Future developments in cyber risk assessment for the internet of things

Petar Radanliev and David De Roure and Razvan Nicolescu and Michael Huth and Rafael Mantilla Montalvo and Stacy Cannady and Peter Burnap

Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford,, Imperial College London, Cisco Research Centre, Research Triangle Park, USA, School of Computer Science and Informatics, Cardiff University, United Kingdom

September 2018

FUTURE DEVELOPMENTS IN CYBER RISK ASSESSMENT FOR THE INTERNET OF THINGS

Petar Radanliev*, David Charles De Roure*, Razvan Nicolescu, Michael Huth ♣, Rafael Mantilla Montalvo†, Stacy Cannady†, Peter Burnap♠

*Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, petar.radanliev@oerc.ox.ac.uk; david.deroure@oerc.ox.ac.uk; , ♣ Imperial College London, UK, r.nicolescu@imperial.ac.uk, m.huth@imperial.ac.uk; †Cisco Research Centre, Research Triangle Park, USA, montalvo@cisco.com; scannady@cisco.com; ♠ School of Computer Science and Informatics, Cardiff University, p.burnap@cs.cardiff.ac.uk

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

This article is focused on the economic impact assessment of Internet of Things (IoT) and its associated cyber risks vectors. We report the results of an empirical study that correlates cyber risk impact assessment approaches with academic literature and IoT risks vertices. We adapt the Cyber Value at Risk model and the MicroMort for cyber risk assessment of IoT risks vertices. From the findings, we build a new impact assessment model for the IoT cyber risk. We therefore advance the efforts of integrating cyber risk impact assessment standards and offer a better understanding of economics impact assessment of cyber risk.

Keywords: IoT Cyber Risk; IoT risk analysis; IoT cyber insurance; IoT MicroMort; Cyber Value-at-Risk.

1 Introduction

The IoT term was created in 1999 (Ashton 2011) and the first IoT principles were published shortly after in the book 'When Things Start to Think' (Gershenfeld 1999). According to Gartner's IT Hype Cycle, the IoT market adoption should take 5-10 years, as of 2012 (Gubbi et al. 2013). The increased adoption of the IoT represents multiple categories of cyber-physical systems (Orojloo and Azgomi 2017), integrating technologies related to smart grids, smart homes, intelligent transportation, manufacturing and supply chain and smart cities, to name a few. Such new technologies come with new types of risks that existing risk assessment/management methods are not designed to anticipate or predict. Safeguarding an IoT deployment, while simultaneously harnessing its economic value, requires systematic consideration of multiple risk factors. Cyber-attacks are increasing in frequency, and the and increasingly target IoT devices (for example the Mirai botnet). The severity of future attacks could be much greater than what has been observed to date.

A critical question for government policy and for private sector business strategies for IoT connected products, platforms and services is the sufficiency of cyber security to minimise cyber risk that accompanies IoT deployments. This answer must be partially addressed by economic analysis, such as cost and frequency analysis of cyber-attacks (P. Radanliev, De Roure, Cannady, et al. 2018). Such analysis would complement the process of building frameworks and methodologies for mitigating the economic impact of cyber risk of commercial use of deployments of IoT connected products and services (P. Radanliev, De Roure, Nurse, et al. 2018).

The research methodology in this article proposes adopting the Cyber Value at Risk (CyVaR) and the MicroMort (MM), and evaluating other cyber risk assessment approaches, to build a new model for calculating the economic impact of IoT cyber risk. There is a limited research on the economic impact of cyber risk. There is even less research on the economic impact

related to cyber risks from different IoT verticals. The economic impact of IoT related cyber risks in present time are assessed by applying methodologies established before the development of IoT verticals (ex. automated, digital, social machines, cyber-physical and coupled systems). Present day critical infrastructure systems are far more complex, creating new risks for failures. Further, risk in an IoT deployment might extend to many entities. An interruption in services delivered by a smart grid or smart city would impact many businesses, agencies and individuals. For example, failure in MY IoT deployment might cost millions due to interrupted services. This creates the rationale that a new impact model and assessment methodology are needed that would anticipate economic impact of cyber risks and benefits from the IoT ecosystem. This research would build upon existing cyber risk models (e.g. VaR, Cyber VaR). The research aim is to develop a robust economic model to estimate the economic impact in IoT verticals (ex. communications network, or critical infrastructure).

2 Literature review

The literature review is probing the essence of impact measurements and sources of probabilistic data of cyber risk impact assessment methods. Taxonomic classification is applied for identifying and grouping impact measurement units into an intuitive scheme and to categorise IoT cyber risk vertices.

