



INTERNAL NEWLINE EFFICIENCY AND EXTERNAL EFFECTIVENESS OF CYBER SECURITY ANALYSIS BY USING NEWLINE CONSTRUCTIVIST GROUNDED THEORY

Nandini Gargula, Computer Network and Systems Engineer

INFORMATION TECHNOLOGY, Charles Stuart University

Sydney Australia

ABSTRACT

New technologies such as SMAC and IOTs have ushered in a new era in the information technology sector. Cyber security threats to digital infrastructure have grown exponentially as a result of this development and are a cause for concern in terms of the sustainability of the current business growth situation. Continuous improvement in the cyber security posture of organisations is needed to keep pace with the rising threats. Using capability maturity models is a good way to get there. There has been a sea change in the world of information technology due to disruptive technologies like social, mobility, analytics, and the cloud (SMAC) and the internet of things (IOT). The cyber security dangers to digital infrastructure have grown exponentially as a result of this evolution and are a major worry for the long-term viability of corporate growth. Continuous improvement in the cyber security posture of organisations is needed to keep pace with the escalating threats. Models of capability maturity assist in achieving this goal. Using a comparison of nine contemporary maturity models and an empirical study of inputs from 200 or more relevant cross-industry specialists, this research offers the development and validation of a new cyber security capability maturity model (CSCMM). CSCMM is expected to help organisations combat the new generation of cyber threats by strengthening their cyber security posture.

1. INTRODUCTION

Industry v4.0 is expected to rely heavily on CPS (Cyber Physical Systems), which have been classified as critical components of the Industrial Internet of Things. It's possible to run smart apps and services that are accurate and real-time thanks to CPS. They are built on the real-time transmission of data and sensitive information between cyber and physical systems [1]. [2] Both researchers and manufacturers are involved in the development of CPS. The German gross

value will increase by 267 billion Euros by 2025 as a result of the implementation of CPS into Industry v4.0 because of its great economic potential [3].

embedded systems that interact with physical input and output make up a CPS. With the ability to monitor and control real IoT-related objects and processes, CPS is a collection of numerous networked systems. Scanners, aggregators, and actuators make up the core components of a CPS. Furthermore, CPS

systems are able to adapt and manage the physical world by sensing and adapting to their surroundings [5]. This is mostly due to their adaptability and capacity to alter the runtime of system processes via real-time computing [6]. Figure 1 illustrates the wide range of applications of CPS systems, which include power transmission and communication

networks; agricultural and ecological systems; military systems; robotics; and autonomous systems like drones and autonomous cars. As a result of this, in addition to medical care domains, medical services can be improved. It can also be utilised to facilitate an eco-friendly, transient, cost efficient and safe production process in supply chains.




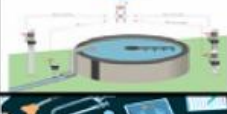



Naming	Classification	Description
 Smart House	Industrial-Consumer IoT	<ul style="list-style-type: none"> Control Smart Devices Homeowner Security & Comfort
 Oil Refinery	Industrial-Transportation IoT	<ul style="list-style-type: none"> Naphta, Gasoline, Diesel Asphalt, Petroleum, Fuel, Oil
 Smart Grid	Industrial IoT	<ul style="list-style-type: none"> Smart Efficient Energy Energy Control & Management
 Water Treatment	Industrial-Consumer IoT	<ul style="list-style-type: none"> Improved Water Quality Overcome Contamination & Undesirable Components
 Medical Devices	Medical-Wearable IoT	<ul style="list-style-type: none"> Improved Patients Life Enhanced Medical Treatment Remote Patient Monitoring
 SCADA	Industrial IoT	<ul style="list-style-type: none"> Control & Monitor Telecoms. Control & Monitor Industries
 Smart Cars	Industrial-Transportation IoT	<ul style="list-style-type: none"> Echo Friendly Enhanced Driver Experience Advanced Safety Features
 Supply Chains	Industrial-Transportation IoT	<ul style="list-style-type: none"> Real-Time Delivery Source/Destination Less Delays & Echo Friendly

Fig. 1CPS description & classification.

