Design principles for cyber risk impact assessment from Internet of Things (IoT)

Preprint · March 2019

DOI: 10.13140/RG.2.2.33014.86083

5 authors, including:

Petar Radanliev
University of Oxford
79 PUBLICATIONS **932** CITATIONS

SEE PROFILE

Design principles for cyber risk impact assessment from Internet of Things (IoT)

Corresponding author: Petar Radanliev: petar.radanliev@oerc.ox.ac.uk [1]

Petar Radanliev[1], David Charles De Roure[1], Jason R.C. Nurse[2], Pete Burnap [3], Eirini Anthi[3], Uchenna Ani[4], La'Treall Maddox[5], Omar Santos[5], Rafael Mantilla Montalvo[5]

[1]Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, petar.radanliev@oerc.ox.ac.uk; david.deroure@oerc.ox.ac.uk; [2]School of Computing, University of Kent, UK, j.r.c.nurse@kent.ac.uk; [3]School of Computer Science and Informatics, Cardiff University, p.burnap@cs.cardiff.ac.uk; [4]STEaPP, Faculty of Engineering Science, University College London, u.ani@ucl.ac.uk; [5]Cisco Research Centre, Research Triangle Park, USA, lamaddox@cisco.com; osantos@cisco.com; montalvo@cisco.com

Funding sources: This work was supported by the UK EPSRC with project [grant number EP/N02334X/1 and EP/N023013/1] and by the Cisco Research Centre [grant number 2017-169701 (3696)].

Abstract:

Digital IoT technologies present new cyber risk in the supply chain of the digital economy which are often not visible to companies participating in the digital supply chains. This paper discusses how the IoT cyber risks can be visualised in the process of designing business and supply chain strategies. The literature reviewed includes industry and government papers and compares established business and supply chain models with studies on new IoT technologies. This article defines the design parameters for a decision support system for visualising cyber risk from IoT supply chain in the digital economy. The design process is grounded on a case study on two IoT companies. The methods applied in the case study include open and categorical coding and discourse analysis.

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

represent too many topics and lead to a lack of focus. Instead, the reviews and categorises the best practices, design principles, common approaches, and standards affecting the supply chains in the digital economy [19]. The review identifies concepts related to the SME's digital capabilities for the digital economy [17,20–26], focusing on the supply chains in relation to IoT technologies.

4 Building a new Framework from Existing Supply Chain Models

Business and supply chain integration requires consensus on objectives, identification of the best level of integration, confirming organisational compatibility, willingness to integrate operations and focus on improved collective performance [3–6].

The focus of business strategies in on supply chain integration, but complexities remain in prioritising collective as opposed to individual performance improvement [5]. Addressing individual integration obstacles should be a priority and strategies should follow the supply chain collective factors [7]. Holistic design would enable visualising how different types of integration, creates different effect. Basic holistic design is represented in Figure 1, building on the notion that supply chain design is a dynamic concept and interdependencies are related in an individual context where the supply chain structural elements are based on a business model as multi-level strategic themes, representing a structured system. Thus, a hierarchical method can be applied for network design and for deconstructing supply chains in hierarchical trees to create supply chain design decompositions. The synthesised knowledge from the reviewed models derives with the initial design of an epistemological framework in Figure 1.

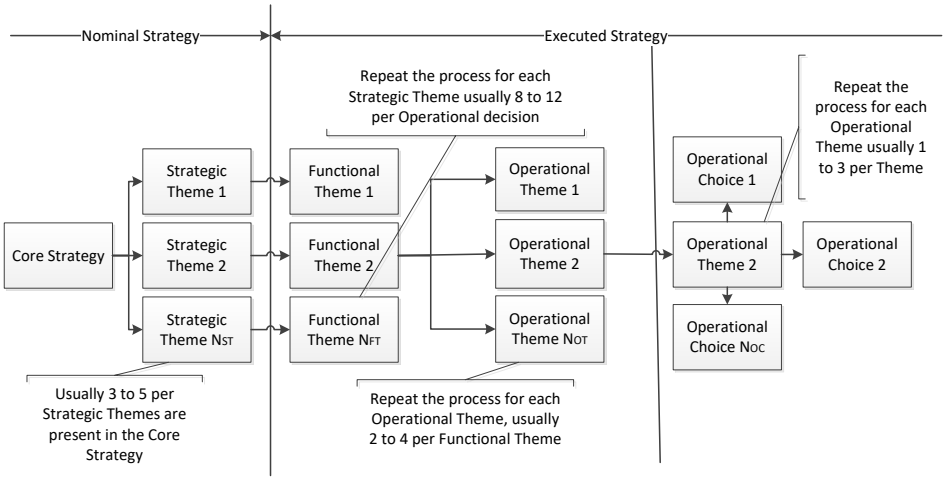

Figure 1: Framework synthesising the findings related to designing supply chain model with IoT technologies in the digital economy

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 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).

