices and Home Energy Management Systems (HEMS) software. [23] [24]. We consider concepts from IEC 61850 and develop a diagram that integrates the electric power distribution systems.

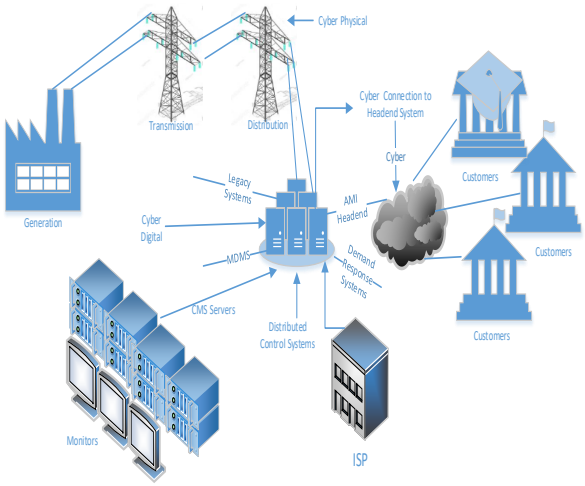

Figure 1. Proposed Smart Grid System Infrastructure

The supporting infrastructures include the integrations of intelligent devices that use various hardware and software components as well as communications networks to provide monitoring and controlling of the core business operations and processes for the energy management system [10] [24] [25]. According to IEC 61850, the smart grid uses Modbus and DNP3 network for field devices and advance protocols [27]. The control centers communicate with the field devices at various substations through wireless network protocols such as Inter Control Centre Protocols (ICCP) and TCP/IP.

2.3 Cyber Physical Systems Attacks

CPS attacks are those cyber attacks that include DDoS, Spyware and Ransomware attacks that could lead to various cybercrimes on the system such as industrial espionage and ID theft, data theft and data manipulations after gaining access to the system resources. CPSs have been at the core of national and international critical infrastructure and major industrial systems [2]. The increasing dependency on CPS has brought about the increased cybercrime attacks as these control systems become the backbone of every economy. There are various attack scenarios that can be initiated on CPS that could cause a zero-day attack. An attacker could insert malware or spyware into the software to exploit an unpatched vulnerable spot that is usually unknown to the vendor who bought the software

off the shell. The following are a few attacks that could be initiated:

2.3.1 Evil Maid Attack

An evil-maid attack is a security exploit that targets a computing device that has been left unattended or shut down. Here the evil maid who is mostly internal staff (a Corporate Spy) or (Industrial Espionage) attacker could boot the system with a boot loader or USB drive, installs a key logger and then captures encryption keys then uses it to steal data.

2.3.2 Resonance Attack

Resonance Attack is an attack that the perpetrator compromises some sensors or controllers that forces the physical system to oscillate at its resonant frequency. For instances, exploiting the zero-day attack vulnerability and then compromise the real timer systems and prevent the actuators from picking up the correct signals from the sensors thereby providing wrong information.

2.3.3 Denial of Service Attack (DoS)

DoS attack is a cyber-attack that the perpetrator interrupts the network in an unauthorized manner, disrupts services and denies authorized users from having access to the network resource affecting the control systems performance, especially in a distributed system. On a Wireless Network Control Systems, a perpetrator could cause optimal jamming attack which maximizes the linear quadratic Gaussian control in plants to affect the control system performance [28].

2.3.4 Malware Attack

Malware is a software program that propagates a network system and exploits vulnerable spots such as virus and Trojans. A malware attack 'Stuxnet' [2] was designed to target five Iranian Critical Infrastructures an Organizations suspected to be Uranium enrichment Infrastructures. The worm initially spreads discriminately, and have a highly sophisticated malware payload designed to target Siemens Supervisory Control and Data Acquisition (SCADA) systems configured to control and monitor specific industrial processes. Malware such as a random access Trojan attack the victims CPS remotely, hide and install itself as a payload without the victim's knowledge and obfuscate.

2.3.5 Ransomware

A malicious software virus designed to stop a system from functioning completely by encrypting the data and sending a message to the owner to pay a ransom amount before the data will be released. Consequences are that they cause financial loss, puts human health at risk and industrial sabotage Wanna cry attack [5]. Infected 230,000 computers in over 150 countries with NHS, Spanish Phone Company Telefonica, German State Railways and others. [6], Petya ransomware spread rapidly through network systems that use MS windows operating systems infected and subverts the Programmable Logic Control (PLC) on the industrial systems. [5].

2.4 Cyber Physical System Threats

A threat is anything that has the potential to cause harm and securing CPS from threats comes with its own challenges. Here we identify the threats that have the potential to cause general threats and then look at specific threats to CPS. Potential threats may cause a lot of damage and disruptions to the systems, and loss of data to organizations [9]. We identify five potential sources that a perpetrator can pose a threat. These are the source, target, motive, attack vectors, and potential consequences [10]. Threat source falls in three categories:

1. Social engineering is a threat that attackers us to deceive victims to release private information. The use that to cause DoS attack, panic, fear, and chaos.

- Unexpected threat or accidental threat, are threats that happen accidentally or through legitimate CPS components such as network system faults that lead to failures and down times.
- Target: Application components or users such as servers, network, and sensors.