2.1 Cyber risk impact assessment

The IoT security enables a trustworthy IoT (Yan, Zhang, and Vasilakos 2014; Sicari et al. 2013) with minimal human intervention (Ashraf and Habaebi 2015). Such autonomous IoT, requires a risk-based adaptive assessment framework (J. R. C. Nurse et al. 2018) for risk analysis (Abie and Balasingham 2012; Balasingham et al. 2012). Risk-based adaptive assessment involves ability to predict problems; ability to predict impact; ability to

implement planned actions, ability to maintain focus on risk mitigation, and ability to reduce risk exposure (Abie and Balasingham 2012). Since cyber risk is constantly changing, the risk has not been clearly quantified through historical measures (DiMase et al. 2015). The common figure stated is a loss of $1 trillion to cybercrime, but estimates range from: 300bn and $1tn (Biener, Eling, and Wirfs 2014), $400bn to over $575bn (DiMase et al. 2015), or $400bn to over $2tn (Shackelford 2016). The difference in these figures shows that the numbers are rough estimates at best, and the real economic impact of cyber risk remains unknown (Shackelford 2016). The main difficulties in calculating the economic impact of cyber risk are the lack of suitable data and the lack of universal standardised framework to assess cyber risk (Koch and Rodosek 2016). Adding to these, there is the need to quantify accumulated risk on a shared technology platform (such as cloud computing) and the digital supply chain (Ruan 2017).

2.2 Economic Impact from the Internet of Things

The world is experiencing the fourth industrial revolution (Rajkumar et al. 2010; Wahlster et al. 2013; Jazdi 2014), where the IoT real-time enabled platforms (Marwedel and Engel 2016) represents the foundation for digital industry (Wahlster et al. 2013; Carruthers 2016). Digital industry would be supported with more intelligent, resilient and interconnected manufacturing equipment (Lee, Bagheri, and Kao 2015; Leitão, Colombo, and Karnouskos 2016; Marwedel and Engel 2016). The integration of artificial intelligence and machine learning (Francalanza, Borg, and Constantinescu 2017), the cloud (Babiceanu and Seker 2016) and IoT has created systems of machines capable of interacting with humans (Carruthers 2016; Marwedel and Engel 2016). The application of behavioural economics into these systems of machines (Leonard 2008) already enables market speculation on human behaviour (Rutter 2015) and even neuromarketing (Lewis and Brigder 2004) to determine

consumer purchasing behaviour. We can expect to see autonomous machines adopting to predetermine human behaviour (Carruthers 2016).

Technologies that would enable the integration of IoT in the digital industry include software defined networks (Kirkpatrick 2013) and software defined storage (Ouyang et al. 2014). The IoT and industrial integration are built upon cloud hosting (Carruthers 2016), automation (Leitão, Colombo, and Karnouskos 2016), robots and artificial intelligence (Khalid et al. 2018), machine learning (Kambatla et al. 2014) and mesh networks (Wark et al. 2007). The IoT creates security and risk management vulnerabilities from integrating less secured or unsecured systems, triggering liability for breaches or damages (Carruthers 2016).

IoT is essential for future economic competitiveness, but technological innovations are necessary for harnessing the economic value (Leitão, Colombo, and Karnouskos 2016; Biennier and Favrel 2005; Nicolescu et al. 2018b)**.** Maximising the economic impact of IoT requires energy-aware buildings and cities (Rajkumar et al. 2010; Marwedel and Engel 2016)**,** with preventive maintenance and self-correcting systems (Rajkumar et al. 2010; Leitão, Colombo, and Karnouskos 2016). On the other hand, the electric power grid represents one of the largest complex interconnected networks (Leitão, Colombo, and Karnouskos 2016), and under stressed conditions, even a single failure can trigger complex cascading effects, creating wide-spread failure and blackouts (Rajkumar et al. 2010). Distributed energy resource technologies such as wind power, create additional stress and vulnerabilities (Rajkumar et al. 2010; Leitão, Colombo, and Karnouskos 2016; Marwedel and Engel 2016).

In terms of data ownership, data privacy and Economic lifespan of digital assets, it has already been established that digital assets can outlive humans (Ruffle et al. 2014), triggering the question of data ownership after end of data owners' life. Some studies have simplified the topic with the assumption of a limited economic lifespans for all classes of digital assets (Ruan 2017). The literature reviewed is organised in a taxonomic classification of cyber risk

assessment requirements in Table 1. The categorisation follows recommendations from earlier literature (J. Nurse, Creese, and De Roure 2017) and separates IoT cyber risk assessment requirements into (1) risk identification assessment strategy, (2) risk estimation strategy, and (3) risk prioritisation strategy.

