TEST Engineering & Management

Impact of Cyber Risks from Internet of Things

Mr. Amitabh Sharma
Chandigarh Engineering College
Department of Information Technology, Chandigarh Group of Colleges, Chandigarh
cgcpapers@gmail.com

Article Info
Volume 82
Page Number: 2484 - 2487
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *18 January 2020*

Abstract

This paper proposes visualization of IoT cyber risks in designing strategies of supply chain and business. It is seen that cyber risk are presented by Digital IoT technologies in a supply chain which companies. The literature review comprise of government and industry papers and comparison is done between supply chain models and business with studies conducting on new technologies of IoT. The design parameters for support system of decision for looking at the cyber risk in digital economy from supply chain of IoT. A case study on two companies of IoT was done for grounding design process. This study includes methods based on discourse analysis and categorical and open coding.

Keywords: *cyber risk, supply chain, digital economy, internet of things, SME.*

I. INTRODUCTION

A new category of cyber risk is exposed by digital supply chains from shared infrastructure in digital economy. The academic literature fails to discuss the impact of IoT on cyber risk of supply chain[1]. There is a negligence of cyber risk's visibility in the perspective of IoT digital technology in SME's supply chain. The resources and complexities are managed efficiently with IoT digital technology's integration need reference architecture which is standardised. There is a lack of clarification in digital economy on functional, operational and strategic challenges faced from IoT technologies in supply chain.

II. METHODOLOGY

The methodology of research is applied for building system of decision support including case study, literature review and synthesis of data by using the approach of grounded theory. This is done by theme based categorization of emergent concepts by using primary/secondary resources. The "Industry Classification Benchmark" analyses case study diversity which is represented in sample of population, for determining representatives of industry and elimination of industry bias [2]. Previously reviewed literature use this approach[3]–[6]. The findings are validated by the application of techniques of qualitative research[7]. The qualitative data is categorised and analysed by application of categorical and open coding. A complimenting method which is time tested for grounded theory is represented by it [8]. The collected data is reliably represented by open coding while profounder concepts are recognized by categorical coding [9]. The approaches of explicit state have connotation that is interpret and evaluated by discourse analysis [10].

III. LITERATURE REVIEW

Reviewed literature did not contain "mutually exclusive viewpoint of supply chains of IoT" and no visible cyber risk [11]. Supply chain models have just position and IoTdigital technologies [12]. Two areas of research are placed together having contrasting effect [13]. The areas of horizontal and vertical integration, visibility of supply chain and smart supply chains are not addressed. Too many topics are represented and focus would lack. The best principles of design, practices, common approaches and standards that affect digital economy's supply chains [14]. The contexts which are related to digital capabilities of SMEs are identified for digital economy [12], which focus on IoT technologies in supply chains.

IV. PROPOSEDFRAMEWORK

Integration of supply chain and business needs consensus on recognition of best integration level, confirmation of compatibility of organisation, attention on collective performance, and integration of operations. It should be a priority to address obstacles of individual integration and collective factors of supply chain should be followed by strategies[15]. Different effect is created by visualization of different categories of integration enabled by holistic design. Figure 1 represents holistic design approach. It is built on a notion of dynamic concept of supply chain and relation of interdependencies where structural elements of a supply chain are based on multilevel strategic themes of a business model which represents a structured system. Thus, decompositions of supply chain design are created by deconstruction of supply chains by applying hierarchical method for network design. Figure 1 illustrates the epistemological framework of knowledge synthesized by models reviewed.