1. Motives: A reason to launch an attack. Attacker's motives are revenge, economic,

political, create terror and panic, or cyberwar.
2. Attack vector: Attack method and trajectories used to deploy attacks successful such as interception, interruption, modification, and fabrication.
3. Consequences: Impact of the damage caused by the compromise of the CPS security triad confidentiality, Integrity, and availability, reputation, cyber industrial espionage.

2.4.1 CPS Threats Motives

The motives and intents of the cybercriminal determine the nature of an attack. To be able to ensure that CPS risks are assessed for proper mitigation, we look at attacks on CPS applications and methods that are specific to attacker's motivation, intentions, sources used, target, vector, and the impact.

- **APT Hacker: attackers (motive) is to cause APT attack:** Attacker carries out reconnaissance to identify (vulnerable spot) and penetrate the system and exploit the wireless capabilities (vector) and manipulate, control and disrupt operations (impact).
- **Financially Motivated (Motive):** Could be internal and uses social engineering or external remote attack (vulnerable spots) aim is to reduce utility bill and tariff, or divert money, hack into the system or inject false data (vector) cause system to record wrong utility data (target) and cause financial loss (impact).
- **Politically Motivated:** Passive espionage attack. The attacker uses spyware to gather intelligence remotely (vulnerable spots) carry out reconnaissance on targeted nation's critical infrastructures (target) and initiate malware (vector) to steal confidentiality information (impact).
- **Cyberwarfare**: military power (motive) initiated an attack from a nation (vulnerable spots) to cyberwar against another nation (target) by remotely attacking its critical infrastructures e.g., national grid or access field devices (vector) leading to power shut down sabotage, or economic loss (impact).
- **Physical System Attack:** (motive) on power plants or cause cyber terrorism: an attacker identifies (vulnerable spot) on CPS, could cause resonance attack sensor and actuators that measures the temperatures of a particular environment (target) manipulate and cause the system to to oscillate (vector) sending false data measurement to the control center or shut system down (impact) [9].

2.4.2 Advance Meter-Reading Infrastructure (AMI) Attack

The CPS Smart grid uses smart meter appliances to provide electric power to organizations and households. The AMI is a device that provides advanced energy monitoring and recording, data collection, and load management capacities of consumers to the organization. The AMI is a two-way communication system that can reach every device in a distributions space [10]. For instance, the electric power company may use AMI for reading digital meters and has a diagnostics port and a wireless adaptor embedded on the digital devices that interact with the meter's data for billing and diagnostics. The AMI takes the various data readings and sends them to the control system.

- An internal attacker could exploit the hard-coded password that is used to authenticate users. Then manipulate the development tools that integrate with HEMS and CMS application software that interfaces with the wireless mobile devices.
- A malware or DDoS attack can be initiated externally on the digital meter that is equipped with a diagnostics port and wireless interface meter readings.

2.5 Vulnerabilities

CPS Vulnerabilities are those spots on network nodes, link and the various endpoints on the infrastructures that could be exploited. These vulnerable spots are the firewalls, IEDs, IPs, HTTP headers, filters, Routers, network, Websites, password, and servers. Other vulnerabilities include inserting malware or spyware in software that is bought off the shelf.

2.6 Cyber Physical System Risks

The risk is the probability of an attack being initiated or something bad happening to the critical infrastructure. CPS risks include those threats that have the potential to cause harm to

the application processes, network, and physical infrastructures. We review works that considered assessing those risks as discussed in 2.3. Nicol et al 2016, proposed a risk assessment of cyber access to physical infrastructures in CPSs [8]. Cardenas et al. 2011, analyzed security mechanisms applicability and challenges to CPS for deterring attacks [9]. Wand & Lu 2013, presented a survey of cybersecurity issues for smart grid and highlighted cyberattacks from substation control systems [11]. Similarly, Sun et al 2018, review cybersecurity testbeds for research that demonstrates cybersecurity risks [12]. However, Axelrod 2013, proposed a model that determines CPS risk across a broad range of public and private sectors organization. [21]. However, the authors did not factor in cybercrime risks on the application systems.

2.7 Managing Cyber Physical System Risks

Managing CPS risk is a challenging task for industry adoption due to the heterogeneous nature of the CPS smart grid. CPS risks of cybercrime attacks include process failure, component failure or application failure as discussed in 2.5. Humayed et al. 2015 proposed a unified framework that consists of three orthogonal coordinates [10]. Wan & Al Farugue. 2015, proposed a framework for the design of secure control systems for CPS [29]. Al Faruque et al. 2010, proposed a security-aware model based on the design in methods to assess the security of CPS within four types of architecture level attacks [30]. Lewi 2002, reassess the risks of cyber threat on national critical infrastructures and highlights the set of issues that relate to cyber-terrorism and cyber-attacks on critical infrastructures [27]. The author posits that the premise of cyber terrorism is that as national infrastructures become more dependent on computer networks for organizational requirements and operations so are new vulnerabilities. However, the emphasis placed on cybercrimes such as manipulation, alteration, APT and exfiltration is not addressed.