Taxonomic classification of IoT cyber risk assessment requirements	
Risk identification assessment strategy	Identification assessment strategy should cover: espionage, theft, or terrorist attacks, which in effect requires electronic and physical security (Rajkumar et al. 2010; Leitão, Colombo, and Karnouskos 2016), to anticipate and mitigate any risks (Penas et al. 2017). Risk identification should be supported with forensics, prognostics, and recovery plans, for analysis of cyber-attacks and for coordination with agencies responsible to identify external cyber-attack vectors (DiMase et al. 2015).
Risk estimation strategy	A cyber risk estimation strategy should cover information assurance, data security and protection for data in transit, from physical and electronic domains and storage facilities (Longstaff and Haimes 2002; DiMase et al. 2015; Marwedel and Engel 2016). A cyber risk estimation strategy also requires supply chain risk analysis of components introduced in the supply chain (Hofmann and Rüsch 2017), modified from its original design to enable a disruption or an unauthorised function (Evans and Annunziata 2012; DiMase et al. 2015).
Risk prioritisation strategy	Risk prioritisation strategy should limit the source code access to crucial personal provides software assurance and application security is necessary for eliminating deliberate flaws and vulnerabilities (Rajkumar et al. 2010). To prevent continuation of cyber-attacks, risk prioritisation should focus on information sharing and reporting, fast cyber-attack reporting and shared database resources should also be developed (Wahlster et al. 2013; DiMase et al. 2015).

Table 1: Taxonomic classification of cyber risk assessment requirements

The IoT creates new types of cyber risk which are not anticipated or considered in existing cyber risk assessment standards (J. Nurse, Creese, and De Roure 2017). To adapt the current cyber security models, firstly the specific IoT cyber risk vertices are identified in Table 1. By risk vertices, we refer to IoT attack vectors from particular approach used, to exploit IoT vulnerabilities. Subsequently, these specific risk vertices need to be integrated in a holistic

cyber risk impact assessment model, because IoT technologies have already been integrated into traditional computer networks. Integrating IoT technology in the communications networks of critical infrastructure implies major ethical aspects that humans should be able to sense and understand, while benefiting of maximum possible levels of trust and privacy. This concern is represented by the needs that different IoT risk vertices have to be integrated in reliable cyber security frameworks; such would prevent abuse from malicious interventions, including those originated by organised crime, terror organisations or state-sponsored aggressors. Analysis of the complete economic impact of data compromise would empower the communications network providers to create clear, rigorous, industry-accepted mechanisms to measure, control, analyse, distribute and manage critical data needed to develop, deploy and operate cost-effective cyber security for critical infrastructure.

3 Research methodology

This section outlines the research methodology applied in the research. The methodology starts with a literature review to create a taxonomical categorisation of impact assessment classes. Then the complexities of designing a new impact assessment model are discussed through SWOT analysis of the existing frameworks, methods and models. Finally, a new quantitative model is developed, by adopting the Cyber Value-at-Risk (CyVaR) and MicroMort (MM) for impact assessment of IoT cyber risk.

The CyVaR model has been promoted for standardisation of language, models and methods (World Economic Forum 2015). This model attempts to understand the economic impact of cyber risk for individual organisations (Koch and Rodosek 2016). Building upon the CyVaR, a unifying economic framework proposed measurement units for cyber risk (Ruan 2017). Other cyber value analysis methods have advanced to calculate the cost of different cyber-attack types (Roumani et al. 2016), but the same problem with lack of data to validate the model persists. This lack of data has motivated the development of a proof of concept method

(Koch and Rodosek 2016) that is based on data assumptions. The weakness in this approach is that economic impact is calculated on organisations' 'stand-alone' cyber risk, because data assumptions can only be made on individual cases. However, Business impact for the same risk can vary widely between companies based on the specific circumstances of each company. Furthermore, that approach ignores the correlation effect of organisations sharing infrastructure and information, and by default, sharing cyber risk exposure. Cyber risk exists in multiple physical, information, cognitive, and social domains, (software, hardware, firmware, adjacent systems, energy supplies, supply chains) and the economic impact is related to these closely interconnected systems. This close interconnection of disparate systems increases the probability of 'cascading impacts' (DiMase et al. 2015). This article applied multidisciplinary methodologies, along with established risk measurement methods e.g. MicroMort (MM) to define individual risk units and Value-at-Risk (VaR) for measuring market cyber risk

4 Strengths, weaknesses, opportunities and threats (SWOT) analysis of Cyber Risk Frameworks, methods, systems and models

Earlier literature suggested methods based on Return on Investment (ROI) and Net Present Value (NPV), have been proposed to assess the information security investment, that include broad set of criteria, including 'economics of privacy' (Anderson and Moore 2006), 'optimal amount to invest' (Gordon and Loeb 2002), 'risk averseness' (Rodewald and Gus 2005), but these methods are not validated with real data. In addition, cyber risk covers more elements than information security financial cost, and a method is needed that would integrate cyber risk directly with economics (Ruan 2017). Because the motivation for cyber risk can be different than purely financial (ex. espionage), and yet still creating economic impact. Therefore, the impact should be calculated in terms of average and in the most severe scenario (Koch and Rodosek 2016).

To make such calculations with a reasonable precision of the impact assessment, different modelling approaches need to be integrated in a new and more reliable impact assessment model. Such integration is important, because the diversity of approaches for impact assessment, complicates the process of performing cyber risk assessment for the insurance companies. This diversity, found in different frameworks, methods, systems and models, is evaluated with strengths, weaknesses, opportunities and threats (SWOT) analysis in Table 2. The SWOT analysis of the reviewed frameworks, methods, systems and models is summarised in the Table 2.

