Journal of Universal Computer Science, vol. 25, no. 11 (2019), 1478-1502
submitted: 14/2/19, accepted: 30/8/19, appeared: 28/11/19 © J.UCS

Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure

Halima Ibrahim Kure
(School of Architecture, Computing and Engineering, University of East London
United Kingdom
h.kure@uel.ac.uk)

Shareeful Islam
(School of Architecture, Computing and Engineering, University of East London
United Kingdom
shareeful@uel.ac.uk)

Abstract: Cyber-attack is one of the significant threats affecting to any organisation specifically to the Critical Infrastructure (CI) organisation. These attacks are nowadays more sophisticated, multi-vectored and less predictable, which make the Cyber Security Risk Management (CSRM) task more challenging. Critical Infrastructure needs a new line of security defence to control these threats and minimise risks. Cyber Threat Intelligence (CTI) provides evidence-based information about the threats aiming to prevent threats. There are existing works and industry practice that emphasise the necessity of CTI and provides methods for threat intelligence and sharing. However, despite these significant efforts, there is a lack of focus on how CTI information can support the CSRM activities so that the organisation can undertake appropriate controls to mitigate the risk proactively. This paper aims to fill this gap by integrating CTI for improving cybersecurity risks management practice specifically focusing on the critical infrastructure. In particular, the proposed approach contributes beyond state of the art practice by incorporating CTI information for the risk management activities. This helps the organisation to provide adequate and appropriate controls from strategic, tactical and operational perspectives. We have integrated concepts relating to CTI and CSRM so that threat actor's profile, attack detailed can support calculating the risk. We consider smart grid system as a Critical Infrastructure to demonstrate the applicability of the work. The result shows that cyber risks in critical infrastructures can be minimised if CTI information is gathered and used as part of CSRM activities. CTI not only supports understanding of threat for accurate risk estimation but also evaluates the effectiveness of existing controls and recommend necessity controls to improve overall cybersecurity. Also, the result shows that our approach provides early warning about issues that need immediate attention.

Keywords: Cybersecurity, Cyber Threat Intelligence, Cyber Security Risk Management, Critical Infrastructure, Security Control
Categories: H.4.0, K.6.5

1 Introduction

Critical infrastructure (CI) is vital for any country to function, and its reliable operations are essential upon which daily life and the government operations depend. CI system is complex by its inherent nature, and the interdependent among various components (people, processes and technology) have made it a prime target for the criminals. The

cyber-attack landscape for such system is evolving at a rapid rate. Attacks are now multi-vectored and well organised. This makes the CSRM (CSRM) task more challenging in terms of understanding the risks due to evolving threats and mitigation of the risks materialized by these threats. It is therefore necessary to gather information about the threats likely to affect the organisation [Bromiley 16]. Cyber Threat Intelligence (CTI) deals with the collection and analysis of information by an organisation about the potential attacks that threaten the safety of its assets. Such information is used to identify cyber threats and helps organisations to respond accordingly [Reveron 12]. It provides evidence-based knowledge about the threat and turns unknown threat to known threat. CTI can support not only the CSRM activities but also supports the organisation with the strategic, tactical and operational decision for improving overall cybersecurity. Recent survey result from cybersecurity professionals by [Poller and Oltsik 18] shows that improve risk management efficiency and effectiveness is the top-ranked objective of the CTI program. Despite the significant efforts in developing methods for CTI, there is a lack of consideration of CTI information for effective cybersecurity risk management decision making.

Within the above context, we consider using CTI extensively for improving existing CSRM practice focusing on critical infrastructure. Specifically, the novel contributions of this paper are in three folds: Firstly, a unified approach to integrate CTI with cybersecurity and risk management activities. We consider concepts relating to CTI such as threat actor, tactics, techniques and procedures (TTP), indicator, and incident and integrate with the CSRM concepts such as actor, vulnerabilities, assets, risks, and controls and finally link with the CI. The unified approach considers relevant widely used industry standards and practices to analyse the risks and select controls to mitigate the risks. Secondly, the approach considers a holistic view of critical infrastructure cybersecurity context from a strategic, tactical and operational perspective so that organisation can consider the right level of controls for the improvement of overall cybersecurity. Finally, we evaluate the unified approach through a real life case study involving CI. The result suggests that organisations dealing with CI should adopt CTI for improving CSRM activities in detecting and responding to both known and unknown threats and support determining the right risk level. Furthermore, CTI also supports in identifying the system weakness and attack trends; the result from the examples outlines the applicability of the proposed approach.

2 Related work

This section presents existing works in various CI areas including cybersecurity, cyber-physical systems (CPS), risk management and CTI, which are related to our work.

2.1 Cyber-Physical Systems and Security Risk management for Critical Infrastructure

CPS is real-time and robust independent systems with high-performance requirements for maintaing CI services[Wu ei al 2015]. They are widely used technological systems in many CI application domains, including power grid system, defence, nuclear, oil and gas, transportation, and healthcare systems. Cyber-attack is one of the significant threats that affects critical infrastructure because of its complexity and

interdependencies among the various technological system components of CPS [Kim and Kumar 13]. To evaluate cybersecurity risk of CPS, a significant number of research works have been published in this area. An integrated cybersecurity risk management framework to assess and manage risks for CI is proposed, but effectivessnes of control is not addressed [Kure et al. 18]. Generally, CPS depends on the deployment of information and communication technology (ICT) to support new communication and control functions; this dependency expands risk from cyber-attack. This requires the development of testbeds to analyse the complex relationships between the cyber-based control mechanisms and the physical systems. However, various mitigation efforts through both cyber and physical approaches need to be exploited from more sophisticated attacks [Hahn et al. 13]. The systematic deployment of CPS in manufacturing industries within which information from all related perspectives is carefully monitored and synchronised between cyber and physical components [Lee et al. 15]. As described in [Ray et al. 10], the necessity of a unified approach includes models, methods and technologies to provide a correlated view of CI specifically power systems and cyber impacts. A risk-based methodology is proposed to assess security management systems which were applied to railway infrastructure.

2.2 Cyber Threat Intelligence

CTI is the provision of evidence-based knowledge about existing or potential threats, and determining the effectiveness of control capabilities [Chismon and Ruks 15]. CTI aims to obtain unstructured and ad-hoc sources of information that is made publicly available and analysed the information for making informed decisions. With CTI as an advanced concept, organisations faced with numerous malware variants can prevent security breaches before they occur [Kao and Hsiao 18]. Also, the increasing number of cyber-attack requires that cybersecurity and forensic specialists detect, analyse and defend against the cyber threats in almost real-time [Dehghantanha et al. 18]. To further advance the understanding of the concept of CTI, a much-needed definition of CTI is presented by creating a model of the intelligence creation process thereby not only improving communication between different intelligence teams but also the defensive posture of the company and the general safety of the cyber domain [Planqué 18]. A taxonomy for classifying threat sharing standards is proposed using an abstracted framework. The aim is to decompose these standards and analyse dependency and interoperability within the current cyber threat sharing communities. This holistic approach automates the sharing of threat intelligence, which can only be successful if tomorrow's attacks are well handled [Burger et al. 14]. However, some challenges relating to CTI is identified such as threat data being overloaded, quality of threat data that is shared amongst community members, privacy and legal issues which governs the lawful sharing of data and the interoperability issues faced by threat sharing platforms and standards used by the platforms. With all these challenges, adopting CTI by organisations to help them minimise future threats still outweighs its lack of adoption [Abu et al. 18]. Therefore, it is critical to integrate various CTI gathered from community resources, past security breaches, open source intelligence to improve better the ability to prevent and detect attacks in organisations with CI. Additionally, organisations implement countermeasures to future attacks because timely dealing with a large number of attacks is not possible without intensely perusing the attack features

and taking similar intelligent defensive actions, this, in essence, defines the notion for CTI.