2.8 Cybercrime Risk Controls and Standards

Cybercrime risks in CPS are inevitable, however, with risk assessments, analysis, and reviews in place, it could be managed in the event of any threat. CPS risk could prove more damaging to organizations due to its integrated nature should something bad occur that could impact negatively on an organizational goal. For us to have a risk on these CPS in a given situation, we need to have both the probable threats and vulnerabilities that when exploited, and could cause major disruptions. Shoukry et al 2013, devised a robust output feedback controller that is resilient to attacking the scheduling of packets in a network control system. [32]. Similarly, Kayode et al 2014 [33], proposed a formal model for risk management in cybercrime control systems. The framework recommended three steps namely, Risk Assessment, Risk Mitigation, and Evaluation. However, the framework does not include evolving threats and vulnerabilities such as Advanced Persistent Threats (ATP). Leyden 2017 [34], a proposed framework built on vulnerability disclosure, ISO/IEC29147-2014, to provide reports of security flaws consistent with what NCSC describe as an active cyber defense. Similarly, Gordon et al [35], proposed a three-step approach to cyber-incidence risk management framework to manage the risk arising from cyber incidents. However, the work did not include software vulnerabilities that can negate all the features proposed including resonance attacks and APTs that are evolving. NIST 2014 [36], proposed a cybersecurity framework that will provide collaboration between government and private sector to use common mechanisms to address and manage cybersecurity risks without placing additional regulatory needs on businesses. NIST 2017 [37], provides context on how an organization views cybersecurity risks and proposes four ties from Partial (Tier 1) to Adaptive (Tier 4) that align cybersecurity activities with its business requirements, risk tolerance, and controls. CIS Controls 2018 [38], provides a prioritized set of practices that mitigate attacks. ISO27005:2011 [39], provides information security risks applicable to application systems. ISO31000:2009 [40], provide risk management principles and guidelines for varying needs of an organization.

2.9 Existing Gabs

The related works revealed several gaps. In assessing risk, we observed that [8], [9], [11] analyzed security mechanism applicability and challenges to CPS, and did a survey of cybersecurity security requirements on the smart grid.

- However, the authors did not consider cybercrime threats to CPS application systems.
- Their works did not consider cybercrime risk from the integration of information and smart grid communication perspective.
- Existing the studies focused on the cyberattacks, not the cybercrimes

In managing CPS risks [10], [28], [29], [30], proposed different to managing risks. However, the work did not include:

- Identifying emerging threats and vulnerabilities in software bought off the shelf and cybercrime attacks such as spyware and APTs attacks that are evolving.
- The existing work did not consider attacks from SMEs, suppliers, and distributors who are more susceptible to cybercrimes.
- Exiting works relied more on cybersecurity for CPS attacks and not on cybercrime.

Based on our observations, our work seeks to assess cybercrime and risk from evolving organizational threat landscape using the Analytical Hierarchical Process (AHP). The paper identified cybercrimes and risks that are associated with a smart grid business application system to determine the motives and intents of the cybercriminal. The contributions of this paper discussed in section 1, includes using AHP and subjective judgments to identify and assess risks for decision makings. The paper contributes to using AHP method to determine the net risk levels for cybersecurity strategic planning, resource selection, resource allocation, and policy formulations. The results show that using the AHP approach to identify cybercrime and risk on CPS, provides specific risk mitigation goals.

3. METHODOLOGY

In this section, we adopt the AHP and semi-quantitative approach for the methodology based on the art and observations. We use CPS cyber-attack vectors to determine the risk levels as impediments of the mitigation goals. To determine their relative importance, we prioritize the goals using the Analytical Hierarchical Process (AHP) [14] [15]. The concept includes identifying tangible and intangibles assets and how much more one element dominates another in term of relative importance with respect to a given attribute. We quantify the attributes to be the cyber attack risks on the assets that need assessment to ensure the CPS are secure.

3.1 Analytic Hierarchy Process (AHP)

The AHP uses pairwise comparisons and relies on expert judgement to derive priority scales [14]. We use the AHP method to derive pairwise comparisons for decision making in identifying cybercrime risks. We evaluate the relative importance of the goals in 3.3 using expert judgment and semi-quantitative approach to determine the net risk level. The reason for using the AHP approach to identifying cybercrime and risks on CPS is that:

- AHP uses subjective judgements in decision makings. From an organizational perspective, AHP is used for cybersecurity strategic planning, resource, and budget allocation, audit purposes, policy formulations, and implementation. This may influence business value.
- From an implementation point of view, the AHP approach provides a logical risk assessment framework to determine the benefits of each alternative. The pairwise comparison matrix provides us the ability to determine the preferences of each alternative over another, hence, the results for determining organizational requirements are reliable.
- The reason for considering the mitigations goals is that cybercrimes threats are only identified after it has occurred. Organizations that intend to evolve their business on cyber supply chain platforms may use the AHP

approach as part of requirements capture.

3.1.1 The Rationale for Using AHP Approach for Cybercrimes and Risks for CPS

Most organizations integrate their systems with SMEs, suppliers, and distributors for business processes and service deliveries in the cyber supply chain environment [41] to achieve organizational goal. In CPS application developments, we look at people, process before the technology required to support the integration and processes. We believe using AHP and subjective judgements approach places more emphasis on people and processes to identify and assess risks for decision making and cybersecurity strategic planning. The rationales below are for assets, business, and socio-economic impact factors:

- **Impact on Assets:** cybercrime risks on SMEs in terms of their business assets, finance, socio-economic, and insurances are high as they are most susceptible to cyber attacks leading to cybercrimes and cascading effects. Webber 2003, posits that SMEs are the heart of every economic growth as they make up the social fabric [42]. However, these businesses are mostly the victims of cybercrime as they fail to deploy security policies to manage cyber risks and are used as targets to CPS systems in a supply chain environment. SMEs [19] make up 99% of all businesses in the EU employing 86.8 million people, equivalent to 66% of the workforce.
- **Financial Impact**: SMEs use inexperience IT personnel's, hence are prone to threats and vulnerable to attacks. Anderson et al. 2012 [13], looks at the infrastructures supporting cybercrime and proposed a framework for analyzing the cost of cybercrime against defense cost, direct losses, and indirect losses. Capgemini 2012 [43], estimated the global cost of cybercrime to $388 billion with a direct cash cost of $114 billion including money stolen and spent on attack resolutions. However, a study in 2009 estimated the cost of stolen intellectual property and expenditures for fixing the damage from the data breach to be $1 trillion.
- **Economic Impact:** According to Ponemon Institute, cybercrime has increased 22.6%, the average cost of cybercrime on 95% companies suffer 64% experienced web-based attacks, 44% experienced stolen or hijacked computing devices, and 42% on experience malicious codes attack. UK spent £27 billion per year loss to the UK economy on cybercrime. Approximately 80% or £21 million borne in companies. In Germany, the estimated cybercrime losses were 90 billion Euros in 2010. In a study conducted in five countries, Australia, France, Germany, UK and US, the cost per company arising from data breaches reached $4 million in 2010, a rise of 18% from 2009. However, these estimations did not factor in developing countries such as Africa, looking at the global and evolving nature of cybercrimes.
- **Business Impact:** WEF 2008, the report indicates that without adequate policies in place, the economic losses caused by cyber attackers could be up to $3000 billion by 2020 [21]. The impact was evident in the 2017 WannaCry and Petya Ransomware attacks. WEF highlighted the need to address cybercrime risks by all stakeholders. Hence, we use AHP to evaluate cybercrime risks.

3.2 Survey Context

Based on the understanding of the CPS security issues, we used IT security experts from an organization that uses smart grid systems. The participants were IT Directors, CISOs, IT managers, systems administrators, and technical experts. Online questionnaires were considered as well as face to face interviews in the case. Considering the nature of the questionnaires and the sensitive nature of cybercrime the question was generic to provide us the basics of threats and vulnerabilities.

3.3 CPS Risk Mitigation Goals

In this section, we compare the CPS risk mitigations goals qualitatively and quantitatively and follow the AHP approach to evaluate the relative importance. We compare the risk mitigation against these four goals: Business Value, Organizational Requirements, Threat Agent and Impact Vectors.

- **Business Value:** This includes organizational assets, market value, customer base, collaborations, business partners, market stance, directions, and system infrastructures.
- **Organizational Requirements:** Includes the activities and operational requirements needed for successful implementation of business objectives such as service delivery, policies, and procedures, service level agreements, roles, and responsibilities.
- **Threat Agent:** This goal identifies all the nature of threats, vulnerabilities, and attacks. The threats include phishing, spear phishing, cross-site scripting attack, session high jacking attacks, and SQL injections. The vulnerabilities include the spots that the threat agent could exploit such as the web servers, firewalls, DMZ, and IDS/IPS. Attack vectors include malware, ransomware, spyware, Advanced Persistent Threat (ATP) and DoS attacks that could be initiated in the threat landscape.
- **Impact Vectors:** This function considers all the probable consequences of the cyberattacks listed as the threat agents on the CPS. The impact includes loss of assets, revenue, reputation, expertise, customers, market stance and collapse of the business.

3.4 Risk Assessment Method

The study adopts a semi-quantitative risk assessment method to determine the risk level due to the invisibility nature of cybercrime.

Using a complete quantitative method to determine the risk probability values will be challenging for risk management. The Semi-quantitative risk assessment approach will assist in determining the relative importance of implementing the countermeasures to protect the CPS assets and the cost of alternatives. We calculate the net risk value expected based on the threat vectors of a particular attack on a system with the frequency of occurrence within a period to estimate the number of times a threat exploited would be successful on a vulnerability. Therefore, the risk assessment follows a semi-quantitative method to calculate the net risk values.

4 RELATIVE IMPORTANCE OF THE RISK MITIGATION GOALS

The study follows the AHP net risk mitigation calculation for the relative importance of the mitigation goals. [14], [15], based on an organizational context, each goal's relative importance level is compared with other goals. We use the scales of the (1-9). Refer table 1. (1) indicates extremely low risk in terms of the importance to a threat or an attack and (9) indicates extremely high risk in terms of its importance should a cyber-attack actually occurs on the CPS compared to another goal. Ones the importance levels of each goal is obtained compared to another, the Comparative Matrix (CM) levels are stabilized to determine the weight. The AHP method is used to calculate the ratio in the equation to confirm levels of consistencies. The weighted value should sum up to (1). Where the ratio is 10, it shows inconsistent and the value must be redefined [15].

Let:
CR: Consistency Ratio
CV: Consistency Vector
RV: Random Consistency Vector
CM: Comparison Matrix Value

Risk Mitigation Goals

- BV: Business Value
- OR: Organization Requirements
- TA: Threat Agent
- IV: Impact Vectors

4.1 Risk Mitigation Goals

The relative importance of the net risk mitigation calculation depends on the business value in terms of assets, organizational requirements in relation to (user, systems and operational requirements), the assigned vulnerability that the treating agent could exploit and the impact vector.