The strengths	• OCTAVE has developed a standardised questionnaire that can be applied to investigate and categorise recovery impact areas. • TARA is a predictive framework that enables targeting of the most crucial exposures, as opposed to promoting the defence of all possible vulnerabilities. • CVSS is relatively easy to use and translate results. Moreover, it is based on input and feedback from various sources and can be used to translate simple qualitative input into a numerical score reflecting severity and characteristics of a vulnerability. • Exostar System enables enterprises to assess, measure, and mitigate risk in real-time across multi-tier partner and supplier networks and determines the gaps between cybersecurity posture and regulatory compliance. • CMMI combines set of best practices in the disciplines of systems analysis and design, software engineering and management. CMMI can simultaneously address multiple as opposed to stand alone improvements. This enables improvement in the entire enterprise risk and the full product development life cycle risk. • The NIST framework is valuable in assessing cyber risk, but more valuable in managing cyber risks. NIST is also the most advanced framework in terms of disaster and recovery planning. • FAIR model promotes a quantitative, risk based, acceptable level of loss exposure. • ISO promotes standardisation of cyber risk and reflects international experience and knowledge. ISO provides standards for cyber risk and disaster recovery. • RiskLense presents a quantitative assessment with Monte Carlo simulations. • CyVaR presents a method to quantitatively assess risk with Monte Carlo simulations.
The weaknesses	• OCTAVE fails to provide a quantification method for calculating the required level of recovery. • TARA fails to quantify the impact of cyber risks, which is crucial for deciding on appropriate recovery planning.

	• CVSS contains scoring range between 0.0 to 10.0, but is based on a 3-level system and because the score is derived from a limited number of variables, it creates dissimilar vulnerabilities receiving similar score. • Exostar System does not assess enterprises own cyber risk exposure. Instead, it helps enterprises to manage risk by understanding the strengths and vulnerabilities of their supply chain partners. • CMMI does not explain how to implement improvements, but only indicates where improvements are needed. The improvements are not methodological processes and the actual processes an enterprise chooses depend on multiple factors. The CMMI may simply not map the processes in a specific enterprise. • NIST framework is documented, not an automated tool and does not contain an impact assessment model for quantifying cyber risk. • FAIR framework promotes standardisation of quantitative models, but is difficult to use and is not as documented as other frameworks, e.g. OCTAVE. The greatest shortcoming is the lack of access to current information about the methodology and examples of how the methodology is applied. • ISO is based on voluntary shared knowledge and is consensus based. International standardisation requires a level of compulsory compliance. • RiskLense contains a lack of details on the algorithm supporting its risk assessment. • CyVaR has the potential issue of a lack of the required risk data to perform adequate and comprehensive assessments.
The opportunities	• OCTAVE is aimed at companies with limited resources, it is free and can be used as the foundation risk-assessment component or process for other risk methodologies. • TARA is a methodology that can be implemented as a complementary method, in combination with other risk assessment processes. • CVSS currently has a 3-level scoring system, and as such the biggest opportunity is to integrate more levels in the calculator to represent cyber risk with greater precision. Since the numbers are based on experts' opinion and do not represent an ultimate precision, the calculator represents a guiding point. As such, colour coded system with more risk categories could be easier to understand than a number. Numbers may also provide a fake sense of precision, while the numbers in the calculator are not based on established mathematical or statistical probabilistic data. • Exostar System could evolve into a system that assesses enterprises own cyber risk exposure, while enabling the assessment of cyber risk from supply chain partners. • CMMI is related to ISO 9001. The ISO 9001 specifies a minimal acceptable quality level, while CMMI specifies continuous process improvement. Biggest opportunity is to adapt CMMI with continuous updates from ISO 9001 and other standards. • The NIST is based on an extensive use of acronyms, which can be confusing and require a detailed understanding of the standards referred to in the acronyms. Hence, the greatest opportunity would be changing and simplifying the design. This could be done by replacing the acronyms with a new user friendly tool to incorporate a fully automated guidance process (e.g. such as CVSS calculator).