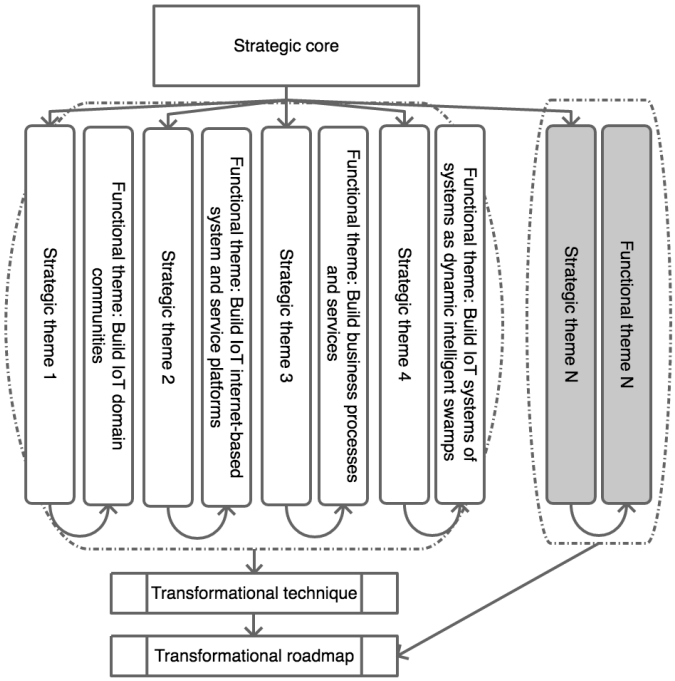

Figure 2: DSS roadmap for visualising supply chain cyber risk

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*. *Working paper.* (2019). 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

30. Nicolescu, R., Huth, M., Radanliev, P. & De Roure, D. *State of The Art in IoT - Beyond*

Economic Value. (2018). at <https://iotuk.org.uk/wp-content/uploads/2018/08/State-of-the-Art-in-IoT-–-Beyond-Economic-Value2.pdf>

31. Hussain, F. in *Internet of Things: Building Blocks and Business Models: SpringerBriefs in Electrical and Computer Engineering* 1–11 (Springer International Publishing, 2017). doi:10.1007/978-3-319-55405-1_1

32. Marwedel, P. & Engel, M. in 1–30 (Springer International Publishing, 2016). doi:10.1007/978-3-319-26869-9_1

33. DiMase, D., Collier, Z. A., Heffner, K. & Linkov, I. Systems engineering framework for cyber physical security and resilience. *Environ. Syst. Decis.* **35,** 291–300 (2015).

34. Biener, C., Eling, M. & Wirfs, J. H. Insurability of Cyber Risk 1. *The Geneva Association* 1–4 (2014). at <https://www.genevaassociation.org/media/891047/ga2014-if14-biener_elingwirfs.pdf>

35. Shackelford, S. J. Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Rev.* **19,** 412–445 (2016).

36. Koch, R. & Rodosek, G. *Proceedings of the 15th European Conference on Cyber Warfare and Security : ECCWS 2016 : hosted by Universität der Bundeswehr, Munich, Germany 7-8 July 2016*. (2016). at <https://books.google.co.uk/books?hl=en&lr=&id=ijaeDAAAQBAJ&oi=fnd&pg=PA145&dq=economic+impact+of+cyber+risk&ots=50mTo8TVSV&sig=sD4V76yG5tG6IZIglmnGz3L1qqw&redir_esc=y#v=onepage&q=economic impact of cyber risk&f=false>

37. Baker, G., Lomax, S., Braidford, P., Allinson, G. & Houston, M. Digital Capabilities in SMEs: Evidence Review and Re-survey of 2014 Small Business Survey respondents. (2015). at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/457750/BIS-15-509-digital-capabilities-in-SMEs-evidence-review-and-re-survey-of-2014-small-business-survey-respondents.pdf>

38. Ruan, K. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Comput. Secur.* **65,** 77–89 (2017).

39. Radanliev, P. *et al. Definition of Cyber Strategy Transformation Roadmap for Standardisation of IoT Risk Impact Assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart*. *Working paper.* (2019).

40. Radanliev, P. *et al.* Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **102,** 14–22 (2018).

41. Rajkumar, R., Lee, I., Sha, L. & Stankovic, J. Cyber-Physical Systems: The Next Computing Revolution. in *Proceedings of the 47th Design Automation Conference on - DAC '10* 731 (ACM Press, 2010). doi:10.1145/1837274.1837461