Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardization of Regulations, Risk Maturity, Strategy Design and Impact Assessment

Petar Radanliev and David De Roure and Jason R.C. Nurse and Pete Burnap and Eirini Anthi and Uchenna Ani and La'Treall Maddox and Omar Santos and Rafael Mantilla Montalvo

Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, School of Computing, University of Kent, UK, School of Computer Science and Informatics, Cardiff University, STEaPP, Faculty of Engineering Science, University College London, Cisco Research Centre, Research Triangle Park, USA

5 March 2019

University of Oxford

Type of the Paper: Article

Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardization of Regulations, Risk Maturity, Strategy Design and Impact Assessment

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

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

Abstract: The Internet-of-Things (IoT) enables enterprises to obtain profits from data but triggers data protection questions and new types of cyber risk. Cyber risk regulations for the IoT however do not exist. The IoT risk is not included in the cyber security assessment standards, hence, often not visible to cyber security experts. This is concerning, because companies integrating IoT devices and services need to perform a self-assessment of its IoT cyber security posture. The outcome of such self-assessment needs to define a current and target state, prior to creating a transformation roadmap outlining tasks to achieve the stated target state. In this article, a comparative empirical analysis is performed of multiple cyber risk assessment approaches, to define a high-level potential target state for company integrating IoT devices and/or services. Defining a high-level potential target state represent is followed by a high-level transformation roadmap, describing how company can achieve their target state, based on their current state. The transformation roadmap is used to adapt IoT risk impact assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart model.

Keywords: Internet of Things; Micro Mart model; Goal-Oriented Approach; transformation roadmap; Cyber risk regulations; empirical analysis; cyber risk self-assessment; cyber risk target state

1 Introduction

Economic impact of Internet-of-Things (IoT) cyber risk is increasing with the integration of digital infrastructure in the digital economy (Petar Radanliev *et al.*, 2018). Cyber security standardisation and regulation would play a key role in the process of reducing cyber-attacks while continuing to harness the economic values.

The cyber risk from IoT devices is present across different and sometimes at a higher level in sectors where such risk is unexpected. For example, in the US, healthcare is now the largest target of cyber security attacks, reportedly at greater risk than manufacturing and banking (IBM, 2016). According to the same report (IBM, 2016), the value of stolen personal health information is ten to twenty times greater than the value of a stolen credit card number. To understand and define a

generic target state for cyber maturity, we need to understand the business context and the cyber risk priorities through discussions between cyber security experts and decision makers (Deloitte, 2017).

This research article conducts epistemological analysis focused on understanding the best approach for increasing safety, security and economic value in the IoT space. Our research has two objectives. To identify and capture a high-level target state for the mitigation of cyber risk from the IoT, and to adapt existing cyber security practices and standards to include IoT cyber risk in a high-level cyber security transformation roadmap. We discuss and expand on these further in the remainder of this article. In Section 2 we present the research methodology.

2 Methodology

There is a strong interest in regulating the cyber risk assessment procedures. Regulation and standardisation of cyber security frameworks, models and methodologies has not been done until present. Standardisation in this article refers to the compounding of knowledge to advance the efforts on integrating cyber risk standards and governance, and to offer a better understanding of cyber risk assessments. Here we combine literature analysis with an empirical with a comparative analysis. The empirical analysis is conducted with seven cyber risk frameworks and two cyber risk models. The comparative analysis engages with fifteen high-tech national strategies.

3 Current state of cyber risk

Current cyber risk trends are based on risk from intelligent manufacturing equipment, artificial intelligence, the cloud, and IoT, creating risk from systems of machines capable of interacting with the cyber-physical world (Nurse *et al.*, 2018; P. Radanliev, D. De Roure, *et al.*, 2018). The integration of new technologies creates cyber security risk, e.g. integrating less secured systems (Carruthers, 2016) in manufacturing (DiMase *et al.*, 2015) and supply chains (Radanliev, Rowlands and Thomas, 2014; Radanliev, 2015c, 2015a, 2015b, 2016). Existing cyber risk assessment models (Gordon and Loeb, 2002; Rodewald and Gus, 2005; Anderson and Moore, 2006; World Economic Forum, 2015; Koch and Rodosek, 2016; Roumani *et al.*, 2016; Ruan, 2017) ignore the risk impacts of sharing infrastructure and the cyber risk estimated loss range variously (Petar Radanliev *et al.*, 2018). Further cyber risk assessment challenges emerge from compiling of connected systems devices and platforms (Nurse, Creese and De Roure, 2017; Nurse *et al.*, 2018). The machines are becoming social CPS (Evans and Annunziata, 2012; Giordano, Spezzano and Vinci, 2016; Marwedel and Engel, 2016) operating as real-time IoT systems of systems (Wang, Törngren and Onori, 2015; Leitão, Colombo and Karnouskos, 2016), creating cyber risk from data in transit. This requires standardisation of design and process (Sangiovanni-Vincentelli, Damm and Passerone, 2012; Ruan, 2017) because such system security is complex.