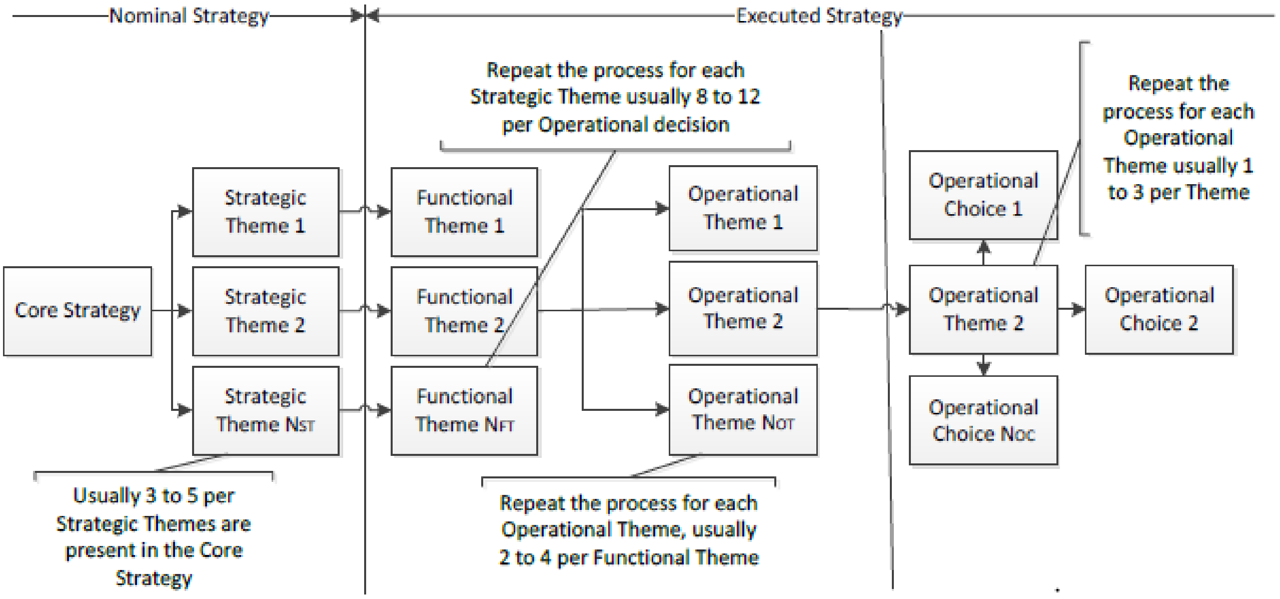
Nominal Strategy
Executed Strategy
Repeat the process for each Strategic Theme usually 8 to 12 per Operational decision
Repeat the process for each Operational Theme usually 1 to 3 per Theme
Core Strategy
Strategic Theme 1
Strategic Theme 2
Strategic Theme NST
Functional Theme 1
Functional Theme 2
Functional Theme NFT
Operational Theme 1
Operational Theme 2
Operational Theme NOT
Operational Choice 1
Operational Theme 2
Operational Choice 2
Operational Choice NOC
Usually 3 to 5 per Strategic Themes are present in the Core Strategy
Repeat the process for each Operational Theme, usually 2 to 4 per Functional Theme

Fig. 1 "Framework synthesising the findings related to designing supply chain model with IoT technologies in the digital economy"

The differentiation of previous models by enabling the investigation of actual capabilities of supply chain by the analysis of digital operational activities in figure 1. A generic design is represented by framework but objectives of specific supply chain are not represented. Instead, the requirements for operational activities is presented as scaffolding by which the themes and categories with cyber activities are populated by enabling the process of design. The comparison of these activities is done with SME supply chains digital activities.

4.1 The Framework - IoT and the Digital Economy

The digital economy has business opportunities in supply chains networking. The productivity of resource is increased, business processes are provided with flexibility and value opportunities are created by enabling customer requirements by smart manufacturing. The IoT theories are integrated and physical systems are controlled and humans and IoT 32 interact. An inherent risk of constant changes in cyber risk exists leading to a range loss and lack of online security threat understanding. The cyber risks are measured with an inconsistency. There is a need to quantify accumulated risk of cyber chain. It is vital to have shared risk in infrastructure in digital economy.

4.2 Framework populating through a Case Study

The "Decision Support System (DSS)" for Digital Economy and IoT are designed by the application of case study research. The participants are requested for defining overall business objective to apply to the concept of IoT.The emerging concepts from interviews are categorised and analysed by applying summative, directive and conventional analysis. The methodology of grounded theory is given in figure 2. It is done for the relation and identification of functional themes that lie behind individual strategic themes[16].