Existing cyber risk assessment standards should be standardised, as both industry and academia have a significant interest in doing so. Existing standards are being combined in an effort to standardise cyber security frameworks, models, and procedures. Until now, this has never been done. For the sake of advancing efforts to integrate cyber risk standards and governance and to provide a clearer picture of cyber risk assessments, the term "standardisation" is used in this article to describe the accumulation of knowledge. Literature analysis [1], epistemological analysis [2], and a comparative research [3] are all combined here. Fifteen national high-tech (high-tech) plans, seven cyber risk frameworks, and two cyber risk models

were used in the empirical study.. Fifteen high-tech national policies are examined in the comparative study. Cyber risk impact assessment is the subject of an epistemological and empirical investigation. The specific IoT cyber risk vectors must first be identified in order to modify current cyber security requirements. Internet of Things (IoT) attacks that target large data vulnerabilities are referred to as "risk vectors" [4]. A comprehensive model for assessing the impact of cyber risk must incorporate these specific risk vectors [5].

2. LITERATURE REVIEW

Automation and control systems are a given in the modern workplace (IACS). These so-called "cyber-physical systems" are employed in a variety of different fields, including manufacturing, transportation, and public utilities (CPS). Smart devices can be found in homes, offices, and factories, all of which use the Internet of Things (IoT) [1]. IoT is well-known for its components and applications but it's not always clear how these things work together in an industrial setting.

While IoT is a useful concept when discussing digital technology use in industry, current definitions of IoT all assume the same approach to high-level system architecture, which prevents

analysis of alternative system structures, such as the location of data or information processing, along with performance and security issues associated with these structures.

Researchers in this article set out to update existing Industrial IoT definitions as a starting point for investigating how IoT technologies are being used and deployed in industrial environments (IIoT). The purpose of this research was to provide a framework for analysing the nature and uses of IIoT devices, as well as the vulnerabilities and risks they pose. It is our hope that by analysing risks and vulnerabilities across sectors, we would be able to uncover trends that may otherwise go unnoticed.