This section presented a summary of works that have proposed different solutions towards addressing cybersecurity issues in critical infrastructures and the importance of CTI to support organisations. These works already advocated the applicability of CTI for understanding the threat and undertaking informed decision. However, despite these significant efforts, there is a limited focus on the integration of CTI information to improve risk management practice. CI struggle to detect threats due to their concealed and complex nature. Therefore, organisations need visibility beyond their networks and information about the threat traces left behind. Traditional CSRM begins by knowing a background profile of assets, vulnerabilities, threats and then estimate risk severity. Our work takes into consideration CTI information to improve CSRM with its enhanced visibility; organisations can gain improved insight into ongoing exploits, identification of cyber threats and the threat actors behind them. It is necessary to analyse the risk, considering the CTI information so that appropriate control can be identified. Our work fills this gap by proposing a unified approach that integrates CTI concepts with the existing risk management practice for all domains of CI.

3 Unified Approach

For an effective risk management practice in the critical infrastructure domain, it is necessary to understand threats before calculating the risk level. The proposed unified approach advocates using CTI information for the CSRM practice in CI. CTI provides evidence-based information about the threat which can support determining the level of risk so that appropriate control can be considered for the risk. Figure 1 shows the CTI information and its integration for the CSRM. This provides organisations with a comprehensive view of threats and associated risks. In essence, risk management needs to know the detailed threat information, including the threat actor's profile (skill, location, motivation), resources and TTP used to execute the threat. This information is essential for not only accurately estimate the risk but also to evaluate the vulnerabilities of affected critical infrastructure and the effectiveness of the existing control. Towards improving CSRM, we consider the necessary levels of maturity and see where the organisation sits and then begin to make improvements proactively. The different levels include initial, developing, defined, managed and optimising levels.

We consider CTI from a strategic, operational and tactical perspective to support organisations in the attainment of business objectives and to control risks effectively. The strategic plan embodies the functionalities and services that support organisations in attaining their business objectives and long-term goals. This includes information about who is responsible (threat actor), why they carried out the attack (campaign) and the process in which they carried out the attack (TTP). All this information helps the organisation in analysis and information that can help them understand the type of threat they are defending against. The organisation's security team can plan for adequate resources needed to protect and mitigate both current and future threats. The tactical plan deals with what threats the organisations should look for in networks and systems and why (indicator). This threat information is derived from real-time monitoring including which domains have been taken over by threat actor and affected systems. This information helps organisations to take tactical decisions. The operational plan

informs day-to-day decision making, resource allocation and prioritisation of tasks which includes trend analysis, showing the technical direction such as; where has the threat been seen (incident), what can be done (controls), and what weaknesses does the threat exploit (vulnerability).

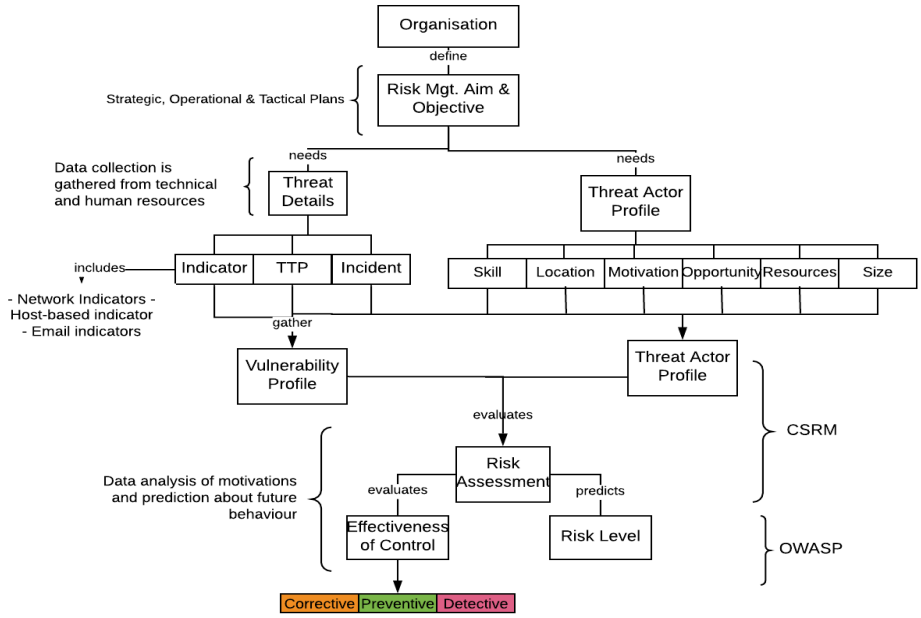

Figure 1: Integration of CTI with CSRM

The unified approach considers the existing widely used standard and practices such as Structured Threat Information Expression (STIX) for CTI, Common Weakness Enumeration (CWE) for communicating the impacts of vulnerabilities, Open web application security project (OWASP) provides basic techniques to protect against web application security challenges, NIST SP800-30 and ISO 27005:2011 for risk management guidelines and CIS_CSC for control as shown in figure 2 below. The reason for considering these methods is because they are accepted standards whose goal is to raise awareness about the application of security by identifying some of the most critical risks facing organisations with cyber functions. Note that, even though these approaches are used by the unified approach, but our contribution is beyond these existing works and focuses on improving critical infrastructure risk management practice by using CTI information. Our approach supports analysing risks by considering the attacker's profile and the evolving threat landscape. This makes our work different from STIX, which emphasises on analysing the threat profile and share this information. However, our work uses CTI has a clear and critical role in improving CSRM to identify, assess, and track threats as well as evaluate existing vulnerabilities in light to those threats. Integrating CTI with CSRM helps the organisation to analyse and determine the likelihood and impact of risk.

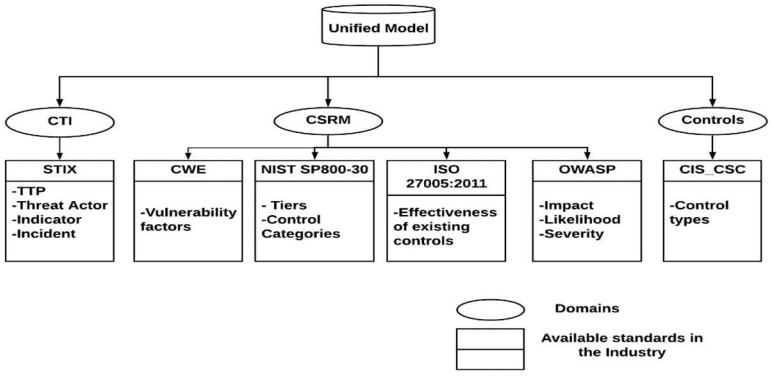

Figure 2: The Components of the Unified Approach

3.1 Cyber Threat Intelligence Models

CTI: For organisations to respond to their specific threats and make informed decisions on which countermeasures to deploy, it is necessary to have a detailed threat information.