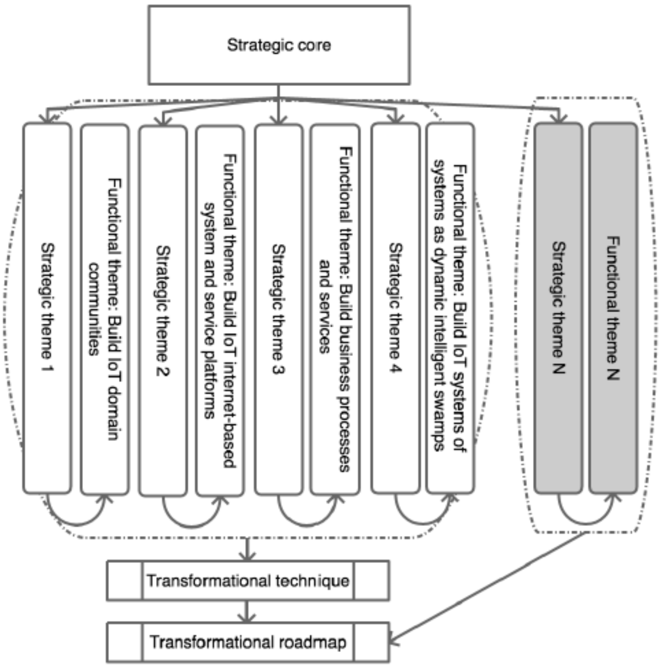
Strategic core
Strategic theme 1
Functional theme: Build IoT domain communities
Strategic theme 2
Functional theme: Build IoT internet-based system and service platforms
Strategic theme 3
Functional theme: Build business processes and services
Strategic theme 4
Functional theme: Build IoT systems of systems as dynamic intelligent swamps
Strategic theme N
Functional theme N
Transformational technique
Transformational roadmap

Fig. 2 Roadmap of DSS for visualisation of supply chain cyber risk

4.4 Conclusion

This work grounds on the representation of generic roadmap for cyber risks segment in supply chains. It has been confirmed by DSS that integration of IoT technologies leads to an inherent cyber risk and the operational capabilities related to cyber are evaluated for visualizing the cyber risk. This work focusses on the development of a system for guiding practitioners and academics in the visualization of cyber risk of supply chain from IoT technology. The information is given by case study by "sustained engagement of the UK EPSRC IoT Research Hub 'PETRAS' (https://www.petrashub.org)" with wide set of partners for wide variety of government agencies, charities and private sectors at international scale.

REFERENCES

[1] F. Russell, "Industry Classification Benchmark (Equity)," *FTSE Group*. 2017.

[2] 565–582. doi:10.1016/j.jaridenv.2004.03.022 Wood, E.., Tappan, G.., Hadj, A., 2004. Understanding the drivers of agricultural land use change in south-central Senegal. J. Arid Environ. 59 *et al.*, "A conceptual framework for analysing and measuring land-use intensity," *Curr. Opin. Environ. Sustain.*, 2013.

[3] C. Tsinopoulos and K. Bell, "Supply chain integration systems by small engineering to order companies," *J. Manuf. Technol. Manag.*, vol. 21, no. 1, pp. 50–62, 2010.

[4] C. Vasiliu and M. Dobrea, "State of implementation of supply chain management in companies in Romania," *Amfiteatru Econ.*, vol. 15, no. 33, pp. 44–55, 2013.

[5] F. Toth and T. Hartvanyi, "Operation and supply chain optimisation for small companies.," *Ann. Fac. Eng. Hunedoara - Int. J. Eng.*, vol. 13, no. 3, pp. 37–44, 2015.

[6] V. C. and D. M., "State of implementation of supply chain management in companies in Romania," *Amfiteatru Econ.*, vol. 15, no. 33, pp. 44–55, 2013.

[7] U. Ramchandra Raut and N. Balaso Veer, “Management research: To understand the role of epistemology in management research,” *J. Manag. Sci.*, vol. 4, no. 1, pp. 2249–1260, 2014.

[8] P. Burnard, “Constructing Grounded Theory: A practical guide through qualitative analysis Kathy Charmaz Constructing Grounded Theory: A practical guide through qualitative analysis Sage 224 £19.99 0761973532 0761973532,” *Nurse Res.*, vol. 13, no. 4, pp. 84–84, 2016.

[9] A. Bryant, *Grounded Theory and Grounded Theorizing*. 2017.

[10] L. Yeomans, “Qualitative methods in business research,” *Action Learn. Res. Pract.*, 2017.

[11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, 2013.

[12] P. Radanliev, D. Charles De Roure, J. R. C. Nurse, P. Burnap, and R. M. Montalvo, “Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies,” *Univ. Oxford*, 2019.

[13] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, “Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance,” 2018.

[14] P. Radanliev *et al.*, “Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0,” 2018.

[15] N. Aydin, “Green supply chain management practices,” *Int. J. Enhanc. Res. Sciece Technol. Eng.*, vol. 4, no. 4, pp. 340–344, 2015.

[16] R. M. Dijkman, B. Sprenkels, T. Peeters, and A. Janssen, “Business models for the Internet of Things,” *Int. J. Inf. Manage.*, 2015.