	• FAIR is complementary to existing risk frameworks and applies knowledge from existing quantitative models. This represents an opportunity for developing a standardisation reference architecture. • ISO could evolve into an international standardisation of cyber risk/security frameworks, models and methodologies. • RiskLense could evolve into the first standardised quantitative model for cyber risk assessment. More academic research is required on this model to define and disclose the algorithm. This would increase the acceptance of this model, as academic research would enable the model to be verified and validated. • CyVaR needs to be adapted and modified to include units of measurement for IoT cyber risk vectors.
The threats	• OCTAVE method is complex and takes time to understand. This is the main weakness as it is a qualitative method that does not provide mathematical or financial modelling. • TARA focuses on reducing cost by covering only the exposures that are most likely to occur. Considering that not all exposures are covered, greater focus should be on recovery planning. TARA promotes and facilitates system recovery, but does not address the level of cyber risk impact. • CVSS converting qualitative data into a quantitative result, with relatively low level mathematical approximation, could create a false level of security. • Exostar System uses third-party sources to provide insights in the cyber health and viability of supply chain partners. The validity of the data depends on the third-party sources and if this cyber data is incomplete or compromised, the insights would also be compromised. • CMMI measures are easy to recognise but difficult to develop. For instance, CMMI does not provide guidance on how to implement improvements, it simply indicates where improvements are required. • NIST as a documented model, depends on many documents being continuously updated. Unless it evolves into a more automated process, the framework would need constantly to be reviewed and updated as new technology and laws emerge. • FAIR depends on a computational engine for calculating risk and a model for analysing complex risk scenarios RiskLens (RiskLens 2017). RiskLens (RiskLens 2017) is a commercial product and the software comes at a cost. Standardisation of commercial products could create disadvantages for small enterprises that lack resources of large enterprises. Small enterprises may choose free models such as OCTAVE. • ISO contains members from 161 countries and 778 technical committees and subcommittees. This presents a major challenge in coordination and integration of specific standards. • RiskLense, without the academic peer-review rigour and industry expert review, represents a model that is very difficult to verify and validate. Without such validation, the results would be questionable. • CyVaR is a fairly complicated approach and unless simplified, in a software format, similar to the CVSS, it could be difficult to implement as a standard model for cyber impact risk assessment.

Table 2: SWOT analysis of cyber risk frameworks, methods, systems and models

The SWOT analysis in Table 2 explains multiple issues in building one quantitative model that would rule all of the complexities of cyber risk assessment. Existing cyber risk frameworks and methodologies are constrained by a number of limitations. For instance, cyber risk assessment frameworks are based on security control domains and assess security posture, but are not effective in assessing high risk loss scenarios developed around critical digital assets (Ruan 2017). Furthermore, cyber risk assessment methodologies have created an inconsistency in measuring cyber risk, because of the absence of a common point of reference (Ruan 2017).

There are additional complexities not discussed in the SWOT analysis in Table 2, because they are almost impossible to quantify. For example, in information assets such as intellectual property of digital information, the future value is lost regardless of early detection (Koch and Rodosek 2016). Therefore, the economic value of digital assets has to reflect their economic functions first before their value can be properly assigned (Ruan 2017). In addition, analysing the economic impact of cyber risk is also complicated because of the impact on brand reputation, the cost of downtime, legal liability, cost of intellectual property loss, and many other variables. Merely the media coverage of cyber risk has created such significant economic impact that managing risk has become 'imperative' (Biener, Eling, and Wirfs 2014). The following section, proposes a design of a holistic model for calculating the economic impact of IoT cyber risks.

5 The model

We need a reliable model for costing cybercrime (Armin et al. 2015) and the first step in developing a costing model for IoT cyber risk, is to determine the cybercrime units of costings. To determine the risk of cybercrime, we refer to established methods for calculating risk.

Risk = Likelihood × Consequences, and cyber-risk can be defined as a function of:

$R = \{si, pi, xi\}, i = 1, 2, \ldots, N,$

R – risk; s – the description of a scenario (undesirable event); p – the probability of a scenario; x – the measure of consequences or damage caused by a scenario; N – the number of possible scenarios that may cause damage to a system.

To build a model for calculating the impact of IoT cyber risk, we need to combine established risk models (Ruan 2017), such as MicroMort (MM) and Value-at-Risk (VaR) for measuring market risk and adapt a new cyber risk units for IoT MicroMort (IoTMM) and IoT MicroMort2 (IoTMM2) as the value of reducing the risk by a given IoTMM.

The economic functions of IoT assets requires an International IoT Asset Classification (IIoTAC). The term is chosen to be compliant with the proposed International Digital Asset Classification (IDAC) (Ruan 2017).

IoT digital assets can be categorised as: (1) IoT core value assets (IoTCA), where digital assets which are directly part of goods or services that T profits from; (1a) IoT digitised assets (IoTDA), where goods and services digitised from traditional goods and services; (1b) IoT assets born digital, representing things and services that are intrinsically digital; and (2) IoT operational assets (IoTOA), representing assets that support the creation, consumption and distribution of IoT goods and service.

Thing's (T) IoT composition can be described by the ratio of its core value assets to operational assets: $CA:OA=\{ci,pi\}:\{oj,qj\}$ $i=1,2,\ldots,Nc$, $j=1,2,\ldots,No$ where

IoTCA – T's core value assets; IoTOA – T's operational assets; c – a type of asset listed in IDAC which is of core value to T; p – T's core digital asset c; o – a type of asset listed in IDAC which is of operational value to T; q – T's operational asset o; Nc – the number of core value assets in T; No – the number of operational assets in T.