Table 1. Net Risk Relative Importance

Levels	Relative Importance Probability	Explanations
1	Extremely Low	Acceptable mitigation of two goals that contribute equally
3	Low	Moderate mitigation or slightly in favor of a goal over the other
5	Medium	Strong mitigation goal that favor one goal over the other
7	High	Very strong mitigation goal that its dominance demonstrate practice
9	Extremely High	Extremely High Evidence of favoring one mitigation goal over the other is clear
2, 4, 6, 8.	Variance	Intermediary values that determines oscillations between mitigations vectors

Table 2. Comparative Matrix

	Comparative Matrix Values				
		BV	**OR**	**TA**	**IV**
	BV	**9**	**7**	**5**	**9**
	OR	**7**	**1**	**7**	**5**
CM_i	**TA**	**5**	**3**	**1**	**9**
	IV	**9**	**2**	**3**	**1**

$$(CR)= \frac{CI}{RI} \quad (1)$$

Step 2: Net Risk Mitigation Calculations

The net risk mitigation calculations depend on the related threat agents (TA). The threat agents are the causes of risks factors that we need to determine the threat probability level and impact to estimate the outcome. Refer to table 2. Due to the invincibility nature of cybercrimes we use subjective judgment and consider the rules below [9], to support our estimations:

- Rule 1: Impact depends on the affected mitigation goal: were risk impacts mitigation goals such as business value and organization requirements, then the impact is deemed as high.

- Rule 2: Where the risk is higher than what the organization expects, we consider the risk factor it as extremely high.

- Rule 3: Subjective judgement is suitable for calculating the net risk as it assists in avoiding wrong estimations.

4.2 Net Risk Results

The net risk results has used the summation of the various levels of risk that impacts on the goals. We calculate the various level of risks and relative importance by risk mitigation goals. We apply the same approach to calculate the risk value, probability, and impact.

Let,
Ri: Value of Risk

ri: Individual risk factor value

ri1……riN: N influence risk factor of a risk Ri.

P(ri): Probability of risk factor ri….

Probability scales = low/unlikely (less than 0.30), medium/likely (0.30-0.49), high/critical risk (0.49--0.59), extremely/certainly high (above 0.60)

I: Impact of overall risk Ri

Impact scales = low(less than 0.30) medium (0.30--0.49) high (0.49--0.59) extremely high (above 0.60)

Rnet: Net risk of Ri

Rw: Relative weight of the affected mitigation goal [BV, OR, TA, IV] by Ri.

Risk level scales: low risk (less than 0.30), medium (0.30--0.49) critical risk (0.49--0.59), highly critical risks (above 0.60)

$$ri=P(ri) \times I \quad (2)$$

$$Ri= \frac{1}{N} \sum\{ri1, ri2, ri3\ldots\ldots,rin\} \quad .(3)$$

$$Rnet = \sum Rw \times Ri \quad (4)$$

4.3 Determining Risk Levels

Determining risk levels using AHP methods requires a tradeoff between the mitigation goals. Saaty [14], posits that in using AHP, decisions involve many intangibles and tangibles that need to trade off. To achieve that, we measured the decisions alongside tangibles and evaluated the measurements to determine how well they serve the objectives of the decision. We adopt the pairwise comparisons method to determine which risk level has a greater risk impact and requires mitigation. We determine risk level using table 1 as follows:

- **Low risk** of (less than 0.30) TA has minimal impact on BV: Implement security strategy to mitigate the risk such as formulation Policies, educating users, regular updates and constant monitoring of the threat.
- **Medium risk (**between 0.30-0.49) TA is considered moderate and needs constant monitoring and as it may never happen such a Zero-day attack, but when it does the consequences may cost system failure and financial impact.
- **High risk** (between 0.49-0.59) OR process needs to be evaluated to mitigate TA: Indicates has a high impact factor and effect on the CPS and requires security reviews to mitigate the risk. Developed a plan for the execution of the control measures within a specific period. Implement controls to counter such cyber-attacks as DoS Attack, APT, spoofing, evil-maid attack. The risk management process includes having countermeasures in places such as regular backups, regular updates, insurance, training and awareness workshops and adoption of cloud services.
- **Extremely High risk** (above 0.60) TA could impact on BV with high impact factor on IV and implies that identified control measures on the CPS for the risks are required to be implemented immediately with a contingency plan. This could cause financial loss, economic, trust and reputation damage to the organization. The countermeasures are required for such attacks resonance attacks, ransomware attack and malware attack that may sabotage the systems.

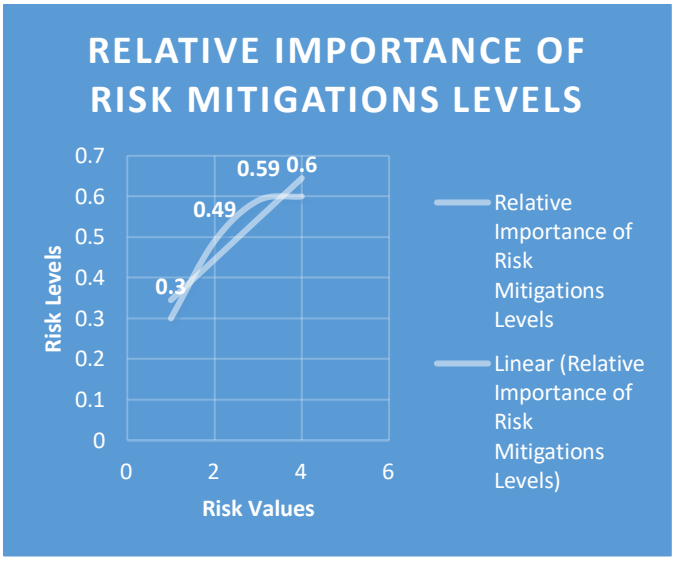

Figure 2. Relative Importance of Risk Mitigation Goals

5 IMPLEMENTATION

In this section, we use a case study to evaluate the likelihood of cybercrime risks on the smart grid. The goal is to determine the level of risk associated with each of the mitigation goals in the event of a cybercrime.