4 Uncovering the best method to define a unified cyber risk assessment through a comparative empirical research study

4.1 Comparative study of IoT in Industry 4.0

From this comparative study, the main IoT risk elements of each IoT strategy are compounded into categories representing the most prominent IoT cyber risk vectors (see Table 1). However, the compelling of data into these categories is quite challenging, as some strategies, represent a collection of descriptive explanations and do not provide explicit IoT cyber risk vectors. Such descriptive explanations present complexities in developing a unifying strategy. To resolve this issue, we use the grounded theory methodology, where most prominent IoT cyber risk vectors are categorised and used as reference themes. Then, the categories are used for examining IoT cyber risk, to define a standardisation approach that relates various IoT risk vectors to eliminate conflicts in different and sometimes contrasting assessments of risk vectors.

4.2 Empirical analysis of gaps in cyber risk impact assessment approaches

The empirical analysis aims to identify cyber security frameworks and to compare interlinkages with the IoT risk in the Industry 4.0. Some of the frameworks reviewed propose diverse qualitative methods, and some qualitative approaches for measuring cyber risk propose methodologies(Petar Radanliev, D. C. De Roure, Nurse, Burnap, Anthi, *et al.*, 2019b, 2019a; Petar Radanliev, D. De Roure, *et al.*, 2019; Petar Radanliev, D. De Roure, Nurse, Nicolescu, Huth, *et al.*, 2019d, 2019c).

The most advanced cyber risk impact assessment framework is the US NIST (NIST, 2017). The NIST framework argues that to reach the required cyber security maturity level, the current cyber state can be transformed into a given a target cyber state by applying a specific cyber security framework implementation guidance (Barrett *et al.*, 2017). However, the NIST guidance is specifically designed for Federal Agencies and requires adaptations to be applicable to enterprises. The NIST framework requires determining a detailed current cyber profile and a maturity level but does not provide a model for these steps.

The CVSS calculator (FIRST, no date; CVSS, 2017) could be used to create a current cyber profile, in addition to the Exostar system (Shaw *et al.*, 2017) for determining the supply chain cyber maturity level, and CMMI (CMMI, 2017) the overall current state of cyber maturity. The final gap in the NIST framework is the lack of cyber risk quantitative assessment, which is crucial for making an informed and detailed recommendations for a target cyber profile. The Factor Analysis of Information Risk Institute (FAIR) (FAIR, 2017a) aims to address this gap in the NIST framework. FAIR Institute adapts existing quantitative models, e.g. RiskLens (RiskLens, 2017), and Cyber VaR (CyVaR) (FAIR, 2017b). In a way, FAIR is complementing the work of NIST and the International Organisation for Standardisation (ISO) (ISO, 2017), which is the international standard-setting body and includes cyber risk standards. Notable for this discussion, only FAIR (FAIR, 2017a) provides recommendations for quantitative risk estimation. To complete the risk assessment, the cyber risk from supply chains needs to be simplified (Petar Radanliev, D. C. De Roure, Nurse, Montalvo and Burnap, 2019b, 2019a; Petar Radanliev, D. De Roure, *et al.*, 2019). To identify a current cyber risk state that includes supply chain cyber risks, the Exostar system (Shaw *et al.*, 2017), can be used for complimenting the CVSS and covering the supply chain aspect of cyber risk. Further analysis, including SWAT and GAP analysis are considered beyond the scope of this conference paper, but can be found in other articles (P. Radanliev, C. D. De Roure, *et al.*, 2018; P. Radanliev *et al.*, 2019; Petar Radanliev, D. C. De Roure, Nurse, Burnap, *et al.*, 2019; Petar Radanliev, D. C. De Roure, Nurse, Montalvo and Burnap, 2019a; Petar Radanliev, D. C. De Roure, Nurse, Montalvo, Burnap, *et al.*, 2019).