STIX Model: STIX model represents structured threat information, which is meant to convey the full range of CTI [Barnum 12]. STIX is actively being adopted or considered for adoption by cyber threat-related organisations, and this helps organisations to understand the true nature of threats to make intelligent defensive decisions. For a valid defence against current and future threats, it is necessary to understand threat actor's behaviour, capability in the form of tactics, TTP and the threat actor's intent. Therefore, we adopted some of the STIX properties such as TTP, threat actor, indicator and incident and integrated them with CSRM concepts to improve CSRM in CPS.

3.2 Cyber Security Risk Management Standards

We consider two widely accepted risk management standards i.e., NIST SP800-30 and ISO 27005:2011, CWE for understanding the underlying weaknesses. OWASP methodology is also used for determining the impact of risks because it estimates risks from and technical perspectives and it is also highly adaptable and applicable to most organizations of any sizes.

Common Weakness Enumeration (CWE): CTI seeks to understand and characterise of vulnerabilities, misconfigurations or weaknesses that are likely to be targeted. It introduces common weakness scoring system (CWSS) which provides a mechanism for prioritising software weaknesses in a consistent, flexible, and open manner. It is a standardised approach for characterising weaknesses and thereby allowing organisations to make more informed decisions during the risk management phase and give attention to higher risks [Martin 07].

NIST SP800-30: Risk assessments support risk response decisions at the different tiers of the risk management hierarchy. We implemented the three different tiers proposed by the standard. The Tiers focus on the organisational operations, assets and individuals and selection of standard controls. Also, we adopt the different types of

control categories presented in the standard to help us categorise our controls into preventive, corrective or detective [Stoneburner et al. 02]. This helps the organisation to prioritise controls based on the severity of risks.

ISO 27005:2011: considers risk management as an integral part of the overall organisational processes, including evaluating the effectiveness of controls [ISO and Std, 11]. We consider identifying the existing controls and their effectiveness by following this standard.

OWASP: To ensure consistency and relevance of risks and their impact, we adopted the OWASP risk methodology [Open Web Application Security Project 14]. This methodology helps organisations to estimate risk from business and technical perspectives. Many factors that make up the likelihood and impact of each risk is included; therefore, the severity of risk is determined.

3.3 Controls

Risk controls are generic fundamental technical or procedural methods that are used to manage security risks.

The Centre for Internet Security Critical Security Controls (CIS_CSC): CSC_CIS provides 20 controls categorised into three prioritised areas [Centre for Internet Security 18]. They provide a prioritised set of actions that mitigate the most common attacks against systems and networks and can be applied for CI sectors. It also provides adequate controls that organisations should take to block or mitigate known attacks into their defensive cybersecurity portfolio.

4 Framing Concepts

This section presents an overview of the concepts necessary for the integration of CTI to improve CSRM. These concepts are linked with each other to support vulnerability assessment, threat identification, risk management, and analyse the effectiveness of controls. The concepts incorporate many standards for enhancing cybersecurity and concentrates on providing a comprehensive means for assessing threats in organisations. Therefore, we consider asset, threat and vulnerability factors from the widely used standards to calculate risk likelihood and impact. An overview of the concepts used by the proposed approach is given below.

4.1 Actor

For an organisation to achieve its goals, it is necessary to identify its key stakeholders that carry out various tasks and their contributions. They are highly significant in enabling the organisation to manage the process of the proposed approach, as well as preventing potential conflict of interests [Dietz and Hoogervorst 18]. There is also an external actor in CI, such as third-party vendors who are responsible for delivering various services. These actors are also considered for the approach.

4.2 Threat Actor

Threat actors are a particular type of actor with malicious intentions to execute the cyber attack [Abomhara (15)]. CTI considers various threat actor profile, including skill,

motivation, location along with resources and opportunity to understand the attack and its trend. Table 1 shows the weight of each threat actor profile, which is used for calculating the risk event likelihood by following the OWASP methodology. The threat actor factors that can help organisations to determine risk likelihood. Each factor has a set of options with a likelihood rating from High =3, Medium =2 and Low = 1 as shown in table 1 below.

Threat Actor factors	**Description**	**Likelihood Rating** **Weight/Value**
Skill level	How technically skilled is the threat actor?	3 (Advanced computer user)
		2 (Some technical skills)
		1 (No technical skills)
Location	Through what channel did the threat actor communicate to reach the vulnerability?	3 (Internet)
		2 (Adjacent Network)
		1 (Local /physical Network)
Motivation	How motivated is threat actor to find and exploit vulnerability?	3 (High reward)
		2 (Possible reward)
		1 (Low or no reward)
Resources	What resources are required for the threat actor to find and exploit vulnerability?	3 (Expensive resources required)
		2 (Some resources required)
		1 (No resources required)
Opportunity	Opportunities required for the threat actor to find and exploit vulnerability?	3 (Full access required)
		2 (Some access required)
		1 (No access required)
Size	How large is the group of the threat actor?	3 (Anonymous internet users)
		2 (Authenticated users)
		1 (Systems administrators)

Table 1: Threat Actors Profile

4.3 Asset

Assets can be data, people, services, facilities that threat actor aims to attack, causing a significant impact on the CI [Moteff and Parfomak 04]. It is necessary to outline assets in terms of their boundary, criticality, components and importance for understanding the impact of the assets. Each asset aims to achieve a security goal which is used in determining the impact that may result from unauthorised access. Criticality is measured as the consequences associated with the degradation or loss of an asset. It is the major indicator used by organisations to determine which asset is of more value to the organisation. Table 2 shows assets impact factors with relative weights).

Asset Impact factors	Description	Impact rating
		Weight / Value
Loss of confidentiality	How much data could be disclosed and how sensitive is it?	1 (Minimal non-sensitive data disclosed)
		2 (Minimal critical data disclosed)
		3 (Extensive critical data disclosed)
Loss of availability	How many services could be lost, and how vital is it?	1 (Minimal secondary services interrupted)
		2 (Minimal primary services interrupted)
		3 (Extensive primary services interrupted)
Loss of integrity	How much data could be corrupted and how damaged is it?	1 (Minimal slightly corrupt data)
		2 (Minimal seriously corrupt data)
		3 (Extensive seriously corrupt data)
Loss of accountability	Are the threat actors traceable to an individual?	1 (Fully traceable)
		2 (Possibly traceable)
		3 (Completely anonymous)
Loss of conformance	How much deviation from specified behaviour constitutes non-conformance?	1 (Minor variation)
		2 (Clear variation)
		3 (High profile variation)

Table 2: Asset Profile

4.4 TTP

TTP is used by a threat actor to plan and manage an attack by following specific technique and procedure. They involve the pattern of activities or methods associated with a specific threat actor and consist of the threat actor's specific behaviour (attack pattern) and specific software tools that can be used by threat actors to perform an attack [Barnum12]. Therefore, TTP from the STIX model is used to categorise attacks into the eleven tactics and the different techniques under each tactic provided by MITRE (Strom et al., 2017).