By using the same formula, T's DA (digitised assets) to AD (assets born digital) ratio can also be calculated. T's digital value composition describes its nature of innovation, e.g.

traditional goods have a high OA:CA ratio, while software has a high CA:OA ratio and a high AD:DA ratio. Other valuation parameters are: Intrinsic value of IoT digital asset can be determined through fundamental analysis without reference to its market value. Market value of IoT digital asset is the price at which the digital valuable would trade in a competitive market. Subjective value of IoT digital asset is determined by the importance the T places on it.

Following these valuation parameters, the value of (1a) IoT assets is directly converted from their physical equivalents. The value of (1b) IoT assets requires their own valuation analyses. (2) IoT assets can be valued with Business Impact Analysis (BIA). According to this formula of the existing economic theory of value to digital asset, the T's total digital value can be calculated as:

$$V = \sum_{i=1}^{Nc} cv_i + \sum_{j=1}^{No} ov_j$$

where:

V – total digital value of T; cv – value of core value asset c of T; ov – value of operational asset o of T; Nc – the number of core value assets in T; No – the number of operational assets in T.

This valuation requires Key IoT Cyber Risk Factors (KIoTCRF) correlated with a T's risk profile. Established Key Cyber Risk Factors (KCRF) risk categorisations (Ruan 2017) can be adopted to IoT, where: Technological factors are related to the usage of technology. Non-technological factors are related to: people, process, socio- economic, geo-political factors. Inherent factors are related to T's nature of business, industry, core operations, goods and services. Control factors represent T's control effectiveness against cyber loss. Therefore, the T's residual cyber risk can be calculated as: Residual cyber risk = inherent risk ÷ control effectiveness. This valuation allows for MM to be applied to define cyber risk units for class D assets and to define IoT MicroMortD (IoTMMD) for a given class D digital assets as 1 in a

million probability of its digital death, where the value of 1 IoTMMD is the amount of money T is willing to pay to reduce 1 IoTMMD for its class D assets.

Since IoT residual risk IoTMM is not statistically available, when it becomes statistically available for various types of IoT assets, it could be aggregated with asset values to generate a cyber VaR curve, representing T's residual cyber risk:

$$VaR = \sum_{i=1}^{n} V_i f_{Di},$$

To compute the cyber VaR curve, historical simulation and Monte Carlo simulation can be used, where VaR is Value-at-Risk for all IoT digital assets of T; T's digital asset inventory D = {D1, D2, ..., Dn}; the value of each asset V = {V1, V2, ..., Vn}; and fDi is the amount of residual risk Di is exposed to, measured in IoTMMD is. Monte Carlo can generate a large number of paths using repeated random sampling to produce a probability distribution. In this scenario, the risk measure IoTMM2 can be defined as a 12-month IoTMM2 VaR representing the loss limit T can afford from cyber incidents. Where IoTMM2 is the cost T is willing to pay to reduce its IoTMM2 by 1% for the same loss limit. The VaR can be calculated for 12 months to represents cyber risk exposure over one financial year, required for budget planning in ERM frameworks.

The proposed valuation depends on advanced data analytics, capable to support a trajectory of exponential growth. We have the advantage of storing and processing large datasets, hence the main obstacle is not the lack of capabilities to compute datasets, but to break down non-technological barriers and establish a wide range of data points in the proposed categories. It may take years or decades to validate the economic impact of IoT cyber risk, because of the time required for data collection. However, it is important to set the categories in order for the data collection to be performed in a structured manner.

6 Applying the proposed model for IoT MicroMort calculations

To test, validate and verify the findings of the new model, (a) the IoTMM for 2017 is calculated; and (b) for 2020 is forecasted, from the following data. There are estimated 378 Million Devices Potentially Vulnerable to Hacking in 2017 out of 8.4 billion connected things (Lipman Paul 2017). These numbers emerged from the BullGuard's IoT Scanner, where 310,000 users scanned their network for vulnerabilities and 4.5 percent (nearly 14,000 devices), were reported as 'could be easily hacked'. This data is combined with Garner report that 8.4 billion connected things will be in use worldwide in 2017 (Meulen 2017). To forecast the IoTMM for 2020, the forecasted data is used from the same report showing that the number of IoT connected devices will reach 20.4 billion by 2020, with more than 900 million potentially vulnerable devices by 2020.