4.3 Transformation roadmap for standardisation of IoT risk impact assessment

To define a transformation roadmap for standardisation of IoT risk impact assessment, the methodology follows recently established approaches (Nicolescu *et al.*, 2018; Nurse *et al.*, 2018; P. Radanliev, C. D. De Roure, *et al.*, 2018; P. Radanliev, D. De Roure, *et al.*, 2018; Petar Radanliev *et al.*, 2018; Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith *et al.*, 2018; Petar Radanliev, D. C. De Roure, Nurse, Montalvo, Burnap, *et al.*, 2019). The design principles define how to identify, manage, estimate, and prioritise cyber risk (Table 1).

Vectors	FAIR	CMMI	CVSS	ISO	NIST	Octave	TARA
Risk identification (measure)	Financial	Maturity models	Base metrics	ISO 27032	Categorising	Workshops	Threat Matrix
Risk management (standardise)	Compliance	ISO 15504 - SPICE	Mathematical approximation	ISO 27001	Assembling	Repeatability	Template threats
Risk estimation (compute)	Quantitative	Maturity levels	Qualitative	Compliance	Compliance	Qualitative	Qualitative
Risk prioritisation (strategy)	Level of exposure	N/A	N/A	ISO 27031	Compliance	Impact areas	System recovery

Table 1: High level target state for standardisation of IoT risk impact assessment

In Table 1, the resulting definition of transformation roadmap are reduced in content with the controlled convergence methods (Petar Radanliev, D. De Roure, *et al.*, 2019).

5 Case study research

5.1 The case study

The case study research involved four workshops that included 18 distinguished engineers from Cisco Systems, and 2 distinguished engineers from Fujitsu. The workshops with Cisco Systems were conducted in the USA in four different Cisco research centres. These centres were as follows: First Centre - Security and Trust Organisation; Second Centre - Advanced Services; Third Centre - Security Business Group; and Fourth Centre - Cisco Research Centre. In pursuit of validity, a separate workshop was conducted with two experts from Fujitsu centre for Artificial Intelligence the UK. The Fujitsu workshop was conducted separately to avoid those experts being influenced or outspoken by the larger group from Cisco systems.

The first two Cisco workshops were conducted to apply the controlled convergence (Radanliev, 2015a; Petar Radanliev, D. De Roure, *et al.*, 2019). This approach to pursuing validity follows existing literature on this topics (Eggenschwiler, Agrafiotis and Nurse, 2016; Axon *et al.*, 2018) and provides clear definitions that specify the units of analysis for IoT cyber risk vectors. The IoT risk units of analysis from individual IoT strategy are combined into standardisation vectors. The process of defining the standardisation vectors followed the controlled convergence method (Radanliev, 2014, 2015c), where experts were asked to confirm the valid concept, merge duplicated concepts, and delete conflicting concepts. The main limitation of the Pugh controlled convergence method is the difficulty in gathering large number of experts in one location.

5.2 Transformation imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach

Following the identification of a high-level target state in the comparative empirical analysis, the controlled convergence was applied to narrow the emerging implementation tasks through case study. The controlled convergence was applied for the development of a transformation roadmap for the high-level target state (Table 1). To build the transformation roadmap, the emerging categories are validated with applying the controlled convergence with a group of experts. The process of confirming validity of the data in Table 2, outlines the transformation process but does not include all the steps as the aim is to present a methodology, not the actions. The rationale is that different enterprises will have different cyber security steps to perform in order to transition to a higher maturity lever. A long and detailed list of steps can be found in some of our work in progress articles (Petar Radanliev, D. C. De Roure, Nurse, Burnap, *et al.*, 2019; Petar Radanliev, D. C. De Roure, Nurse, Montalvo and Burnap, 2019a, 2019b).

