Peer-reviewed version available at SN Applied Sciences 2020, 2, 169; doi:10.1007/s42452-019-1931-0

CYBER RISK IMPACT ASSESSMENT

ASSESSING THE RISK FROM THE IOT TO THE DIGITAL ECONOMY

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

Petar Radanliev[1], Dave De Roure[1], Jason R.C. Nurse[2], Razvan Nicolescu[3], Michael Huth[3],

Stacy Cannady[4], Rafael Mantilla Montalvo[4]

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

We present an updated design process for adapting and integrating existing cyber risk assessment approaches for impact assessment for the risk from IoT to the digital economy. The new design process includes a set of changes to the original standards (e.g. NIST) that are adapted for the IoT cyber risk in this paper. This paper also presents a new framework for impact assessment of IoT cyber risk, specific for the digital economy.

Keywords: Cyber risk; Internet of Things cyber risk; Digital Economy Risk Assessment; Economic Impact Assessment.

1 Introduction

The developments in IoT technologies have presented new types of cyber risk which are difficult to assess with the existing cyber risk approaches. This creates a specific risk for the digital economy that cannot be assessed with the existing models. This research aims to define the parameters for adapting and integrating these models for performing cyber risk assessment with the existing cyber security

frameworks, models and methodologies but for the IoT risk in the digital economy. This has not been done until present. The adapting and integrating process in this article refers to the compounding of knowledge to offer a better understanding of cyber risk assessments for the IoT risk in the digital economy.

2 Methodology

We use practical studies to bridge the gaps, to assess the impact and overcome some of the cyber risk limitations and to construct the relationship between IoT and the digital economy.

The methodology applies theoretical analysis through logical discourse of knowledge [1], to define what does it mean to say that we understand something [2], referring to the question of assessing cyber risk from IoT in the digital economy. The aim of the research is to define how do we understand that we really understand cyber risk assessment. This approach was considered relevant to this question because most cyber security frameworks and methodologies propose answers to a quantitative question with qualitative assessments [3–10].

3 Literature Review

The increasing number of high-impact cyber-attacks has raised concerns of the economic impact [11] and the issues from quantifying cyber insurance [12]. This triggers questions on our ability to measure the impact of cyber risk [13]. The literature review is focused on defining the IoT risk vectors for the digital economy [14], which are often overlooked by cyber security experts [10]. The IoT risk vectors are investigated in the context of Social Internet of Things [15], the digital economy and the Industrial Internet of Things (IIoT). In the Social Internet of Things, the IoT is autonomously establishing social relationships with other objects, and a social network of objects and humans is created [16,17]. The digital economy is also known as the fourth industrial revolution and brings new operational risk for connected digital cyber networks [18]. Finally, the IIoT represents the use of IoT technologies in manufacturing [19].

The cyber risk challenges from IoT technological concepts, mostly evolve around the design and the potential economic impact (loss) from cyber-attacks [4,5]. There are multiple attempts in literature

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 April 2019 doi:10.20944/preprints201903.0109.v2

Peer-reviewed version available at SN Applied Sciences 2020, 2, 169; doi:10.1007/s42452-019-1931-0

where existing models are applied understand the economic impact of cyber risk [11]. However, understanding the shared risk is vital for risk assessment [20,21]. Because the cyber risk estimated loss range can vary significantly [22–26].

IoT technologies need to be supported with supply chain process for updating the list of assets that are added to the network across multiple time-scales [27–31], to prevent IoT components modified to enable a disruption [4,5,7]. But such digital supply chain system security is complex and risk assessing IoT systems for the digital economy is not easy. Regardless of the difficulties, the digital economy networks need to be secure, vigilant, resilient and integrated. But the reality of assessing security risks in Internet of Things systems is that *'If you can't understand it, you can't properly assess it!'*[20]. In what follows, we reflect on cyber risk standards, frameworks and models. The diversity of approaches for cyber risk impact assessment, reemphasises the requirement for standardisation of cyber risk assessment approaches. This becomes clearly visible in Table 2. This variety of approaches presents conflict in risk assessment [4,5,14,32–36,6–13]. To avoid such conflicts, the core cyber impact assessment concepts are extracted to defining the design principles for cyber risk impact assessment from IoT in the digital economy.