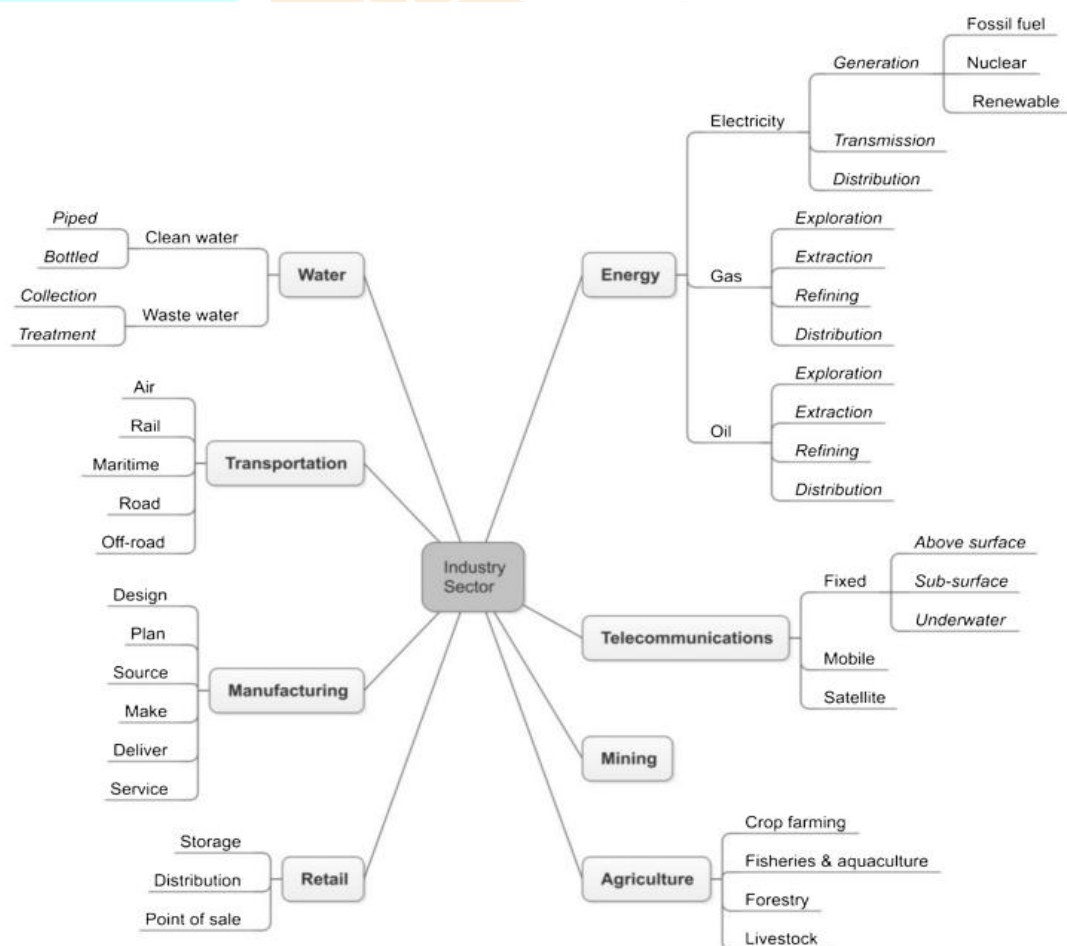


Fig. 2. Industry Sector category

There are a number of industries depicted in Figure 2 that have an impact on an organization's operational systems and the IIoT devices that are utilised in those systems [2]. It's expected that the IIoT will be more widely used in the future,

given the current developments in the business. Only retail is considered to be a non-essential aspect of today's modern economies. Many retail stores have recently gotten more technologically advanced, such as with building automation,

management, or security systems, hence retail has been included to the list.

GE was the first to use the phrase "the industrial internet includes two key components" [3]. A network of sensors and actuators from industrial machines that can generate value on their own. The difference between the consumer and social internets and the industrial internet lies in how and how much value is created. For consumers and social networks, advertising is responsible for the great bulk of the Internet's value [4].

Smart components can be integrated into ordinary objects, and these might be considered IoT devices and parts of cyber-physical systems according to industrial IoT criteria (CPS). The following terms should be considered:

- As defined by the Internet of Things (IoT), linked objects are "sensors and/or actuators carrying out a declared purpose that are capable of interacting with other equipment" [5], with the goal of connecting "connected things" and enabling access to the data that they generate.
- IoT is a term that refers to the increasing usage of computer technology in previously disconnected items, gadgets, sensors and other things. It is possible to connect these "smart objects" to a variety of remote data gathering, analysis, and management systems, requiring little to no human involvement in any of these processes. [6].
- Using the Internet of Things, any object or "thing" has a sensor that may transmit data about its current state to other things and automated systems elsewhere in the environment (IoT). Nodes in the virtual network constantly send massive amounts of data about themselves and their immediate surroundings, making any object a data node. [7].

3. PROPOSED METHOD

A combination of qualitative and quantitative methods was employed to meet the goals of this study. Because the results of qualitative research can't always be measured and quantified, it's best suited for smaller samples. Collis & Hussey (2003, p. 63). Qualitative survey research, on the other hand, is a less prescriptive approach of conducting research. Use this method to acquire

a deeper understanding of the respondent's underlying thoughts and feelings. In quantitative research, there is less reliance on the subjective judgement of the researchers themselves.

3.1 Develop Research Method

Qualitative and quantitative aspects are both present in survey research. Survey researchers, on the other hand, ask respondents to answer questions based only on their own beliefs, feelings, and behaviours. A high sample size is preferred in survey research since it better reflects the population as a whole, and so sampling is given a lot of attention. In survey research, random sampling is a common practise, but this is a first for the method. Even while surveys can be carried out in a variety of ways, such as in person, by telephone or via the mail, or over the Internet, in the current study, an online survey approach using the Internet was used. The goal of conducting a survey is to gather information by interviewing a large number of people on a variety of topics, such as their voting intentions, consumer preferences, social attitudes, and their general health. In our case, we polled the professionals in the area to find out their thoughts on the best way to construct a cyber security maturity model.

3.2 History and Uses of Survey Research

As early as the early 20th century, American and English scholars used "social surveys" in their study. Social problems such as poverty and inequality were the primary focus of these surveys (Converse, 1987). Numerous surveys were carried out in 1930s by US Government to examine and document economic as well as social circumstances in America. A larger and more representative sample is more likely to reflect the total population, which is why sampling procedures have evolved over time to meet this demand. During the same period, a number of scholars conducted significant studies on the preferences of American consumers. Since then, the "survey research approach" has been a popular instrument for predicting election results, and it continues to do so today. There has been a lot of progress in sample selection and questionnaire/scale building, as well as in

administering questionnaires, despite the procedure being essentially the same.