High level transformation imperatives
Training and awareness
Control goal (parent) 1: Security skills assessment and training
Control objective (child) 1: Skills and integrated plan to support defence of the enterprise.
Control element (orphan) 1: Analysis of needed skills; provide training to match the required skills and validate skills through periodic tests. More advanced control orphans include: security assessments using real-world examples to measure mastery or skills.
Control goal (parent) 2: Penetration testing.
Control objective (child) 2: Test the defences by simulating cyber-attacks.
Control element (orphan) 2: Regular focussed penetration tests for detecting unprotected systems through vulnerability scanning and penetration testing combined.
Control goal (parent) 3: Mobile device
Control objective (child) 3: Mitigate cyber risk from mobile devices.
Control element (orphan) 3: Mobile devices should have access controls to enforce policies and option to remotely clean the device.

Cyber threat intelligence
Control goal (parent) 1: Boundary defence
Control objective (child) 1: Manage the flow of information between network trust levels.
Control element (orphan) 1: Prevent communications with malicious IP addresses, use two-factor identification; design DMZ network and scan connections that aim to bypass the DMZ; block known bad signature or attack behaviour.
Security event monitoring
Notes: links with: (a) network security; (b) identity and access management.
Control goal (parent) 1: Maintenance, monitoring and analysis of audit logs
Control objective (child) 1: Collect, manage and analyse audit logs of events.
Control element (orphan) 1: Two synchronised timestamps in logs to ensure consistency; develop a log retention policy.
Control goal (parent) 2: Secure configurations for network devices such as firewalls, routers and switches
Control objective (child) 2: Actively manage the security configuration of the network infrastructure.
Control element (orphan) 2: Documenting all new configurations rules that allow traffic to flow through network security devices; use two-factor identification and encryption.
Control goal (parent) 3: Account monitoring and control
Control objective (child) 3: Control the life-cycle of system and application accounts.
Control element (orphan) 3: Disable unused account; imprint accounts expiration date; enable revoking system access accounts; log-off users after a standard period of inactivity; encrypt transmitted passwords.

Table 2: Transformation roadmap- describing examples of how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach

For implementing the recommendations emerging from the transformational imperatives, we refer to the NIST cyber security implementation tiers as support guidance. These implementation steps are the prime focus of government and industry efforts for improving cyber security exposure. In the following section, the transformation roadmap and imperatives can be used to define a new IoT risk impact assessment with a goal-oriented approach and the Internet of Things Micro Mart model.

6 IoT risk impact assessment with the transformation roadmap and imperatives

Dependency goal-oriented modelling can be applied to connect unconnected risk models and to build a risk model for a complex IoT systems. The first step is to link separate models. This requires identifying the shared principles from the multiple models that we are connecting. Then, to determine the level of dependency risk, we need to understand the dependencies of the shared principles.

6.1 IoT Risk Analysis through Functional Dependency

Dependency modelling and analysis provides a means to support the management of functional and operational complexities within IoT systems with focus on the system elements, measures of a design or operational challenge, as well as the functional dependencies that define their associations. Dependency modelling and analysis can support a superior understanding of connectivity and its implications on performance, and can assist in constructing, improving, and maintaining of such complex system. The construct and exchanges that happen in IoT domain defines a tightly coupled association amongst constituting components and sub-systems such considerably on the correct functions of another linked component or system. This is considered a dependency relationship, and can either be direct (a first order dependency) or indirect (a subsequent higher order dependency) (Laugé, Hernantes and Sarriegi, 2015). For example, from a typical IoT architecture (Bilal, 2017), normal functions for components and services on the application layer typically depend on the normal functioning of their counterparts on the network layer. This latter also relies on the perception layer component and services. If a component or service on the perception layer is compromised, such impairment can alter the correct functioning of connected component or service on the network or application layers. Thus, security risks in an IoT domain may not exactly be drawn from the failure of one specific IoT component, but most often extend to the failure of other IoT components that can be recipients of rippling impacts. This dependency amongst IoT sub-systems and components can

also cause impacts or failures to cascade from one affected system or component onto another; worsening the damaging impacts (Bloomfield *et al.*, 2010; Kotzanikolaou, Theoharidou and Gritzalis, 2013). One way of achieving IoT dependency modelling is through a network-based functionality dimension – analysing how the functionality of one system or component can affect the functionalities of other systems or components (Zhang and Peeta, 2011), explorable on the basis of connectivity and process configurations over multi-layered IoT architecture. Graph theory (Laugé, Hernantes and Sarriegi, 2015; Stergiopoulos *et al.*, 2016) - using vertices and edges; provides a way to simply represent (directly or logically) the dependency of IoT components within and across multiple functionality layers.