Therefore, (a) the IoTMM for 2017 is calculated as 0.045

and (b) the IoTMM for 2020 is calculated as 0.044

The next step is to calculate the enterprises 'willingness to pay' to reduce 1 IoTMM. This is representative of the cost sum for an enterprise to accept a one-in-a-million IoTMM, or the cost sum that enterprise might be willing to pay to avoid a one-in-a-million chance of IoTMM. For the purposes of testing this model, we could apply a nominal Value of a Statistical Life (VSL) or the Value for Preventing a Fatality (VPF) to evaluate the cost-effectiveness of expenditure on cyber security. The IoT security spending is estimated to increase to $840.5 million in 2020 (Savage 2017). This would IoT market value of 1 IoTMM in 2020 as $840.5. However, it is important to understand what does the value of 1 IoTMM represent in this scenario. We can explain this with an example, e.g. each T in a sample of 100,000 T's willingness to pay for a reduction in their individual IoT risk of 1 in 100,000, or 0.001%, over the next year. Since this reduction in risk would mean that we would expect one fewer IoTMM among the sample of 100,000 T's over the next year on average.

Supposing that the answer was $840.5, then the total dollar amount that the group would be willing to pay to save one statistical life in a year would be $840.5 per T × 100,000 T's, or $84,050,000 million. This is a very generic estimate that cannot be used by governments as guidance point for creating standards and governance. Calculating the IoTMM for 8.4 billion connected things would result with a number far greater than the estimated IoT security spending of $840.5 million in 2020. Unfortunately, we have no data as to how the experts estimated the IoT security spending, and the utility functions in such estimates are often not linear. Therefore, the economic value of 1 IoTMM does not represent a precise calculation of the value and risk. It represents more of a guidance point to show that as more IoT devices become connected, their cyber security is not competitively priced, which increases the risk, and we need to be aware that we have no precise calculation of the IoT cyber risk, or cyber risk in general.

Enterprises can obtain a valuation more precise to their T's by assessing the previously described valuation formula where T's digital asset inventory D = {D1, D2, ..., Dn}; combined with the value of each asset V = {V1, V2, ..., Vn}; and fDi is the amount of residual risk Di is exposed to, measured in IoTMMD is. Resulting with the calculation of the value of 1 IoTMMD in 2020 as the amount of money T is willing to pay to reduce 1 IoTMMD for its class D assets, valued with:

$$V = \sum_{i=1}^{Nc} cv_i + \sum_{j=1}^{No} ov_j$$

7 Analysis of results

The figures we are applying are just to verify the new model. Since there is no International IoT Asset Classification (IIoTAC) and no established Key IoT Cyber Risk Factors (KIoTCRF), the calculations of the new model serve just to verify the new model. After the

establishment of IIoTAC and KIoTCRF, the new model could be applied to calculate more precise ‘willingness to pay’ that T is willing to pay to reduce 1 IoTMMD.

We need to mention that the local linearity of the utility curve means that the MicroMort is useful for small incremental risks and rewards, not necessarily for large risks. Therefore, the IoTMM is not an ideal measure to calculate the IoT risk. Instead, IoTMM is better placed to measure for a given T willingness to pay to reduce 1 IoTMMD for its class D assets.

Finally, we need to discuss the lack of IoT data. For example, the latest forecast from Gartner Inc. says worldwide information security spending will reach $86.4 billion (USD) in 2017 and $93 billion in 2018. That forecast doesn’t cover the IoT, ICS (Industrial Control Systems) and IIoT (Industrial Internet of Things) security (Morgan 2017). Given the lack of data on IoT cyber risk, cyber loss, or profits from different IoT vectors, it is extremely difficult to conduct IoT cyber risk analysis and argue on the soundness of the analysis. Since the cyber insurance is in its infancy, insurance companies have not mastered the valuation of cyber risk in general. For example, Target was insured for $100 millions of cyber risk in 2017, and suffered over $450 millions of loss, with estimated to total at $1 billion by the end of 2017 (Skroupa 2017). This example clearly states that cyber insurance needs a lot more data to calculate, correlated and transfer risk with an acceptable degree of certainty. While general cyber risk cannot be calculated, the emergence of IoT has created new IoT risk verticals that are not at all defined in the cyber insurance policies.

8 Discussion

The research problem investigated in this article was the present lack of standardised methodology that would measure the cost and probabilities of cyber-attacks in specific IoT related verticals (ex. connected spaces or commercial and industrial IoT equipment) and the economic impact (IoT product, service or platform related) of such cyber risk. As a result of the fast growth of the IoT, cyber risk finance and insurance markets are lacking empirical

data to construct actuarial tables. Despite the development of models related to the impact of cyber risk, there is a lack of such models related to specific IoT verticals. Hence, banks and insurers are unable to price IoT cyber risk with the same precision as in traditional insurance lines. Even more concerning, the current macroeconomic costs estimates of cyber-attacks related to IoT products, services and platforms are entirely speculative. The approach by 'early adopters' that IoT products are 'secure by default' is misleading. Even governments advocate security standards ex. standards like ISA 99, or C2M2 (U.S. Department of Energy 2015; U.S. Department of Energy 2014) that accept that the truth on the ground is that IoT devices are unable to secure themselves, so the logical placement of security capability is in the communications network.