5.1 AHP Participants

Based on the understanding of the CPS security issues, we used IT security experts from an organization that uses smart grid systems. The participants were IT Directors, ISOs, IT

managers, systems administrators, and technical experts.

5.2 Case Study Context

An electric power distribution network communication system uses mesh topologies and SCADA systems as the main infrastructures that support the CPS smart grid system. The organization uses Customer Management Systems (CMS) the application system that integrates the core business objectives. The systems include customer data records, billing systems and bill payment transactions to electronic transaction systems, and banking services.

The organization found out that an intruder has penetrated the network server remotely through the public facing IP service that is used for the prepaid and post-paid service network system. The organization also outsources its sensitive customer data, financial information, business strategy, and organizational structures to third party companies, data centers and vendors for storage, processing, analysis and aggregation for business decisions.

5.3 Asset Identification

Assets identification is the process of documenting all the critical infrastructures of the CPS. Organizational assets are the staff, data, servers, infrastructures that when put together could be used to achieve an organizational goal or the business value. These assets are tangible and intangible assets that could be affected and various cybercrimes that can be committed. In the risk management process, asset identification is critical in carrying out risk identification and assessment.

Table 3. Identification of Assets, Vulnerable Spots, and Cybercrimes

Assets	Vulnerable Spots	Cybercrimes
Smart Grid	Network/ Firewall	DDoS, Resonance
Network System	Sub Station / IPs / Firewall	RAT, Firewalls
CMS	Password/Remote Penetration	ID Theft, Data Theft
Servers	Web Server/Mail Server	Spear Phishing / IP Spoofing
AMI/Handheld Devices	IP Address	Data Manipulation/ Redirect Scripts
HEMS	Password	Alter Billing Systems
SCADA/RTU	Network/Server	Rootkit / Botnet
Prepaid Systems	Website/IP Address	RAT, Session Hijacking

5.4 Threat Identification

Threats are those cyber attacks that have the potential to cause harm to the CPS application systems. We identify those threats as malware, spyware and ransomware attacks that could cause security effects as confidentiality, integrity, availability, accountability, and non-repudiation to the business value. Threat identification assists in risk categorization, risk analysis to determine the likelihood and impact, and for monitoring and control.

5.5 Results

Figure 3 below, depicts the relative importance of risk mitigation goals from the weighted value of the scenario. The prioritized risk is the business value with a weighted value of 70% as it determines the organizational goal and the needed to secure it is critical. Organizational requirements have a weighted value of 55% as it determines the organizational business processes including the user, system and operational policies required to ensure business values are achieved. Threat agent has a weighted value of 45% and it is used to in ensuring business continuity. Failure to identify those threats agents in line with the organizational requirements could cause threats such as malware, spyware and ransomware attacks. The impact value has a weighted value of 60% as the impact could cause security effects such as confidentiality, integrity, availability, accountability and repudiation issues to the business value.

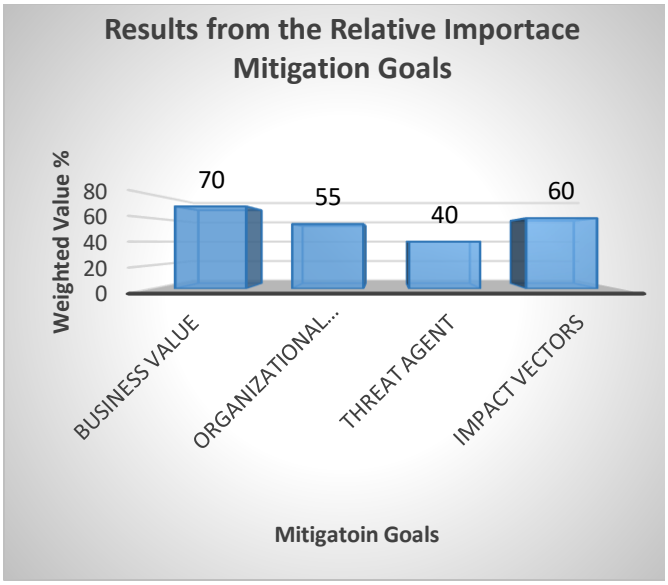

Figure 3. Results of the relative importance of risk mitigation goals from Scenario

5.6 Comparisons of the Results

This section summaries the findings of both the state of the art and the results. Most of the literature justify the need for a considering cybercrime and risk for CPS. Our results and scenario identified the risks and critical areas as well as the related mitigating goals. The results of the case studies and risk mitigation goals indicate that the relative importance of the mitigation goal is subjective to the organizational assets and the associated risk as listed in table 3. Moreover, mitigating factors such as standards and legislative frameworks also affect mitigation goals. Participants agreed that penetration testing, auditing, regular updates, and segmentation are key requirements to prevent and reduce downtime in the event of cybercrime attacks.