6.2 IoT risk impact assessment with a Goal-Oriented Approach

Identifying shared principles for multiple independent cyber risk models is challenging, because risk assessment is not based on shared risk estimation. This can partially be resolved by focusing on the success factors and concentrating on the external dependencies. In this approach, individual risk vertices are considered as representative of a larger complex IoT system. This advocates a top-down, or goal-oriented modelling approach (Petar Radanliev, D. C. De Roure, Nurse, Burnap, *et al.*, 2019; Petar Radanliev, D. De Roure, *et al.*, 2019), where success factors are traversing across multiple isolated models. The paradigm can provide a real-time statistical assessment of cyber risk of all the entities in the model. The dependencies between a dynastic metaphor, such as 'parent', 'child', 'orphan' are explained in the transformational roadmap, can be analysed with computational statistics using a Bayesian analysis engine (Weinberg, no date; Hanson and Cunningham, 1996).

6.3 Micro Mort

Since there is no International IoT Asset Classification (IIoTAC) and no established Key IoT Cyber Risk Factors (KIoTCRF), for the calculations of the new model, we would firstly need to determine the IIoTAC and the KIoTCRF (P. Radanliev, D. De Roure, *et al.*, 2018; Petar Radanliev *et al.*, 2018). After the establishment of IIoTAC and KIoTCRF, the new model could be applied to calculate more precise 'willingness to pay' to reduce IoT cyber risk.

7 Conclusion

This article combines existing literature and performs comparative, empirical and theoretical analysis of common cyber risk assessment approaches and integrates current standards. The findings present a map of the present initiatives, frameworks, methods and models for assessing the impact of cyber risk. Hence, the article advances the efforts of integrating cyber risk standards and governance and offers a better understanding of a holistic impact assessment approach for IoT cyber risk. This enables visualising the interactions among different sets of cyber security assessment criteria and results with a new design criterion specific for cyber risk from the IoT. The visualisation of cyber risk can be used by practitioners and regulators to inform organisations in this space of best practices. The design principles, with the transformational roadmap, can be applied to assess the impact of cyber compromises and to make cyber security recommendations. The findings are relevant to national and international Industry 4.0 networks, specifically for IoT cyber risk planning.

7.1 Limitations and further research

Holistic analysis of all risk assessment approaches was considered beyond the scope of this study. Additional research is required to integrate the knowledge from other studies. The epistemological framework in this article presents a generic approach to guide researchers and practitioners.

Author Contributions: conceptualization, Dr Petar Radanliev, Prof. David De Roure and Dr Jason Nurse; methodology, Dr Petar Radanliev, Prof. Peter Burnap, Miss Eirini Anthi, Dr Uchenna Ani, Miss La'Treall Madox, Mr Omar Santos, and Dr Rafael Mantilla Montalvo; validation, Dr Petar Radanliev, Miss La'Treall Madox, Mr Omar Santos and Dr Rafael Mantilla Montalvo.; formal

analysis, Dr Petar Radanliev and Dr Uchenna Ani.; investigation, Prof. David De Roure and Dr Petar Radanliev; resources, Dr Petar Radanliev and Dr Rafael Mantilla Montalvo.; data curation, Dr Petar Radanliev and Dr La'Treall Madox.; writing—original draft preparation, Dr Petar Radanliev; writing—review and editing, Dr Petar Radanliev; visualization, Dr Petar Radanliev; supervision, Prof.David De Roure and Dr Rafael Mantilla Montalvo; project administration, Dr Petar Radanliev, Prof. David De Roure and Dr Rafael Mantilla Montalvo; funding acquisition, Dr Petar Radanliev and Prof. David De Roure.

Funding: This research was funded 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)].

Acknowledgments: Sincere gratitude to the Fulbright Commission for supporting this project with the Fulbright Visiting Fellowship at MIT.

Conflicts of Interest: The authors declare no conflict of interest.

8 References:

Anderson, R. and Moore, T. (2006) 'The Economics of Information Security', *Science AAAS*, 314(5799), pp. 610–613. Available at: http://science.sciencemag.org/content/314/5799/610.full (Accessed: 2 April 2017).