3.3 Data Collection Methods and Tool

We surveyed 201 experts online to gather the data for this study. Only a few responders were personally contacted to explain the questions if they needed any explanations. A questionnaire is utilised to collect data in this study. Because we want to make sure the CSCMM is structurally sound, we created the questionnaires using numeric scales. "Scale used for classifying variables into various classifications with no quantitative value or order" is what the category or nominal variable scale is all about.

3.4 Sample Selection

A strategy known as the "purposive sampling method" was utilised to create the study's sample. Using "non-probability sampling

procedures," participants are chosen based on their familiarity with, relationships with, and expertise in the research topic at hand (Freedman et al., 2007). Participants in this study were chosen because they had adequate and relevant experience working in the subject of Cyber Security to be included in the study.

More than 200 people took part in the poll, representing five distinct job functions and seven distinct industries. Following is a breakdown of responsibilities and sectors. We conducted a survey among a wide range of IT workers, each of whom had a different position and a different responsibility. "Information Security Managers," "Chief Information Security Officers," "Chief Information Officers," "Chief Technology Officers," and "Subject Matter Experts" were among the IT professionals that answered to the poll. Figure 3 below shows the breakdown by category.

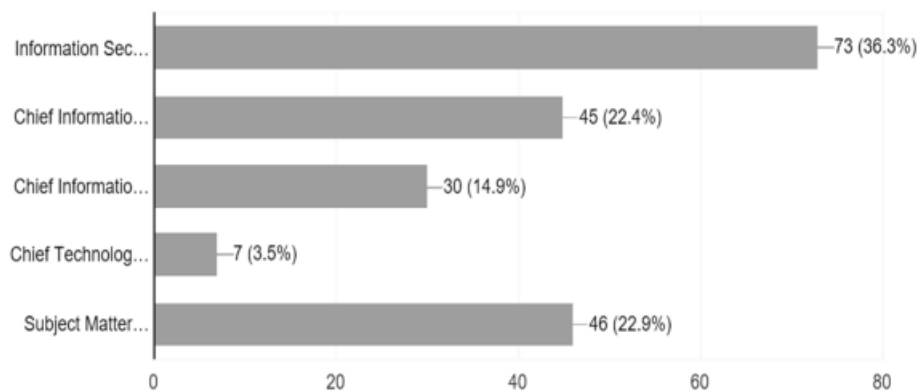


Figure 3: Category wise breakup of the respondents

Business functions are represented by every single one of the above-mentioned

individuals. Figure 4 shows the breakdown by sector.

