International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

INTERNET OF THINGS BASED CYBER RISK IMPACT ASSESSMENT PRINCIPLES

[1]THOTA SRAVANTI M.Tech Associate Professor, sravanti815@gmail.com
[2]MOHAMMED MUJEEBULLAH, M.Tech Assistant Professor,m.mujeebullah117@gmail.com
Department-ECE

Pallavi Engineering College Hyderabad, Telangana 501505.

Abstract:
In virtual IoT technologies present new cyber hazard in the supply chain of the digital financial gadget which may be frequently no longer seen to agencies taking factor within the digital supply chains. This paper discusses how the IoT cyber risks may be visualised within the approach of designing enterprise company and supply chain strategies. The literature reviewed consists of company and authorities papers and compares established business and deliver chain fashions with studies on new IoT generation this text defines the layout parameters for an expansion useful resource device for visualising cyber chance from IoT supply chain in the digital financial gadget. The layout approach is grounded on a case study on IoT organizations. The strategies finished in the case study encompass open and precise coding and discourse evaluation.

Keywords: internet-of-things, cyber risk, supply chain strategy, digital technologies, decision support system.

1 Introduction

The digital supply chains expose new types of cyber risk in the digital economy from shared infrastructure. The impact of Internet of Things (IoT) technologies on supply chain cyber risk has rarely been discussed in academic literature. The visibility of cyber risk is especially neglected in the context of IoT digital technology and digital capabilities in small and medium enterprises (SME's) supply chains in the digital economy. The integration of IoT digital technology in supply chains require standardisation reference architecture for managing complexities and resources efficiently. But the digital economy at present lack clarification on individual levels of the strategic, functional and operational challenges from IoT digital technologies in the supply chain.

2 The Methodology

The research methods applied to build the decision support system include literature review and case study and the data is synthesised using the grounded theory approach 1, using qualitative primary and secondary resources and categorising emergent concepts into themes. The diversity of the case study participants represented in the sample population is analysed with reference to the 'Industry Classification Benchmark' 2, to determine the industry representativeness and to eliminate industry bias 3. This approach has been applied previously in peer-reviewed literature 4– 7. The process of ensuring validity of the findings, applied qualitative research techniques 8–10. Open and categorical coding is applied to analyse and categorise the qualitative data. This represents a time-tested complimenting method for grounded theory 11. Open coding provides a reliable representation of the data collected, while categorical coding subsequently recognises the profounder concepts in the data 12. Discourse analysis is applied to evaluate and interpret the connotation behind the explicitly stated approaches 10, along with tables of evidence 13 and conceptual diagrams 14 to present graphical analysis.

3 Literature Review

In the literature reviewed, there is no clear-cut nor mutually exclusive viewpoint on IoT supply chains and the visibility of cyber risk 15. We have a juxtaposition of supply chain models 16 and IoT digital technologies 17. Represented as two research areas being placed close together with contrasting effect 18. From a technical point of view, the review does not address the related areas of vertical and horizontal integration, smart supply chains, and supply chain visibility. That would

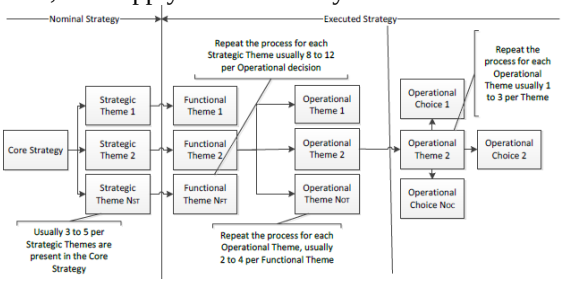

Figure 1: Framework synthesising the findings related to designing supply chain model with IoT technologies in the digital economy

The framework in Figure 1 differentiates from previous models as it enables investigating the supply chain actual capabilities which are analysed through the digital operational activities. The framework represents a generic design and does not represent specific supply chain objectives. Instead, it presents the scaffolding for the required operational activities. The scaffolding enables the design process to populate the categories and

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

themes with cyber activities, related to IoT technologies, and to compare these activities with the digital capabilities in SME's supply chains.