Axon, L., Alahmadi, B., Nurse, J. R. C., Goldsmith, M. and Creese, S. (2018) '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*. San Diego, CA, USA, pp. 1–12. Available at: https://www.cs.ox.ac.uk/files/9802/2018-USEC-NDSS-aangc-preprint.pdf (Accessed: 13 March 2018).

Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G. and Feldman, L. (2017) *Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies*. Maryland. Available at: https://csrc.nist.gov/CSRC/media/Publications/nistir/8170/draft/documents/nistir8170-draft.pdf (Accessed: 9 March 2018).

Bilal, M. (2017) 'A Review of Internet of Things Architecture , Technologies and Analysis Smartphone-based Attacks Against 3D printers', *arXiv preprint arXiv:1708.04560*, pp. 1–21.

Bloomfield, R., Buzna, L., Popov, P., Salako, K. and Wright, D. (2010) *Stochastic modelling of the effects of interdependencies between critical infrastructure, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Edited by E. Rome and R. Bloomfield. Springer Berlin Heidelberg. doi: 10.1007/978-3-642-14379-3_17.

Carruthers, K. (2016) 'Internet of Things and Beyond: Cyber-Physical Systems - IEEE Internet of Things', *IEEE Internet of Things*. Available at: http://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber-physical-systems.html (Accessed: 11 April 2017).

CMMI (2017) *What Is Capability Maturity Model Integration (CMMI)®? | CMMI Institute*, *CMMI Institute*. Available at: http://cmmiinstitute.com/capability-maturity-model-integration (Accessed: 26 December 2017).

CVSS (2017) *Common Vulnerability Scoring System SIG*, *FIRST.org*. Available at: https://www.first.org/cvss/ (Accessed: 26 December 2017).

Deloitte (2017) *Cyber security: everybody's imperative A guide for the C-suite and boards on guarding against cyber risks*. Ontario. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-cyber-security-everybodys-imperative.pdf (Accessed: 20 January 2018).

DiMase, D., Collier, Z. A., Heffner, K. and Linkov, I. (2015) 'Systems engineering framework for cyber physical security and resilience', *Environment Systems and Decisions*, 35(2), pp. 291–300. doi: 10.1007/s10669-015-9540-y.

Eggenschwiler, J., Agrafiotis, I. and Nurse, J. R. (2016) 'Insider threat response and recovery strategies in financial services firms', *Computer Fraud & Security*. Elsevier Advanced Technology, 2016(11), pp. 12–19. doi: 10.1016/S1361-3723(16)30091-4.

Evans, P. C. and Annunziata, M. (2012) *Industrial Internet: Pushing the Boundaries of Minds and Machines*. General Electric. Available at: https://www.ge.com/docs/chapters/Industrial_Internet.pdf (Accessed: 15 April 2017).

FAIR (2017a) *Quantitative Information Risk Management | The FAIR Institute, Factor Analysis of Information Risk* . Available at: http://www.fairinstitute.org/ (Accessed: 26 December 2017).

FAIR (2017b) *What is a Cyber Value-at-Risk Model?* Available at: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model (Accessed: 26 December 2017).

FIRST (no date) *CVSS v3.0 Specification Document*. Available at: https://www.first.org/cvss/specification-document#8-4-Metrics-Levels (Accessed: 3 October 2017).

Giordano, A., Spezzano, G. and Vinci, A. (2016) 'A Smart Platform for Large-Scale Cyber-Physical Systems', in. Springer International Publishing, pp. 115–134. doi: 10.1007/978-3-319-26869-9_6.

Gordon, L. A. and Loeb, M. P. (2002) 'The economics of information security investment', *ACM Transactions on Information and System Security*. ACM, 5(4), pp. 438–457. doi: 10.1145/581271.581274.

Hanson, K. M. and Cunningham, G. S. (1996) *THE BAYES INFERENCE ENGINE, Maximum Entropy and Bayesian Methods*. Available at: http://kmh-lanl.hansonhub.com/publications/maxent95.pdf (Accessed: 17 April 2018).

IBM (2016) *2016 Cyber Security Intelligence Index infographic for Healthcare*. Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SE912352USEN (Accessed: 20 January 2018).

ISO (2017) *ISO - International Organization for Standardization*. Available at: https://www.iso.org/home.html (Accessed: 26 December 2017).