4.5 Vulnerabilities

To estimate the likelihood of an attack, it is necessary to estimate the likelihood of a vulnerability discovered and exploited. We adopt the OWASP factors for characterising weaknesses, which allow stakeholders to make informed decisions when mitigating risks caused by the weaknesses. To apply the OWASP methodology, a rating table is presented in Table 3 with corresponding values assigned to the different factors that can help organisations to determine the likelihood of vulnerability.

Vulnerability factors	Description	Likelihood Rating Weight/Value
Ease of discovery	How easy is it for vulnerability to be discovered?	1 (Practically impossible)
		2 (Difficult)
		3 (Easy)
Ease of exploit	How easy is it for vulnerability to be exploited?	1 (Theoretical)
		2 (Difficult)
		3 (Easy)
Awareness	How well known is this vulnerability to the threat actors?	1 (Unknown)
		2 (Hidden)
		3 (Obvious)
Intrusion detection	How likely is an exploit to be detected?	1(Active detection in application)
		2 (Logged and reviewed)
		3 (Not logged)

Table 3: Vulnerability Rating

4.6 Threats

Threat profile allows the identification and understanding of threat characteristics [Gandhi et al 11].Each threat needs to categorised according to the goals and purpose of the attacks and the assets targeted by those threats. By classifying these threats, the stakeholders check the category that a threat falls under and the most common assets affected by a particular threat. With this, a solid foundation of threat information sources is made available.

4.7 Incident

Incident represents information about an attack on the organisation [Byres and Lowe 04]. Some specific components determine the type of incidents such as threat types, threat actor's skill, capability and location, assets affected, events, parties involved, and time. With a specific attack pattern, the organisation tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the future.

4.8 Indicator

Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity [Cherdantseva et al 16]. They are a detective in nature and are for specifying conditions that may exist to indicate the presence of a threat along with relevant contextual information. Organisations should be aware of the data associated with cyber-attacks, which are known as indicators of compromise (IOC). IOC is commonly partitioned into three distinct categories (Tounsi and Rais, 2018).

- Network indicators are found in URL's, and domain names used for command and control and link-based malware delivery. They could be IP addresses used in detecting attacks from botnets, known compromised servers and systems conducting DDoS attack.

- Host-based indicators are found by analysing infected computers. They include malware names and decoy documents, or file hashes of the malware being investigated. Dynamic link libraries (DLLs) are often targeted, and registry keys could be added by malicious code to allow for persistence.
- Email indicators are created when threat actors use free email services to send social engineering emails to target organisations. The email source address and subject are created from addresses that appear to be recognisable individuals or create intriguing subject lines. Attachments and links are also used for deceiving individuals.

4.9 Risks

Risks are potential consequence due to the cyber-attack can lead to financial loss, reputational damage, privacy violation and non-compliance consequences, leaving users distrustful of services. To understand a cyber-attack, we have to study the nature of the attack and the motivation behind the attack [Gandhi et al. 11). Therefore, for risk severity to be estimated, it is essential for information about the threat actor, vulnerability factors and the impact of a successful exploit affecting security goals of the assets to be gathered. The following steps are involved in identifying the risk severity.

Step 1: To estimate the overall likelihood of the risk, threat actor and vulnerability factors are put into consideration, as shown in equation 1. Each option has a likelihood rating from 3 to 1, as shown in tables 1 and three above. The overall likelihood falls within high, medium and low, which is sufficient for the overall risk score.

$$L = {}^{(TAF + VF)}/_{n} \quad (1)$$

Step 2: Estimate of the overall impact of a successful attack considers the total loss of the goals of the asset, as shown in equation two below. Each factor has a set of option which has an impact rating from 3 to 1, as shown in table 2 above.

$$I = {}^{AF}/_{n} \quad (2)$$

Step 3: Estimate of the likelihood and impact is combined to calculate the overall severity of risk using equation three below. Overall risk severity is rated as *High* (6 to 9): The risk severity requires the implementation of control measures to mitigate the risk immediately. The risk is high when likelihood and impact are high. *Medium* (6 to 3): The risk severity requires the implementation of controls within a specific period. *Low* (0 to 3): The risk level requires the implementation of controls within a specific period.

$$R = L * I \quad (3)$$

Where

R = the risk level; I = the impact of the attack on the organisation's security objectives; L= the likelihood of the attack occurring within a given time-frame; TAF = Threat Actor Factors, VF = Vulnerability Factors; AF = Asset Factors, n = total number of factors

4.10 Controls

These are the corrective, detective and preventive actions to mitigate the risk [Tsegaye and Flowerday 14]. Preventive controls are designed to keep errors or irregularities

from occurring, while detective controls are designed to detect errors and irregularities, which have already occurred and to assure their immediate correction. Corrective controls help to mitigate damage once a risk has materialised. This means that the level of attack determines the type of control to be used and the effectiveness of the existing controls. These three types of controls influence strategic, tactical and operational CTI decisions linking with the business strategy risks, investment priorities and mitigation and detection requirements. The CIS_CSC recommended a list of controls which we adopt for the unified approach. Therefore, an assessment of each control objective is carried out based on subjective judgment. We apply a set of criteria which is used to compare evidence by following the comprehensive assessment model they include; Relevance- The level to which the control addresses the relevant control objectives under analysis, Strength- The strength of the control is determined by a series of factors, Coverage- The level in which all significant risks are addressed, Integration- The degree and manner in which the control reinforces other control processes for the same objective and Traceability- How traceable the control is, which allows it to be verified subsequently in all respects. For each criterion, a rating score from 1 to 5 is given to measure which control addresses the specific control objective. Table 4 shows the five different criteria rating and table 5 shows the overall effectiveness of the controls.

Rating		**Description**
1	Adequate control	The control achieves the objectives intended to mitigate the risks.
2	Adequate control with some areas of improvement	The control achieves the objectives intended to mitigate the risks with evidence of some areas, though not critical, subject to improvement to meet the requisites of sound controls.
3	Generally adequate control, with some critical areas	The control mostly mitigates the risks intended to mitigate the risks. However, the characteristics of some of the controls are not entirely consistent with basic sound controls
4	Inadequate control, subject to significant improvement	The control partially achieves the control objectives intended to mitigate the risks
5	Insufficient control	The control is not enough to achieve the control objectives intended to mitigate the risks.