- .**Business Value:** The results reveal that risks on the BV are extremely high as any cybercrime on the organizational assets, could impact on finance, trust, collaborations, business partners and the smart grid system infrastructures. To mitigate cybercrimes, the organization must ensure that it uses the deep packet inspection firewalls that is able to detect attacks from all the suppliers, third party vendors, and SMEs. The IEDs becomes vulnerable when the firewall is not able to detect and prevent intrusions and can lead to attacks such as DDoS and Resonance attacks that causes oscillation to the power supply and utility readings.
- **Organizational Requirements:** The results show that descriptions of the processes and constraints that are generated during the requirements engineering phase form the basis for the system developments. These processes and constraints are statements that support the user requirements and system requirements used to achieve the organizational goal. The use of activities and operational requirements are needed to identify risk factors that can affect business objectives. The user requirements capture operational constraints, the system requirements set out the detailed functional and service constraints about what the customer requires from a system and the constraints under which it operates. This details will be used for risk assessments to manage risk, implement policies and procedures, service level agreements, roles, and responsibilities.
- **Threat Agent:** The risk to confidentiality, integrity, and availability of organizational assets is as the result of the combination of the threat agent, the vulnerabilities that the threat agent could exploit and the impact on the smart grid. To identify the mitigating factors, the goals that identify all the nature of threats, vulnerabilities, and attacks as listed in.4.1.
- **Impact Vectors:** the probable consequences of the cybercrimes are determined by the likelihood of the threat and the level of impact. The impact of cybercrime on the organization will cause loss of assets such as intellectual property, revenue loss as a result of meter tampering, reputation damage through distrust, loss of customer confidence.

Controls must be established to mitigate the cybercrimes. Although this paper did not focus on CPS risk management, we recommend standard that we may adopt to assist in preventing network intrusions that could lead to cybercrimes. The organization must carry out penetration testing on the distributed network, subnets and substations communication networks to identify all the vulnerable spots on a regular basis especially on the public facing IP addresses. There are organizations that provide

risk management and controls such as NIST Critical Infrastructure Framework, ISO 27002 ISMS, ISO 31000 Risk Management, IEC 61850.

6 CONCLUSION

Cybercrime and risks on CPS are on the increase and its impact on business processes are unquantifiable. There are many challenges facing organizations in their quest to mitigate cybercrime risks. The paper identified cybercrimes, and threats that the attacker could deploy and the vulnerable spots to exploit on the smart grid application system in an organizational business process environment. Due to the invincibility of cyber attacks, and the complex integration of CPS, identifying the potential sources that a perpetrator can exploit provides an understanding of the threat, motives, and intents of the cyber attacker in mitigating risks. Cybercrime risks in CPS are inevitable, however, with risk assessments, analysis, and reviews in place, it could be managed in the event of any threat. Using the AHP method, subjective judgment, expert opinion and semi-quantitative methods to identify the vulnerable spots, target, motive, attack vectors, and potential consequences assist in assessing cybercrime risks. An organizational goal determines the type of risk mitigation goals. We used BV, OR, TA, and IV to determine the results. The prioritize risks and the threat levels assist in cybersecurity strategic planning, resource selection, budget allocation, and policy formulations. The results were determined by the relative importance of the risk mitigation goals. The results revealed that CPS attacks are imminent and require further studies that look at the evolving nature of cyber crimes. Therefore, to mitigate CPS risks, it is important to provide a risk management framework that is able to support specific organizational goal and objectives. Further research is required to determine the relative importance of CPS risk management considering the changing cybercrime threat landscapes.

6.1 Future work

The paper focused on cybercrime and risks on CPS and discussed security threats, attacks risks, and vulnerabilities. Future works will look at CPS smart grid attacks, machine learning, and decision trees in cybersecurity and a comprehensive risk management approach to CPS.

REFERENCES

1. Lee, E. A., Seshia S. A.: Introduction to Embedded Systems – A Cyber-Physical Systems Approach. (2011).
2. Falliere, N., Murchu, L. O., Chien, E.: W32. Stuxnet Dossier. White Paper, Symantec Corp. Security Response. (2011).
3. Chien, E., Murchu, L. O., Falliere, N.: W32. Duqu. The Precursor to the Next Stuxnet. In Presented as Part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA. (2012).
4. Zetter, K.: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. (2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hackukraines-power-grid/.
5. Controller and Audit General: Investigation: WannaCry cyber-attack and the NHS. Department of Health. National Audit Office. UK (2017).
6. Symantec. Petya Ransomware Outbreak: Here's what you need to Know. Symantec Security Response. (2017).https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper
7. Groll, E.: Cyberattack Targets Safety Systems at Saudi Aramco. Foreign Policy. (2017). http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safetysystem-at-saudi-aramco/.
8. Nicol, D. M.: Risk Assessment of Cyber Access to Physical Infrastructures in Cyber-Physical Systems. (extended abstract of CPSS-16 Keynote Address). (2016).
9. Cardenas, A. A., Amin, S., Lin. Z., Haung, Y., Huang, C. Sastry, S.: Attacks against Process Control Systems Risk Assessment, Detection, and Responses. In Proceedings of the 6th ACM. SICCS, page 355-366. (2011).
10. Humayed, A., Lin, J., Li, F., Lou, B.: Cyber Physical Systems Security – A Survey. (2017). https://arxiv.org/pdf/1701.04525.pdf
11. Wang, W., Lu, Z.: Cyber Security in Smart Grid: Survey and Challenges. (2013). https://research.ece.ncsu.edu/netwis/papers/12WL-COMNET.pdf
12. Sun C., Hahn, A., Liu, C.: Cyber Security of a Power Grid: State of the Art. Electrical Power and Energy System. 2018. 99. 45-56. Elsevier. (2018).
13. Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M. J. G. Levi, M. Moore, T., Savage, S.: Measuring the Cost of Cybercrime. Computer Laboratory, University of Cambridge. (2012).
14. Saaty, T. L.: 208. Decision Making With the Analytical Hierarchical Process, International Journal of Services Science. (IJSSCI). Vol. 1, No. 1. (2008).
15. Islam, S., Fenz, S., Weipi, E, Kalloniatis, C.: Migration Goals and Rick Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners. IJSSE. (2016).