Koch, R. and Rodosek, G. (2016) *Proceedings of the 15th European Conference on Cyber Warfare and Security : ECCWS 2016 : hosted by Universität der Bundeswehr, Munich, Germany 7-8 July 2016*. Available 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 (Accessed: 3 April 2017).

Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D. (2013) 'Cascading Effects of Common-Cause Failures in Critical Infrastructures', in Butts, J. and Shenoi, S. (eds) *Critical Infrastructure Protection VII*. Series Vol. Berlin Heidelberg: Springer Berlin Heidelberg, pp. 171–182. doi: 10.1007/978-3-642-45330-4_12.

Laugé, A., Hernantes, J. and Sarriegi, J. M. (2015) 'Critical infrastructure dependencies: A holistic, dynamic and quantitative approach', *International Journal of Critical Infrastructure Protection*. Elsevier, 8, pp. 16–23. doi: 10.1016/j.ijcip.2014.12.004.

Leitão, P., Colombo, A. W. and Karnouskos, S. (2016) 'Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges', *Computers in Industry*, 81, pp. 11–25. doi: 10.1016/j.compind.2015.08.004.

Marwedel, P. and Engel, M. (2016) 'Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions', in. Springer International Publishing, pp. 1–30. doi: 10.1007/978-3-319-26869-9_1.

Nicolescu, R., Huth, M., Radanliev, P. and De Roure, D. (2018) 'Mapping the values of IoT', *Journal of Information Technology*. Palgrave Macmillan UK, pp. 1–16. doi: 10.1057/s41265-018-0054-1.

NIST (2017) *Update to Cybersecurity Framework | NIST, National Institute of Standards and Technology, U.S. Department of Commerce*. Available at: https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework (Accessed: 31 March 2018).

Nurse, J., Creese, S. and De Roure, D. (2017) 'Security Risk Assessment in Internet of Things Systems', *IT Professional*, 19(5), pp. 20–26. doi: 10.1109/MITP.2017.3680959.

Nurse, J. R. C., Radanliev, P., Creese, S. and 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. 28 - 29 March 2018 | IET London: Savoy Place: The Institution of Engineering and Technology, pp. 1–9. doi: 10.1049/cp.2018.0001.

Radanliev, P. (2014) *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. doi: ISNI: 0000 0004 5352 6866.

Radanliev, P. (2015a) 'Architectures for Green-Field Supply Chain Integration', *Journal of Supply Chain and Operations Management*. GB, 13(2). Available at: https://www.csupom.com/uploads/1/1/4/8/114895679/2015n5p5.pdf (Accessed: 11 August 2016).

Radanliev, P. (2015b) 'Engineering Design Methodology for Green-Field Supply Chain Architectures Taxonomic Scheme', *Journal of Operations and Supply Chain Management*. GB, 8(2), pp. 52–66. doi: 10.12660/joscmv8n2p52-66.

Radanliev, P. (2015c) 'Green-field Architecture for Sustainable Supply Chain Strategy Formulation', *International Journal of Supply Chain Management*. GB, 4(2), pp. 62–67. Available at: http://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/1060/pdf (Accessed: 11 August 2016).

Radanliev, P. (2016) 'Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration', *Operations and Supply Chain Management: An International Journal*, 9(1). Available at: http://www.journal.oscm-forum.org/journal/abstract/oscm-volume-9-issue-1-2016/supply-chain-systems-architecture-and-engineering-design-green-field-supply-chain-integration (Accessed: 21 July 2017).

Radanliev, P., De Roure, C. D., Nurse, .R.C., Nicolescu, R., Huth, M., Cannady, C., Montalvo, R. M., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. M. (2018) 'Integration of Cyber Security Frameworks, Models and Approaches - Design Principles for the Internet-of-things in Industry 4.0', in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. London: IET, p. 41 (6 pp.)-41 (6 pp.). doi: 10.1049/cp.2018.0041.

Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Maddox, L., Santos, O. and Montalvo, R. M. (2019a) *Cyber risk from IoT technologies in the supply chain – decision support system for the Industry 4.0*. University of Oxford.

Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Maddox, L., Santos, O. and Montalvo, R. M. (2019b) *Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment*. 201903.0080.v1. Oxford: Preprints. doi: 10.13140/RG.2.2.17305.88167.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., Santos, O. and Montalvo, R. M. (2019) *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*. University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. and Burnap, P. (2019a) *Standardisation of cyber risk impact assessment for the Internet of Things (IoT)*. University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. and Burnap, P. (2019b) *The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises*, *Working paper*. University of Oxford.

Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M., Burnap, P., Roure, D. C. De, Nurse, J. R. C., Montalvo, R. M. and Stacy Cannady (2019) *Design principles for cyber risk impact assessment from Internet of Things (IoT)*, *Working paper*. University of Oxford.

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

Radanliev, P., De Roure, D., Nicolescu, R. and Huth, M. (2019) *A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0*, *Working paper*. University of Oxford.

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. and Burnap, P. (2018) 'Future developments in cyber risk assessment for the internet of things', *Computers in Industry*. Elsevier, 102, pp. 14–22. doi: 10.1016/J.COMPIND.2018.08.002.

Radanliev, P., De Roure, D., Nurse, J., Burnap, P. and Mantilla Montalvo, R. (2019) *Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies, Working paper*. University of Oxford. doi: 10.13140/RG.2.2.32975.53921.

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

Radanliev, P., Roure, D. De, Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. and Montalvo, R. M. (2019d) *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*. University of Oxford. doi: 10.13140/RG.2.2.14133.93921.

Radanliev, P., Rowlands, H. and Thomas, A. (2014) 'Supply Chain Paradox: Green-field Architecture for Sustainable Strategy Formulation', in Setchi, R., Howlett, R. J., Naim, M., and Seinz, H. (eds) *Cardiff: Sustainable Design and Manufacturing 2014, Part 2, International Conference*. Cardiff: Future Technology Press, pp. 839–850.

RiskLens (2017) *Risk Analytics Platform | FAIR Platform Management*. Available at: https://www.risklens.com/platform (Accessed: 26 December 2017).

Rodewald, G. and Gus (2005) 'Aligning information security investments with a firm's risk tolerance', in *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05*. New York, New York, USA: ACM Press, p. 139. doi: 10.1145/1107622.1107654.

Roumani, M. A., Fung, C. C., Rai, S. and Xie, H. (2016) 'Value Analysis of Cyber Security Based on Attack Types', *ITMSOC Transactions on Innovation & Business Engineering*, 01, pp. 34–39. Available at: http://www.itmsoc.org (Accessed: 4 April 2017).

Ruan, K. (2017) 'Introducing cybernomics: A unifying economic framework for measuring cyber risk', *Computers & Security*, 65, pp. 77–89. doi: 10.1016/j.cose.2016.10.009.

Sangiovanni-Vincentelli, A., Damm, W. and Passerone, R. (2012) 'Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems * g', *European Journal of Control*, 18, pp. 217–238. doi: 10.3166/EJC.18.217–238.

Shaw, R., Takanti, V., Zullo, T., Director, M. and Llc, E. (2017) *Best Practices in Cyber Supply Chain Risk Management Boeing and Exostar Cyber Security Supply Chain Risk Management Interviews*. Available at: https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf (Accessed: 9 March 2018).

Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G. and Gritzalis, D. (2016) 'Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures', *International Journal of Critical Infrastructure Protection*. Elsevier, 12, pp. 46–60. doi: 10.1016/j.ijcip.2015.12.002.

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., Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., T. and R.J., Westbury, P. S. (2018) *Internet of Things realising the potential of a trusted smart world*. London. Available at: www.raeng.org.uk/internetofthings (Accessed: 31 March 2018).

Wang, L., Törngren, M. and Onori, M. (2015) 'Current status and advancement of cyber-physical systems in manufacturing', *Journal of Manufacturing Systems*, 37, pp. 517–527. doi: 10.1016/j.jmsy.2015.04.008.

Weinberg, M. D. (no date) 'Computational statistics using the Bayesian Inference Engine', *Monthly Notices of the*

Royal Astronomical Society. Oxford University Press, 434(2), pp. 1736–1755. doi: 10.1093/mnras/stt1132.

World Economic Forum (2015) *Partnering for Cyber Resilience Towards the Quantification of Cyber Threats*. Geneva. Available at: http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf (Accessed: 4 April 2017).

Zhang, P. and Peeta, S. (2011) 'A generalized modeling framework to analyze interdependencies among infrastructure systems', *Transportation Research Part B: Methodological*, 45(3), pp. 553–579. doi: 10.1016/j.trb.2010.10.001.