Table 4: Control Rating

The overall effectiveness of each control is determined by equation 4 using five parameters with five scales range. This helps to determine how effective individual control is and any recommendation for further improvement.

$$OE = R + S + C + I + T \quad (4)$$

Where

OE = Overall Effectiveness, R = Relevance, S = Strength ,C= Coverage, I = *Integration and T = Traceability*

Description	Overall Effectiveness	Effective?
Insignificant	0-5	Yes
Minor	6-10	Yes
Moderate	11-15	No
Major	16-20	No
Critical	21-25	No

Table 5: Overall Effectiveness

The Metamodel illustrated in Figure 3 shows the relationship among the concepts. An actor represents an entity, an organisation or human user having strategic, operational and tactical plans within its organisational setting. The actor has full control over its assets and needs to keep the assets secure for the overall business continuity. Vulnerability is the weakness or mistake within the security program, software, systems, networks or configurations that are targeted and exploited by a threat actor to gain unauthorised access to an asset (system or network) using TTP. These vulnerabilities, when not addressed on time, can lead to a threat which materializes the risk. Risk is the failure of an organisation or individual to achieve its goals due to the malicious attempt to disrupt its critical services by a threat. Organisations cannot fully avoid risk; however, it is the role of the actors to ensure that risks are kept to a minimum level. Security controls are introduced to help mitigate the risks. The threat actor is a type of actor with malicious intent which is characterised by their identity, suspected motivation, goals, skills, resources available for them to carry out a successful attack. This actor uses various types of TTP to generate a cyber-such as impersonate actors by deceiving users of the CI into believing them and then getting hold of some sensitive information or by directly compromising their critical assets and leading to a significant risk to the organisation. This is done when vulnerabilities in an asset of the organisation are exploited using some TTP. TTP is used by a threat actor to plan and manage an attack through following specific techniques and procedures. They involve the pattern of activities or methods associated with a specific threat actor and consist of the threat actor's specific behaviour (attack pattern) and specific software tools that can be used by threat actors to perform an attack leaving behind the incident of the attack. The incident is the type of event that represents information about an attack on the organisation. Some specific components determine the type of incident such as; threat types, threat actor's skill, capability and location, assets affected, events, parties involved, and time. With a specific attack pattern, the organisation tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the future. With Indicators, a pattern that can be used to detect suspicious or malicious cyber activity is gathered.

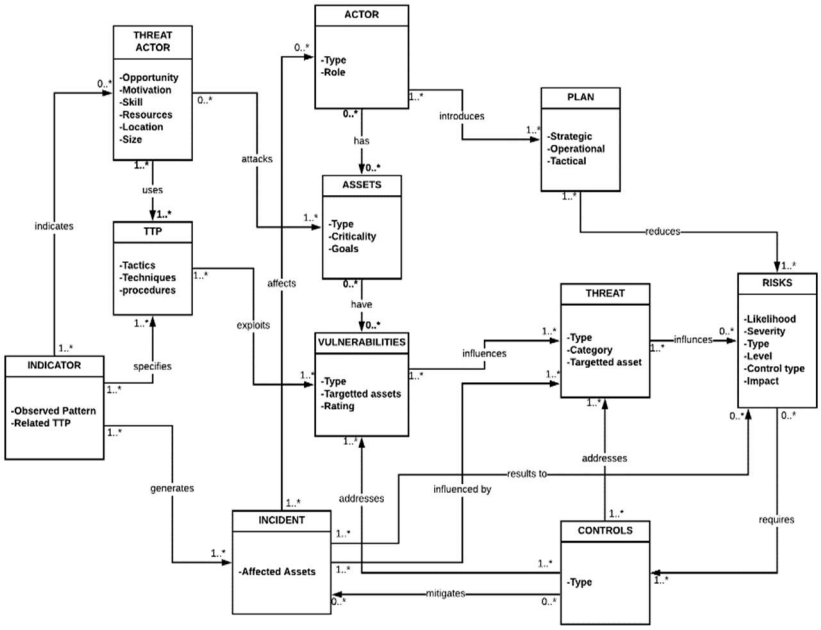

Figure 3: Meta-model Integrating Cyber Threat Intelligence for Cyber Security Risks Management of Critical Infrastructure

5 Case Study

This section presents a case study to demonstrate the applicability of the proposed approach. We employ the approach into a real-world scenario in collaboration with the power holding (DisCos, 2005) company as a CI in Nigeria to determine the usefulness of the approach. The goal of the study is to:

- Understand the threats and risks associated with the studied organisation
- Applicability of integrating CTI for CSRM practice

5.1 Study Context

DisCos power holding company and one of the largest CIs in Nigeria which distributes electricity across the country which serves at least 30,000 customers within a geographical area, with several branches and employees located in different states of Nigeria. The company is structured based on functional divisions, which include administration, support and IT. The first services of the company are to provide last-mile services in the electricity supply value chain, transforming or stepping down electricity from the high voltage at the transmission level to lower voltage depending on the category of the customer. They are responsible for the marketing and sale of electricity to customers, providing a tax to the government, collecting bills, handling electronic payments, and the exchange of information and provision of customer care functions in its geographical area. In improving the continuity of service, timely

recognition of faults, continuous monitoring and protection of the power systems, the company recently implemented a supervisory control system in all its branches for sustainable service delivery.

5.2 Data Collection and Analysis Method

The data collection and analysis followed a sequential explanatory strategy initiated with kick-off session followed by reviewing documents, recent attack and organizing interactive sessions [Creswell, 02]. Note that, we have also followed action research for the study so that the result from the study can be directly contribute for the improvement of CSRM practice and overall cyber security in DisCos. The data was collected from various sources including existing DisCos security documents, recent cyber-attack, risk register, assets inventory, internal audit report and overall organisational policies and procedures. Furthermore, one kick-off and two brainstorming sessions were also conducted with the DisCos IT security team and first author of the paper as the study team to understand their views and presented them the proposed approach. In particular, we have introduced the concepts relating to the CSRM and CTI and provided an overview of the CTI integration for the improvement of CSRM specifically for the CI. The sessions were effective to understand the recent cyber attack in DisCos and to review the existing security documents and CSRM practices in detailed. Finally, we have also conducted an open discussion regarding the applicability of the proposed approach after the end of the study. The collected data was analysed mainly qualitatively and quantitatively using different variables such as weight of vulnerability, asset criticality, TTP, risk level, and control effectiveness. Therefore, the unit of analysis considered actor and threat profile, assets detailed, existing controls, vulnerability, and risk value. After observing the DisCos context, we have identified actor, assets, vulnerabilities, and threats to determine asset weight, vulnerability and risk level, and finally control of effectiveness.

5.3 Recent Cyber Attack

In a recent event, a carefully crafted spear phishing e-mail message which contained a malicious Microsoft file attachment that spread across the network, operating systems, and targeting the SCADA system, of an anonymized company called DisCos. As a result of downloading the file, the organisation gathered hashed credentials over a server message block (SMB) to identify information. The organisation, accessed workstations and servers on the corporate network that contained data output from control systems, accessed files about the SCADA systems, leaked network credentials, organisational design and control system information to a command and control server outside DisCos organisation, and accessed email accounts using outlook web access (OWA). The organisation used a virtual private network (VPN) to maintain access to networks even with the presence of network proxies, gateways and firewalls. A backdoor was installed on the machine, providing the organisation with remote access to the environment (networks, systems, databases). The organisation having available resources, disabled the host-based firewalls, obtained a foothold and the exploration activity primarily centred on identifying the central host computer server with the highest volume of personally identifiable information (PII), then used a batch script to gather folder and file names from hosts. access to the database host computer server is

gained by by leveraging the organisation's active directory information to identify database administrators and their computers. Passwords were cracked using password-cracking techniques, and that allowed the anonymous organisation to gain full access to those systems. This caused a loss of data and operational disruption as a result of network and computer security failure. This incident is reported to have resulted in an electrical power blackout that remained for up to 2 weeks days affecting around 30,000 customers. As a result, DisCos has decided to use CSRM to assess future impact and control measures for similar incidents in the other branches. A brief description of a scenario allows us to exemplify how the DisCos could benefit from our proposed approach.