4.1 Building upon the Framework - IoT and the Digital Economy

There are many business opportunities in networking the supply chains with the digital economy 25,27–29. Smart manufacturing would enable economies of scale and individual customer requirements, creating value opportunities 30, increasing resource productivity, and providing flexibility in business processes 31, but requires integration of IoT theories, control of physical systems, and the interaction between humans and IoT 32. There is also an inherent risk as the cyber risk is constantly changing 33, and estimated loss of range variously 33–36 and many SME's lack of understanding about online security threats 37. In addition, there is an inconsistency in measuring cyber risk 38. The supply chain accumulated risk needs to be quantified 17,26,38,39. Literature calculates the impact on organisations stand-alone risk ignoring the cascading impacts of sharing infrastructure 33. Shared risk in infrastructure 40 is vital in the digital economy 41.

4.2 Populating the Framework through Case Study Research

Case study research is applied for designing the Decision Support System (DSS) for the IoT and the Digital Economy. The case study instigates by requesting the participants to define an overall business objective as a vision that can be applied to the IoT concept. Directive, conventional and summative analysis was applied to analyse and categorise the concepts emerging from the interviews. The process in Figure 2 followed the constructivist grounded theory methodology, to identify and relate the functional themes behind individual strategic themes, as described in the framework (Figure 1).

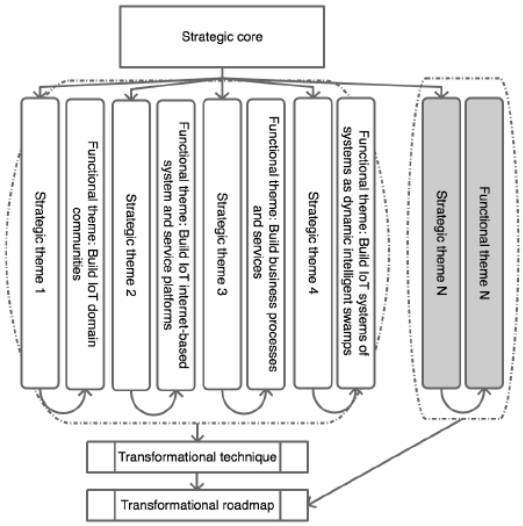

Figure 2: DSS roadmap for visualising supply chain cyber risk

4.3 Discussion

To build the DSS, supply chains must be articulated with consideration of the cyber risks and the operational and digital capabilities for IoT technologies. When multiple parties are involved in the supply chain, the vision to integrate in IoT technologies must be perceived as integrated visions with the other parties and must be correlated to the stated themes and categories.

4.4 Conclusion

The new DSS in this article is grounded on a new framework that represents a generic roadmap for the segments of cyber risks in supply chains, which have until now been overlooked. The DSS confirmed that integrating IoT technologies results with an inherent cyber risk and the cyber risk can be visualised through evaluating the cyber operational capabilities. At a higher analytical level, this article focused on developing a decision support system to provide guidance for academics and practitioners in visualising supply chain cyber risk from IoT digital technology. The case study is also informed by the sustained engagement of the UK EPSRC IoT Research Hub 'PETRAS' (https://www.petrashub.org) with a broad set of user partners for a wide range of private sectors, government agencies, and charities at international scale.

4.5 Limitations and Further Research

Different supply chains could require adjusting the model input, which could contain other types of cyber risks. Further research is needed to apply, test and validate the model for other types of cyber risks e.g. IoT services and third-party software.

4.6 References:

1. Glaser, B. G. & Strauss, A. L. *The discovery of grounded theory : strategies for qualitative research*. (Routledge, 1967).
2. FTSE Russell. Industry Classification Benchmark (ICB) | FTSE Russell. *FTSE International Limited and Frank Russell Company* (2018). At <http://www.ftserussell.com/financial-data/industry-classification-benchmark-icb>
3. Radanliev, P. A conceptual framework for supply chain systems architecture and integration design based on practice and theory in the North Wales slate mining industry. (British Library, 2014). doi:ISNI: 0000 0004 5352 6866
4. Radanliev, P. Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration. *Oper. Supply Chain Manag. An Int. J.* **9,** (2016).
5. Radanliev, P. Green-field Architecture for Sustainable Supply Chain Strategy Formulation. *Int. J. Supply Chain Manag.* **4,** 62–67 (2015).
6. Radanliev, P. Engineering Design Methodology for Green-Field Supply Chain Architectures