Frameworks	**ISO**	**NIST**	**FAIR**
Measure	ISO 27032	Categorising	Financial
Standardise	ISO 27001	Assembling	Complementary
Compute	Compliance	Compliance	Quantitative
Recover	ISO 27031	Compliance	Level of exposure
Methodologies	**TARA**	**CMMI**	**OCTAVE**
Measure	Threat Matrix	Maturity models	Workshops
Standardise	Template threats	ISO 15504 - SPICE	Repeatability
Compute	Qualitative	Maturity levels	Qualitative
Recover	System recovery	Refers to other standards.	Impact areas
Systems	**Exostar system**	**CVSS calculator**	
Measure	ISO 27032	Base metrics	
Standardise	ISO 27001	Mathematical approximation	
Compute	Compliance	Qualitative	
Recover	ISO 27031	Not included	
Models	**RiskLens**	**CyVaR**	
Measure	BetaPERT distributions	VaR	
Standardise	Adopt FAIR	World Economic Forum	
Compute	Quantitative risk analytics with Monte Carlo and sensitivity analysis	Quantitative risk analytics with Monte Carlo	
Recover	Not included	Not included	

Table 1: Analysis of cyber risk frameworks, methodologies, systems and models that can be applied for assessing the IoT cyber risk for the digital economy

The Table 2 has highlighted the challenges in adopting existing cyber risk frameworks for dynamic and connected systems, where the IoT presents great complexities. For example the challenges pertaining to the limited knowledge that risk assessors have of dynamic IoT systems [21].

3.1 Proposed framework for IoT cyber risk assessment for the digital economy

To define a framework for IoT cyber risk assessment for the digital economy, firstly the controlled convergence method [31,37] is applied with a group of experts in the field. The results from the study were presented, including the Table 1, to a group of experts. The controlled convergence was applied to organise the emerging concepts into definitions of the design principles. This approach to pursuing validity follows existing literature on this topics [38,39] and provides clear definitions that specify the units of analysis for IoT cyber risk for the digital economy. The reason for pursuing clarity on the units of analysis for IoT cyber risk, was justified by existing literature, where these are identified as recommended areas for further research [40]. Then, the IoT risk units of analysis from the digital economy are combined into IoT cyber risk vectors associated to units of analysis for specific IoT vectors (in Table 2). In the transcription process, discourse analysis [41] is applied to interpret the data and for recognising the most profound concepts in the data [42].

The Table 2 below presents the IoT risk vectors and the associated units of analysis in a framework. The framework emerges from the decomposition of existing knowledge and understanding, gathered from the current understanding of the IoT cyber risk for the digital economy. The framework is analysed and verified with the controlled convergence method [31,37] for concept selection and for validation of research design.

IoT cyber risk				
Cyber risk vectors	Vector 1	Vector 2	Vector 3	Vector 4
	Cloud	Real-time	Autonomous	Recovery

Vector units of analysis	Cloud-computing platforms; technology skills; data centres; software; guidance; monitoring; Integration in cloud computing; Society 5.0; security networks.	Operational models in real time; Customised products in real time; Digital real-time and interoperable records; Platform for real-time information; Connected industries; CPS.	Automated environments; Robotics and Autonomous Systems; Robotics and artificial intelligence; Active cyber defence; Robots innovation; Robot society; Robotics in IoT; Artificial intelligence and control systems.	Economic impact; Impact assessment; SWAT analysis; HADA - Advanced self-diagnosis tool; Financial and fiscal state control.
Standardisation framework for cyber risk assessment				
Measure	ISO 27032; Categorising; Financial; Threat Matrix; Maturity models; Workshops; ISO 27032; Base metrics; BetaPERT distributions; VaR			
Standardise	ISO 27001; Assembling; Complementary; Template threats; ISO 15504 – SPICE; Repeatability; ISO 27001; Mathematical approximation; Adopt FAIR; World Economic Forum			
Compute	Compliance; Quantitative; Maturity levels; Qualitative; Quantitative risk analytics with Monte Carlo and sensitivity analysis.			
Recover	ISO 27031; Compliance; Level of exposure; System recovery; Impact areas.			

Table 2: Framework for IoT cyber risk vectors and units of analysis for impact assessment – specific for IoT risk on the digital economy

Table 3 defines the IoT cyber risk vectors for the digital economy and relates the risk vectors with units of analysis. Defining the IoT cyber risk vectors and the related units of analysis, represents a crucial milestone in defining the design principles for cyber risk assessment of the IoT risk in the digital economy.