5.4 Implementation of the Framing Concepts of the Proposed Approach

In this section, all the framing concepts of the proposed approach are presented and implemented in the case study to provide a clear assessment for demonstrating the ability of the approach to produce the desired effect. Hence, the implementation process was performed through a series of concepts as presented below:

Actor: We have been able to identify the key actors and the different roles they play within DisCos. We also considered actors from outside DisCos. DisCos is identified as an organisation that provides critical services, that is the supply of electricity. System Administrators are the employees in charge of monitoring the SCADA system in any of the DisCos branches. The third-party vendor is the Globacom telecommunication company that provides internet services to DisCos. IT Manager is in charge of DisCos technology strategy and implementing the process of the proposed approach. System Analyst is responsible for coordinating the development of systems, asset requirements, and control measures for ensuring the security of all assets is responsible for. Responsibilities also include identifying cyber threats and establishing plans, risk analysis and controls to protect assets.

Threat Actor: The threat actor is identified as the anonymous organisation. Table 6below estimates the likelihood of a successful attack by the anonymous organisation.

Threat Actor factors	Value	Weight	Total
Skill level	Advanced computer user	3	14
Location	Local network	2	
Resources	Some resources required	2	
Motive	Possible reward	2	
Opportunity	Some access required	2	
Size	Anonymous internet users	3	

Table 6: Threat Actors Profile Level based on the Attack Scenario

The total threat actor factor score is 14, as shown in Table 8 above. We considered the threat actor factors to calculate the overall likelihood of risk.

Assets: To consider the impact of the attack, we realised the impact on the application assets, the data it uses and the functions it provides in achieving the organisation's goals. The total score is to be used to estimate the magnitude of the

impact on the organisation, because of vulnerability being exploited. The total Asset factors score is 13 as shown in Table 7 below:

Asset factors	Asset Name	Description	Value	Weight	Total
Loss of confidentiality	Databases Customer data Company data	Loss of sensitive data due to the anonymous organisation accessing workstations and servers on the corporate network that contained sensitive data.	Extensive critical data disclosed	3	13
Loss of availability	Management servers Customer data Company data Application servers Databases	Operational disruption because of network and computer failure.	Extensive primary services interrupted	3	
Loss of integrity	Application server Company data Customer data Databases Management server Virtual Private Network Workstation	Compromise of the network and host server by the anonymous organisation and having access to modify, delete and add data in the database	Extensive seriously corrupt data	3	
Loss of accountability	HMI Computers Host computer systems	The anonymous organisation left no trace	Completely anonymous	3	
Non-conformance	Employee training	DisCos services did not meet some specified regulatory requirements as vulnerabilities were exploited and caused unwanted behaviour.	Clear variation	1	

Table 7: Asset Impact base Score

Tactic	Techniques	Procedure
Discovery	Account Discovery	The anonymous organisation used batch scripts to enumerate administrators in the environment.
	System Network Configuration Discovery	
	File and Directory Discovery	The batch script was used to gather folder and file names from hosts.
Persistence	External Remote Services	VPN was used to maintain access to the environment.
Credential Access	Brute Force	The anonymous organisation dropped and executed tools used for password cracking.
	Credential Dumping	The anonymous organisation obtained legitimate credentials, including passwords.
Execution	User Execution	Used Spear phishing to get the employee of the DisCos to open the attachment.
Collection	Data from Local System	The anonymous organisation collected data from the local system.
	Email Collection	Used outlook web access to access email accounts.
Defence Evasion	Disabling Security Tools	The anonymous organisation disabled host-based firewalls.
Initial Access	Spear phishing Attachment	Used Spear phishing with Microsoft office attachments to target DisCos.

Table 8: TTP used on DisCos by the Anonymous Organisation

TTP: We used TTP to categorise the behaviour that the anonymous organisation exhibited in attacking DisCos, as shown in table 8.

Incidents: In this case, the parties involved are the anonymous organisation and DisCos. Assets affected include network, servers, communication lines, SCADA system and sensitive data. The threat actor is an anonymous organisation. The nature of the compromise is a severe operational disruption.

Indicator: They are the specific observable patterns mapped to a related TTP. In this case, the indicators are shown as; Network Indicator (URL, IP address and DisCos domain name), Host-based Indicator (Malicious batch scripts, File Hashes) and Email Indicator (Email Attachments, Phishing email)

6 Results

The result section shows the vulnerability, threat, risk and controls analysis as part of the implementation process. In this section, we provide a detailed description of how these concepts are applied to the case study.

Vulnerabilities: We observed several vulnerabilities by looking at the attack context. Therefore, we estimate the likelihood of the vulnerabilities being discovered and exploited by using the vulnerability factors following the OWASP methodology, as shown in table 9 below.

Vulnerability factors	Value	Weight	Total
Ease of discovery	Easy	3	12
Ease of exploit	Easy	3	
Awareness	Obvious	3	
Intrusion detection	Logged and reviewed	3	

Table 9: Vulnerability Rating

The total vulnerability factor score is 12, as shown in Table 10 above. We considered the vulnerability factors to calculate the overall likelihood of risk.

Threats: To create a threat profile, we identified some threats that potentially affected the assets of the DisCos and compromised sensitive information. The threats and the various assets targeted are presented in table 10 below.

Threat Name	Description	Target Assets
Data breach	Incidents involving unauthorised access, damage, alteration and disclosure of confidential data of DisCos	Company data and customer data
Weak password, credential, identity and access management	Administrator accounts did not have complex passwords across systems on the network.	Application server and databases
Loss of data or documents	Loss of sensitive data as the anonymous organisation accessed workstations and servers on the corporate network that contained the sensitive data	All data
Error in use	Lack of proper security configuration for critical servers such as mail servers, application servers, through unused ports and services, access controls and firewalls to limit access to systems.	Application servers
Loss of power supply	A malicious attack that focuses on shutting down critical services making it inaccessible to legitimate users.	All assets
Lack of employee security awareness	There is a lack of employee training to identify social engineering techniques and Spear phishing emails/links and how to raise suspicion for potentially malicious events.	All assets

Table 10: Threat Profile

Risks: After identifying the various vulnerabilities, security goals and threats, we assessed the risks. It appears that the overall severity of risk is 6.76 (high). Therefore, understanding and evaluating vulnerabilities, asset impact and threat actor factors is critical in making effective decisions for the risk control.

$$L = (14 + 12) \div 10 = 2.6 \qquad (1)$$

$$I = 13 \div 5 = 2.6 \quad (2)$$

$$\boldsymbol{R = 2.6 * 2.6 = 6.76} \quad (\mathbf{3})$$

Controls: We first identified existing controls and calculated the effectiveness of the controls. In case of ineffective existing controls, we have recommended additional controls that need to be implemented, as shown in Table 11 below to address the identified risks. Among the identified controls, two factor authentications, NIDS and DisCos's employees' security training ranked the highest overall effectiveness. Such controls are widely recognized for improving overall security. Furthermore, strict access control policy and file level permission are also necessary for DisCos.