Taxonomic Scheme. *J. Oper. Supply Chain Manag.* **8,** 52–66 (2015).
7. Radanliev, P. Architectures for Green-Field Supply Chain Integration. *J. Supply Chain Oper. Manag.* **13,** (2015).
8. Easterby-Smith, M., Thorpe, R. & Lowe, A. *Management research : an introduction*. (SAGE, 2002).
9. Gummesson, E. *Qualitative methods in management research*. (Sage, 2000).
10. Eriksson, P. & Kovalainen, A. *Qualitative methods in business research*. (SAGE, 2008).
11. Charmaz, K. *Constructing grounded theory : a practical guide through qualitative analysis*. (Sage Publications, 2006).
12. Goulding, C. *Grounded theory : a practical guide for management, business and market researchers*. (SAGE, 2002).
13. Eisenhardt, K. M. Building Theories from Case Study Research. *Acad. Manag. Rev.* **14,** 532 (1989).
14. Miles, M. B., Huberman, A. M. & Saldaña, J. *Qualitative data analysis : a methods sourcebook*. (1983).
15. Nurse, J. R. C., Radanliev, P., Creese, S. & De Roure, D. 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* 1–9 (The Institution of Engineering and Technology, 2018). doi:10.1049/cp.2018.0001
16. Radanliev, P., Rowlands, H. & Thomas, A. Supply Chain Paradox: Green-field Architecture for Sustainable Strategy Formulation. in *Cardiff: Sustainable Design and Manufacturing 2014, Part 2, International Conference* (eds. Setchi, R., Howlett, R. J., Naim, M. & Seinz, H.) 839–850 (Future Technology Press, 2014).
17. Radanliev, P., Charles De Roure, D., Nurse, J. R. C., Burnap, P. & Montalvo, R. M. *Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies*. *Working paper*. (2019). doi:10.13140/RG.2.2.32975.53921
18. Radanliev, P. *et al.* 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* **2018,** 3 (9 pp.)-3 (9 pp.) (Institution of Engineering and Technology, 2018).
19. Radanliev, P. *et al.* 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 - 2018* 41 (6 pp.)-41 (6 pp.) (IET, 2018). doi:10.1049/cp.2018.0041
20. Radanliev, P. *et al. Cyber risk impact assessment – assessing the risk from the IoT to the digital economy*. (2019). doi:10.13140/RG.2.2.11145.49768
21. Radanliev, P. *et al. New developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – future developments in the Industrial Internet of Things and Industry 4.0*. (2019). doi:10.13140/RG.2.2.14133.93921
22. Radanliev, P. *et al. Cyber risk from IoT technologies in the supply chain – decision support system for the Industry 4.0*. (2019).
23. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. & Burnap, P. *Standardisation of cyber risk impact assessment for the Internet of Things (IoT)*. (2019). doi:10.13140/RG.2.2.27903.05280
24. Radanliev, P. *et al. Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment*. (Preprints,2019). doi:10.13140/RG.2.2.17305.88167
25. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. & Burnap, P. *The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises*. *Working paper*. (2019).
26. Radanliev, P. *et al. Design principles for cyber risk impact assessment from Internet of Things (IoT). Working paper*. (2019).
27. Radanliev, P., De Roure, D., Nicolescu, R. & Huth, M. *A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0*. *Workingpaper*.(2019).*b*doi:10.13140/RG.2.2.26854.47686
28. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L. *et al. Internet of Things realising the potential of a trusted smart world*. (2018). At <www.raeng.org.uk/internetofthings>
29. Nicolescu, R., Huth, M., Radanliev, P. & De Roure, D. Mapping the values of IoT. *J. Inf. Technol.* 1–16 (2018). doi:10.1057/s41265-018-0054-1