16. Gordon, S. & Ford, R.: On the Definition and Classification of Cybercrime. Springer-Verage Journal In Computer Virology.2006.
17. Shodhganga: Cyber Crime: A Conceptual and Theoretical Framework. Available on: http://shodhganga.inflibnet.ac.in/bitstream/10603/24790/7/07_chapter%201.pdf
18. Council of Europe: CoE. 2001. Convention on Cybercrime: European Treaty Services, No. 185. Budapest.
19. Zappa, F.: Cybercrime: Risk for the Economy And Enterprises At The EC And Italian Level. United Nations Interregional Crime and Justice Research Institute (UNICRI), 2014.
20. UNODC: United Nations Office on Drugs and Crime: Comprehensive Study on Cybercrime. Austria. 2013.
21. WEF: The Global Risk Report: (2018). https://www.weforum.org/reports/the-global-risks-report-2018
22. Marion, N. E.: The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation. International Journal of Cyber Criminology. University of Akron, USA. Vol 4. Issue 1&2. (2010).
23. Symantec. The Elderwood Project: Zero Day Exploits. (2012).http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood project.pdf
24. Verma, V., Chundri, P.: Enforcing Opacity in Cyber Physical Systems Using State Machine Models. (2016).
25. Tabuada, P.: Secure State-estimation and Control of Cyber-Physical Systems. Cyber-Physical Systems Laboratory. Department of Electrical Engineering. University of California at Los Angeles. UCLA. (2016).
26. Zhu, Q., Basar, T.: Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems. 5th IEEE Conference on Decision and Control and European Control Conference. (2011).
27. Zhu, Q., Basar, T.: Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems. 5th IEEE Conference on Decision and Control and European Control Conference. (2011).
28. Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal Denial-of-Service Attack on Scheduling Against Linear Quadratic Gaussian Control. American Control Conference (ACC). Portland, Oregon. USA. (2014).
29. Wan, J., Canedo, Al Faruque.: Security-Aware Functional Modelling of Cyber-Physical Systems. 20th IEEE International Conferences on Emerging Technologies & Factory Automation. ETFA. (2015)
30. Al Farugue, M., Regazzoni, F., Pajic, M.: Design Methodologies for Securing Cyber-Physical Systems. (2010).http://people.duke.edu/~mp275/pubs/CODES_ISSS15.pdf
31. Lewis, J. A.: Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats. CSIS. (2002). https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats
32. Shoukry, Y., Araujo, J., Tabuada, P., Srivastava, M., Johansson, K. H. Minima.: Control for Cyber Physical Systems under Network Packet Scheduling Attacks. Physical Science and Engineering. (2013).
33. Kayode, A. B. Arome, G. J. Oluwatoyin, O., Daramola, O. A.: Modelling of Risk Management Procedures for Cybercrime Control Systems. Proceedings of the World Congress on Engineering. London. UK (2014)
34. Leyden, J.: UK vuln 'fessing pilot's great but who's going to give a fol? (2017) https://www.theregister.co.uk/2017/03/22/uk_gov_vuln_disclosure_pilot/
35. Gordon, L. A., Loeb. M. P., Sohail, T.: A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM. University of Maryland. USA. https://dl.acm.org/citation.cfm?id=636774 (2003).
36. NIST. Framework for Improving Critical Infrastructure Cyber Security. National Institute of Standards and Technology. Version 1.0 (2014)
37. NIST 1500-203. Framework for Cyber-Physical Systems. (2017). https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=924021
38. CIS Controls.: Basic Organizational Foundational; Ver. 7; Center for Internet Security: East Green Bush, NY, USA, 2018.
39. ISO.: Risk Management Principles and Guidelines; ISO31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.
40. ISO.: Information Technology Security Risk Management. ISO/IEC 27005: International Organization for Standardization: Geneva, Switzerland, 2018.
41. Yeboah-Ofori. A., Islam, I.: Cyber Security Threat Modeling for Supply Chain Environment. MDPI, Future Internet. 2019.
42. Capgemini. Using Insurance to Mitigate Cybercrime Risk. Challenges and Recommendations for Insurers. https://www.capgemini.com/wpcontent/uploads/2017/07/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf
43. Webber, A. M.: The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal. Volume 18. Issue 1. 2003.