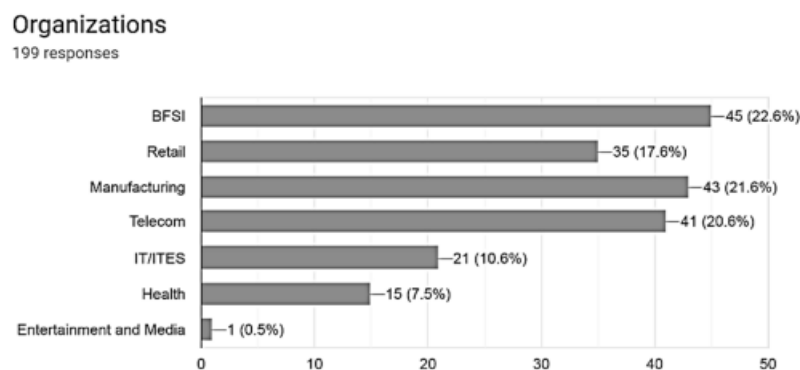


Figure 4: Sector wise breakup of the respondents

CONCLUSION

A methodology for the standardisation of impact assessment methodologies is developed by breaking down cyber risk assessment standards and combining concepts. By using this paradigm, two current issues with estimating IoT device security risk can be addressed. In the first place, the model makes it possible to detect and capture the IoT cyber risk originating from a variety of risk sources. In addition, the model provides new design principles for measuring cyber risk. There was a lot of effort put into this study to figure out the best method for calculating the impact of cyber risk in the Internet of Things. New design for mapping IoT risk vectors and optimising risk impact assessment is documented in the model. The concept outlines a method for incorporating the Internet of Things (IoT) into current cyber security processes and standards. Cyber risk frameworks and procedures have not been standardised till now despite the desire to do so. The epistemic framework is the first attempt to provide a standardisation procedure for assessing the cyber risk impact of IoT vectors, as there is presently no standardisation framework in the literature. Our research in cyber security in the 4th Industrial Revolution era is the topic of this thesis, which is an early and pioneering effort to do so (Industry 4.0). No claims are being made about the finality of some of our findings and interpretations, even if this research exhibits an evolving theme from its inception to the current state of the art and the opportunity for further research and application by using alternative approaches.

REFERENCES

- [1] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc. (2015) 7.
- [2] Beecham Research, M2 M Sector Map, (2014) Available: <http://www.beechamresearch.com/download.aspx?id=18>
- [3] J. Leber, General Electric's San Ramon Software Center Takes Shape MIT Technology Review [online], (2012) Available: <http://www.technologyreview.com/news/507831/general-electric-pitches-an-industrial-internet/> (Accessed September 8 2017).

com/news/507831/general-electric-pitches-an-industrial-internet/ (Accessed September 8 2017).

- [4] D. Floyer, Defining and Sizing the Industrial Internet, Wikibon, June 27, 2013 [online], (2013) Available: http://wikibon.org/wiki/v/Defining_and_Sizing_the_Industrial_Internet.
- [5] B. Dorsemayne, et al., Internet of things: a definition and taxonomy, Proc. – NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol. 2016 (2015) 72–77, <http://dx.doi.org/10.1109/NGMAST.2015.71>.
- [6] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc. (2015) 12.
- [7] P. Satyavolu, et al., Designing for Manufacturing's 'Internet of Things'. Cognizant Report. p.4 [online], (2014) Available: <https://www.cognizant.com/InsightsWhitepapers/Designing-for-Manufacturings-Internet-of-Things.pdf>
8. Haimes YY (2018) Risk modeling of interdependent complex systems of systems: theory and practice. Risk Anal 38(1):84–98
9. Santos JR, Haimes YY, Lian C (2007) A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies. Risk Anal 27(5):1283–1297
10. Malhotra Y (2017) Advancing cyber risk insurance underwriting model risk management beyond VaR to pre-empt and prevent the forthcoming global cyber insurance crisis
11. Radanliev P et al (2018) Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. In: Living in the internet of things: cybersecurity of the IoT, p 41
12. Radanliev P, De Roure D, Cannady S, Montalvo R, Nicolescu R, Huth M (2018) Economic impact of IoT cyber risk—analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In: Living in the internet of things: cybersecurity of the IoT—2018, no. CP740, p 3

13. Nurse J, Creese S, De Roure D (2017) Security risk assessment in internet of things systems. *IT Prof* 19(5):20–26
14. Nurse JRC, Radanliev P, Creese S, De Roure D (2018) Realities of risk: ‘If you can’t understand it, you can’t properly assess it!’: the reality of assessing security risks in Internet of Things systems. In: *Living in the internet of things: cybersecurity of the IoT—2018*, pp 1–9
15. Mitic P (2019) Adaptive risk consensus models: simulations and applications. *SN Appl Sci* 1(12):1743
16. Atzori L, Iera A, Morabito G, Nitti M (2012) The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network

characterization. *ComputNetw* 56(16):3594–3608

17. Ortiz AM, Hussein D, Park S, Han SN, Crespi N (2014) The cluster between internet of things and social networks: review and research challenges. *IEEE Internet Things J* 1(3):206–215
18. Hussein D, Han SN, Lee GM, Crespi N, Bertin E (2017) Towards a dynamic discovery of smart services in the social internet of things. *ComputElectrEng* 58:429–443
19. Peasley S, Waslo R, Lewis T, Hajj R, Carton R (2017) Industry 4.0 and cybersecurity managing risk in an age of connected production
20. IIC (2017) The industrial internet of things volume G5: connectivity framework; industrial internet consortium