Control Type	**Control Description**	**Criteria**					**Overall Effectiveness**
		S	**R**	**C**	**I**	**T**	
Preventive	Account lockout policies after a certain number of a failed login attempt to prevent passwords from being guessed.	4	4	3	4	3	18
	Proper process, registry and file permission should be in place.	4	4	4	3	2	17
Detective	Identify unnecessary system utilities or potentially malicious software.	3	4	4	3	2	16
	Network intrusion prevention systems should be put in place.	5	4	3	4	3	19
Corrective	Limit access to remote services through centrally managed VPNs.	4	4	5	2	1	16
	Use strong two-factor or multi-factor authentication.	5	5	3	4	3	20
	Ensure that administrator accounts have complex, unique passwords.	4	3	2	2	2	13
	Use of two-factor authentication for public-facing webmail servers is recommended.	5	5	3	2	3	18
	Training required for the DisCos employees to raise awareness.	3	4	5	3	4	19
	Anti-virus to automatically isolate suspicious files	2	3	4	2	4	15

Table 11: Control Effectiveness

7 Discussion

The integration of CTI with the CSRM helps the studied smart grid CI to detailed analyse of the threats and to determine the appropriate risk level for the overall cyber security improvement. The novel contribution of this work is to provide new insights into the effect of cybersecurity by incorporating CTI concepts to improve risk management practice for the CI and to discover the existence of unknown threats, fully understanding and mitigating those threats and risks in a proactive manner.

7.1 Applicability of CTI for Improving CSRM

We have applied a real CI case study to demonstrate the applicability of our work. The unified aproach provides a detailed analysis of threat and threat actors profile, existing risk management practice and effectiveness of controls. A brief description of the scenario allows us to exemplify the integration of CTI to improve CSRM in a CI. By applying the concepts, it supports the organisation to have information such as the TTP, incidents, indicators and the threat actors profile to be able to perform an adequate risk assessment. Having CTI information about threats helps to manage risks effectively, provides mechanisms to prioritise efforts and focus on the most significant risks first. If information about what vulnerabilities are being exploited is known, it can be actively exploited to help decide which security patches should be applied first. The threat information can then be leveraged to help draw a clearer understanding of the risks that the threat environment poses to the organisation.

Furthermore, CTI helped by giving them early warning of potential threats so that the organisation can consider specific operational and tactical decision to address the threats and associated risks. Also, by setting up a CTI as part of the risk management process, it is assured that all indicators of compromise are shared, driving towards a better and more informed response to security incidents. It also enables better security investment strategy. In particular, operational, tactical and strategic plans enable to make both long-term and short-term information security planning by focusing on intelligence collection and analysis to understand threat actor's cyber capabilities, plans and intentions as well as relevant countermeasures. Evaluating the effectiveness of the proposed controls is very difficult without a good understanding of the motives, means and methods of the threats being addressed. Lastly, our work allows actors to examine the existence of an attack pattern carefully and to understand threats in a cyber environment. The case study results reveal that having CTI as part of a risk management, supports organisations to know detailed about threats so that risk related to the threats can be determined and controlled in a proactive manner.

7.2 The Result from the Case Study

The risk level generated as a result of the cyber-attack is 6.76, which was calculated using the threat information and the asset security goal. The risk needs immediate attention and controls are identified for risk mitigation. Some of the controls are already existed and categorized as either ineffective or not enough by the unified approach. We advocate DisCos to adopt CTI for improving CSRM to detect and respond to threats accordingly. With the adoption of CTI, organisation can defend

against current and future threats, which involves understanding the threat actor's attack pattern, location, skills, motivation and intent to make intelligent defensive decisions.

7.3 Comparison with the other Works

We have several observations based on the comparisons of this work with existing works. The maturity model to capture the spectrum of threat data and best practices associated threat intelligence is proposed by (Boyson,2014) without focusing on CSRM. A highlight of the importance and role of strategic cyber intelligence to support risk-informed decision making is proposed by (Borum et al, 2015) but the approach only focuses on the strategic level. Various security threats and incidents that occurred on the different CI domains is presented. Security measures, include vulnerability assessment and pentration approaches for CI is introduced. However, having CTI can further effectively help in risk to be assessed, mitigated and controlled (Abouzakhar, 2013). An insightful review of possible solution paths of understanding the ICS security trends about cyber threats is offered but, the work did not implement the use of CTI to assess vulnerabilities, threats and mitigate risks (Ani et al., 2017). The behavioural patterns of fast-flux botnets for threat intelligence is examined. The Threat Intelligence infrastructure, which was developed explicitly for fast-flux botnet detection and monitoring, enables this analysis but did not explain how risk can be managed and controlled (Caglayan et al., 2012). Survey is carried out by (Yadav and Mahajan, 2015) on risk assessment methods, the significant challenges and controls for various aspects of the smart grid such as SCADA systems and communication networks, to address the challenges facing smart grid technologies. However, smart grids, as a provider, require a comprehensive cybersecurity solution by supporting stakeholders to assess cyber threats through integrating CTI and provide guidelines for effective risk management.

In a dynamic environment like CI, it is essential for risk management to have information about threats to be able to assess threats as it continuously changes. Most of the cyber risk is as a result of challenges in identifying critical threats, assets affected, parties involved, attributed threat actor, nature of compromise, and historically observed TTP used by the threat actor. Based on the case study, other factors influence a successful attack, such as weak passwords, weak firewalls, and operator unawareness. Managing these risks requires the involvement of CTI. We concluded that threats caused as a result of a cyber-attack could be mitigated or controlled using the threat information with existing risk management and by creating more proactive and adaptive mitigation solutions.

8 Conclusion

The threat landscape is evolving at a rapid rate with new techniques and more sophisticated attacks. The security strategies for mitigating and eliminating these threats always need improvement for CI. CTI provides comprehensive information about security threats, and this effectively supports the CSRM activities. Organisations need to integrate CTI with risk management to allow faster detection and detailed analysis of attacks on their assets. This work contributes for an effective risk management practice and the novelty focuses on the extensive integration of CTI

information for the CSRM activities to determine appropriate controls from strategic, tactical and operational perspectives for the overall cyber security improvement. Therefore, our work contributes beyond the existing literature by providing a unified approach that uses CTI to improve CSRM. To demonstrate the applicability of the work, we applied the proposed approach to a power grid system as a CI. The result shows that the approach sufficiently supports the organisation to analyse their cyber security including asset criticality, detailed analysis of threat and related vulnerabilities to idetermine risk levels so that apprioriate controls can not only be identifed but also evaluate the effectiveness of the existing controls for the risk mitigation. We advocate for the creation of CSRM awareness within the organisational levels; staff must not ignore their IT responsibilities. Our future work is to apply the proposed approach to other case studies to generalise our findings and validate the applicability of the approach. Furthermore, it is also necessary to create a process for systematically integrating advanced cybersecurity technologies and practice for managing the risk and its evolutions.

Acknowledgements

This work has received funding from the Nigerian Petroleum Development Trust Fund (PTDF).

References

[Abouzakhar, 13] Abouzakhar, N. (2013) 'Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations'. European Conference on Information Warfare and Security: Academic Conferences International Limited, 1.

[Abu, 18] Abu, M. S., Selamat, S. R., Ariffin, A. and Yusof, R. (2018) 'Cyber Threat Intelligence–Issue and Challenges', Indonesian Journal of Electrical Engineering and Computer Science, 10(1), pp. 371-379.