Secondly, the study recommends a decomposition process of cyber risk assessment standards. At a higher analytical level, in Figure 1, the new risk vectors are related to a step by step design process for assessing the cyber risk from IoT risk vectors. The design process refers to established risk assessment frameworks, methodologies and models that have extensively been discussed in existing literature [4,5,7,10–14].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 April 2019 doi:10.20944/preprints201903.0109.v2

Peer-reviewed version available at SN Applied Sciences 2020, 2, 169; doi:10.1007/s42452-019-1931-0

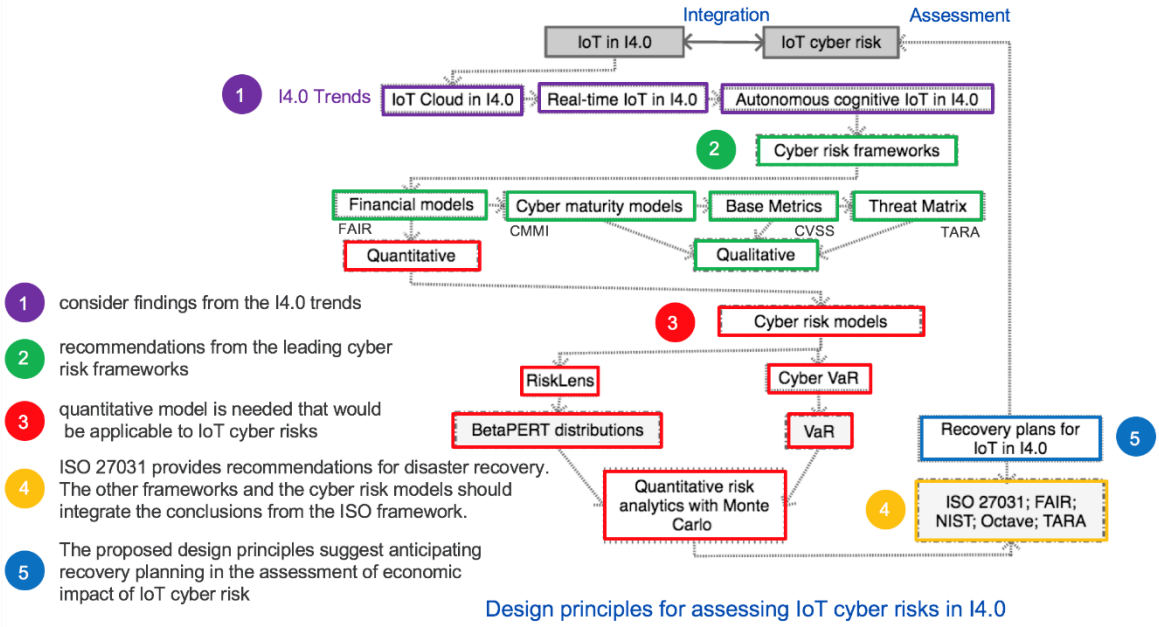

Figure 1: Design process for assessing IoT cyber risks for the digital economy

The rationale of the proposed design process is that the design is developed to advance the existing efforts [20,32] in developing a standardised approach for assessing the impact of IoT cyber risks for the digital economy [34,43].

4 Conclusion

This article decomposes the cyber risk assessment standards and combines concepts for the purposes of building a new IoT risk impact assessment approach for the digital economy. Despite the interest to standardise existing cyber risk frameworks, models and methodologies, this has not been done until present. Cyber risk impact assessment approach for the IoT risk in the digital economy currently does not exist in literature. The framework represents the first attempt to define a process for cyber risk impact assessment of IoT vectors. The study advances the efforts of integrating standards and governance on IoT cyber risk and offers a better understanding of the IoT impact assessment for cyber risk.

4.1 Limitations and further research

The framework in this article is derived from case studies, supported with theoretical analysis of a limited set of frameworks, models, methodologies and high-tech strategies. The set selection was

based on documented availability and on relevance to cyber risk impact assessment of IoT risk vectors. Additional research is required to integrate the knowledge from other risk assessment approaches. This research is conducted already and the aim is to publish the findings in a series of papers [3,4,13,14,20,27–33,5,34–37,43,44,6–12].

5 References

1. Steup, M. *Epistemology: Stanford encyclopedia of philosophy*. (Stanford University. Center for the Study of Language and Information (U.S.), 2005).

2. Wenning, C. J. Scientific epistemology: How scientists know what they know. *J. Phys. Tchr. Educ. Online* **5**, (2009).

3. Radanliev, P., De Roure, D., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. *Cyber risk impact assessment – assessing the risk from the IoT to the digital economy*. (2019). doi:10.13140/RG.2.2.11145.49768

4. Radanliev, P., DeRoure, D., Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *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). doi:10.13140/RG.2.2.12462.77124

5. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Eirini Anthi, Ani, U., … Montalvo, R. M. *Design principles for cyber risk impact assessment from Internet of Things (IoT). Wokring paper.* (2019). doi:10.13140/RG.2.2.33014.86083

6. Radanliev, P., De Roure, D. C., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. *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

7. 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). doi:10.13140/RG.2.2.14140.49283

8. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *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

9. 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

10. 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

11. Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. & Burnap, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **102**, 14–22 (2018).

12. Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. ., Nicolescu, R. & Huth, M. 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* 3 (9 pp.) (Institution of Engineering and Technology, 2018). doi:10.1049/cp.2018.0003

13. Radanliev, P., De Roure, C. D., Nurse, .R.C., Nicolescu, R., Huth, M., Cannady, C. & Montalvo, R. M. 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

14. 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

15. Atzori, L., Iera, A., Morabito, G. & Nitti, M. The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Comput. Networks* **56**, 3594–3608 (2012).

16. Ortiz, A. M., Hussein, D., Park, S., Han, S. N. & Crespi, N. The Cluster Between Internet of Things and Social Networks: Review and Research Challenges. *IEEE Internet Things J.* **1**, 206–215 (2014).

17. Hussein, D., Han, S. N., Lee, G. M., Crespi, N. & Bertin, E. Towards a dynamic discovery of smart services in the social internet of things. *Comput. Electr. Eng.* **58**, 429–443 (2017).

18. Peasley, S., Waslo, R., Lewis, T., Hajj, R. & Carton, R. *Industry 4.0 and cybersecurity Managing risk in an age of connected production*. (2017).

19. IIC. *The Industrial Internet of Things Volume G5: Connectivity Framework; Industrial Internet Consortium*. (2017).

20. 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

21. Nurse, J., Creese, S. & De Roure, D. Security Risk Assessment in Internet of Things Systems. *IT Prof.* **19**, 20–26 (2017).

22. Biener, C., Eling, M. & Wirfs, J. H. Insurability of Cyber Risk 1. *The Geneva Association* 1–4 (2014).

23. 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).

24. 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).

25. 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).

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

27. Radanliev, P. Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration. *Oper. Supply Chain Manag. An Int. J.* **9**, (2016).

28. Radanliev, P. Green-field Architecture for Sustainable Supply Chain Strategy Formulation. *Int. J. Supply Chain Manag.* **4**, 62–67 (2015).

29. Radanliev, P. Engineering Design Methodology for Green-Field Supply Chain Architectures Taxonomic Scheme. *J. Oper. Supply Chain Manag.* **8**, 52–66 (2015).

30. Radanliev, P. Architectures for Green-Field Supply Chain Integration. *J. Supply Chain Oper. Manag.* **13**, (2015).

31. 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).

32. Nicolescu, R., Huth, M., Radanliev, P. & De Roure, D. *State of The Art in IoT - Beyond Economic Value*. (2018).

33. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *Cyber risk from IoT technologies in the supply chain – decision support system for the Industry 4.0*. (2019). doi:10.13140/RG.2.2.17286.22080

34. 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

35. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Rafael, M. M. & Burnap, P. *Supply Chain Design for the Industrial Internet of Things and the Industry 4.0*. (2019). doi:10.13140/RG.2.2.36311.32160

36. Radanliev, P., Charles De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R. & Ani, U. *Cyber Risk in IoT Systems*. *Journal of Cyber Policy* (2019). doi:10.13140/RG.2.2.29652.86404

37. 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

38. Axon, L., Alahmadi, B., Nurse, J. R. C., Goldsmith, M. & Creese, S. Sonification in Security Operations Centres: What do Security Practitioners Think? in *Proceedings of the Workshop on Usable Security (USEC) at the Network and Distributed System Security (NDSS) Symposium* 1–12 (2018).

39. Eggenschwiler, J., Agrafiotis, I. & Nurse, J. R. Insider threat response and recovery

strategies in financial services firms. *Comput. Fraud Secur.* **2016**, 12–19 (2016).

40. de Reuver, M., Sørensen, C. & Basole, R. C. The digital platform: a research agenda. *J. Inf. Technol.* 1–12 (2017). doi:10.1057/s41265-016-0033-3

41. Eriksson, P. & Kovalainen, A. *Qualitative methods in business research*. (SAGE, 2008).

42. Goulding, C. *Grounded theory : a practical guide for management, business and market researchers*. (SAGE, 2002).

43. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B., Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., … R.J., Westbury, P. S. *Internet of Things realising the potential of a trusted smart world*. (2018).

44. Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R. & Huth, M. *Analysing IoT cyber risk for estimating IoT cyber insurance*. (2019). doi:10.13140/RG.2.2.25006.36167