[Abomhara, 15] Abomhara, M., 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), pp.65-88.

[Ani, 17] Ani, U. P. D., He, H. and Tiwari, A. (2017) 'Review of cybersecurity issues in critical industrial infrastructure: manufacturing in perspective', Journal of Cyber Security Technology, 1(1), pp. 32-74.

[Baldoni, 14] Baldoni, R. (2014) Critical infrastructure protection: threats, attacks, and counter-measures: Technical report.

[Barnum, 12] Barnum, S. (2012) 'Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)', MITRE Corporation, 11, pp. 1-22.

[Borum, 15] Borum, R., Felker, J., Kern, S., Dennesen, K. and Feyes, T. (2015) 'Strategic cyber intelligence', Information & Computer Security, 23(3), pp. 317-332.

[Boyson, 14] Boyson, S. (2014) 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems', Technovation, 34(7), pp. 342-353.

[Brewer, 16] Brewer, R. (2016) 'Ransomware attacks: detection, prevention and cure', Network Security, 2016(9), pp. 5-9.

[Bromiley, 16] Bromiley, M. (2016) 'Threat intelligence: What it is, and how to use it effectively', SANS Inst.

[Burger, 14] Burger, E. W., Goodman, M. D., Kampanakis, P. and Zhu, K. A. 'Taxonomy model for cyber threat intelligence information exchange technologies'. Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security: ACM, 51-60.

[Byres et al 04] Byres, E. and Lowe, J., 2004, October. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218).

[Caglayan, 12] Caglayan, A., Toothaker, M., Drapeau, D., Burke, D. and Eaton, G. (2012) 'Behavioral analysis of botnets for threat intelligence', Information systems and e-business management, 10(4), pp. 491-519.

[Centre for Internet Security, 18] Centre for Internet Security (2018) The Critical Security Controls for Effective Cyber Defense. (Accessed: 18/05/2018 2018).

[Cherdantseva et al. 16] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, pp.1-27.

[Creswell, 02] J.W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Sage Publications, 2002.

[Chismon, 15] Chismon, D. and Ruks, M. (2015) 'Threat intelligence: Collecting, analysing, evaluating', MWR InfoSecurity Ltd.

[Dehghantanha, 18] Dehghantanha, A., Conti, M. and Dargahi, T. (2018) Cyber threat intelligence. Springer.

[DisCos, 05] DisCos, N. E. R. C. (2005) Kano Electricity Distribution Plc (KEDC). Available at: http://www.kedco.ng/index.php.

[Dietz and Hoogervorst, 08] Dietz, J.L. and Hoogervorst, J.A., 2008, March. Enterprise ontology in enterprise engineering. In *Proceedings of the 2008 ACM symposium on Applied computing* (pp. 572-579). ACM.

[Gandhi, 11] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011) 'Dimensions of cyber-attacks: Cultural, social, economic, and political', IEEE Technology and Society Magazine, 30(1), pp. 28-38.

[Hahn, 13] Hahn, A., Ashok, A., Sridhar, S. and Govindarasu, M. (2013) 'Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid', IEEE Transactions on Smart Grid, 4(2), pp. 847-855.

[ISO, 11] ISO, I. and Std, I. (2011) 'ISO 27005: 2011', Information technology–Security techniques–Information security risk management. ISO.

[Kao, 18] Kao, D.-Y. and Hsiao, S.-C. 'The dynamic analysis of WannaCry ransomware'. 2018 20th International Conference on Advanced Communication Technology (ICACT): IEEE, 159-166.

[Kim, 13] Kim, K.-D. and Kumar, P. (2013) 'An overview and some challenges in cyber-physical systems', Journal of the Indian Institute of Science, 93(3), pp. 341-352.

[Krebs, 16] Krebs, B. (2016) 'KrebsOnSecurity hit with record DDoS', KrebsOnSecurity, Sept, 21.

[Kure, 18] Kure, H., Islam, S. and Razzaque, M. (2018) 'An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System', Applied Sciences, 8(6), pp. 898.

[Lee, 15] Lee, J., Bagheri, B. and Kao, H.-A. (2015) 'A cyber-physical systems architecture for industry 4.0-based manufacturing systems', Manufacturing letters, 3, pp. 18-23.

[Liang, 17] Liang, G., Weller, S. R., Zhao, J., Luo, F. and Dong, Z. Y. (2017) 'The 2015 ukraine blackout: Implications for false data injection attacks', IEEE Transactions on Power Systems, 32(4), pp. 3317-3318.

[Martin, 07] Martin, R. A. (2007) 'Common weakness enumeration', Mitre Corporation.

[Mills, 17] Mills, J. L. and Harclerode, K. (2017) 'Privacy, Mass Intrusion, and the Modern Data Breach', Fla. L. Rev., 69, pp. 771.

[Mohurle, 17] Mohurle, S. and Patil, M. (2017) 'A brief study of wannacry threat: Ransomware attack 2017', International Journal of Advanced Research in Computer Science, 8(5).

[Moteff and Parfomak 04] Moteff, J. and Parfomak, P., 2004, October. Critical infrastructure and key assets: definition and identification. Library Of Congress Washington Dc Congressional Research Service.

[Open Web Application Security Project, 14] Open Web Application Security Project (2014) OWASP Risk Rating Methodology. Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (Accessed: 05/02/2018)

[Planqué, 18] Planqué, D. (2018) 'Cyber Threat Intelligence'.

[Poller, 18] Poller, J. L. and Oltsik, J. (2018) 'Automation and Analytics versus the Chaos of Cybersecurity Operations'.

[Reveron, 12] Reveron, D. S. (2012) Cyberspace and national security: threats, opportunities, and power in a virtual world. Georgetown University Press.

[Ray, 10] Ray, P. D., Harnoor, R. and Hentea, M. 'Smart power grid security: A unified risk management approach'. Security Technology (ICCST), 2010 IEEE International Carnahan Conference on: IEEE, 276-285.

[Stoneburner, 02] Stoneburner, G., Goguen, A. Y. and Feringa, A. (2002) 'Sp 800-30. risk management guide for information technology systems'.

[Strom, 17] Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., Whitley, S. M. and Wolf, R. D. (2017) Finding Cyber Threats with ATT&CK™-Based Analytics: MITRE Technical Report MTR170202. The MITRE Corporation, 2017.

[Tounsi, 18] Tounsi, W. and Rais, H. (2018) 'A survey on technical threat intelligence in the age of sophisticated cyber attacks', Computers & security, 72, pp. 212-233.

[Tsegaye and Flowerday 14] Tsegaye, T. and Flowerday, S., 2014, December. Controls for protecting critical information infrastructure from cyberattacks. In *World Congress on Internet Security (WorldCIS-2014)* (pp. 24-29). IEEE.

[Wu, 15] Wu, W., Kang, R. and Li, Z. 'Risk assessment method for cyber security of cyber physical systems'. Reliability Systems Engineering (ICRSE), 2015 First International Conference on: IEEE, 1-5.

[Yadav, 15] Yadav, D. and Mahajan, A. R. (2015) 'Smart Grid Cyber Security and Risk Assessment: An Overview', International Journal of Science, Engineering and Technology Research (IJSETR), 4, pp. 3078-308