The findings from this research lead to the conclusion that there many challenges in understanding the types and nature of cyber risk and their dependencies/interactions in this new space. This article informs on how one may assess economic impact with mathematical formalisms. The mathematical formalisms in the article are focused on IoT risk assessment CyVaR approach that would change the future, not explain the past with historical analysis.

9 Conclusion

The multiple complexities explained in the study, in terms of calculating the economic impact of IoT cyber risk, lead to the conclusion that impact can only be assessed with (1) new risk metrics, and (2) a new valuation method specific for the new risk metrics, combined with (3) new regulatory framework and standardisation IoT data bases with (4) new risk vectors as defined in the form of International IoT Asset Classification (IIoTAC) and Key IoT Cyber Risk Factors (KIoTCRF).

This article presents new risk metrics, by adapting established methods for calculating risks and uncertainties, and identifies some specific grand challenges for calculating the economic impact of IoT cyber risk. The article combined common basic terminology, common

approaches and incorporated existing standards into a new model for calculating the economic impact of IoT cyber risk. The new risk metrics enable measuring the IoT risk, while the risk model enables establishing an acceptable IoT risk level. The adapted CyVaR determines the maximum loss sensitivity and enables adjusting the acceptable IoT risk level, by calculating the risk metrics from new operating conditions.

The new model provides an overall understanding of the design, development, and evolution of IoT cyber risks. The model integrates theories of IoT, control of physical systems, and the interaction between the physical and the digital worlds. (Nicolescu et al. 2018a; P. Radanliev, De Roure, Nurse, et al. 2018; Petar Radanliev, De Roure, Nurse, Montalvo, and Burnap 2019a; Petar Radanliev et al. 2019; Petar Radanliev et al. 2019; Petar Radanliev, De Roure, Nurse, Montalvo, Burnap, et al. 2019; P. Radanliev et al. 2019; Petar Radanliev, De Roure, Nurse, Montalvo, and Burnap 2019b; Petar Radanliev et al. 2019; J. R. C. Nurse et al. 2018; Petar Radanliev 2014; Nicolescu et al. 2018b; Petar Radanliev 2015; Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith et al. 2018; Petar Radanliev et al. 2019; Petar Radanliev, Rowlands, and Thomas 2014; Petar Radanliev et al. 2019; Petar Radanliev et al. 2019; Petar Radanliev, De Roure, Maple, et al. 2019)

10 References

Abie, Habtamu, and Ilangko Balasingham. 2012. “Risk-Based Adaptive Security for Smart IoT in EHealth.” *SeTTIT 2012, September 24-26, Oslo, Norway*. https://pdfs.semanticscholar.org/c39d/04c6f3b84c77ad379d0358bfbe7148ad4fd2.pdf.

Anderson, Ross, and Tyler Moore. 2006. “The Economics of Information Security.” *Science AAAS* 314 (5799): 610–13. http://science.sciencemag.org/content/314/5799/610.full.

Armin, Jart, Bryn Thompson, Davide Ariu, Giorgio Giacinto, Fabio Roli, and Piotr Kijewski. 2015. “2020 Cybercrime Economic Costs: No Measure No Solution.” In *2015 10th*

International Conference on Availability, Reliability and Security, 701–10. IEEE. doi:10.1109/ARES.2015.56.

Ashraf, Qazi Mamoon, and Mohamed Hadi Habaebi. 2015. "Autonomic Schemes for Threat Mitigation in Internet of Things." *Journal of Network and Computer Applications* 49 (March). Academic Press: 112–27. doi:10.1016/J.JNCA.2014.11.011.

Ashton, Kevin. 2011. "In the Real World, Things Matter More than Ideas." *RFID Journal* 22 (7). http://www.rfidjournal.com/articles/pdf?4986.

Babiceanu, Radu F, and Remzi Seker. 2016. "Big Data and Virtualization for Manufacturing Cyber-Physical Systems: A Survey of the Current Status and Future Outlook." *Computers in Industry* 81: 128–37. doi:https://doi.org/10.1016/j.compind.2016.02.004.

Balasingham, Ilangko, J. (Jun'ichi) Suzuki, Tao Gu, Social-Informatics Institute for Computer Sciences, SIGCHI (Group : U.S.), and ACM Digital Library. 2012. *Proceedings of the 7th International Conference on Body Area Networks : 24-26 September 2012, Oslo, Norway : Bodynets 2012*. *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). https://dl.acm.org/citation.cfm?id=2442752.

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. 2014. "Insurability of Cyber Risk 1." *The Geneva Association*. https://www.genevaassociation.org/media/891047/ga2014-if14-biener_elingwirfs.pdf.

Biennier, Frédérique, and Joël Favrel. 2005. "Collaborative Business and Data Privacy: Toward a Cyber-Control?" *Computers in Industry* 56 (4): 361–70. doi:https://doi.org/10.1016/j.compind.2005.01.004.

Carruthers, Kate. 2016. “Internet of Things and Beyond: Cyber-Physical Systems - IEEE Internet of Things.” *IEEE Internet of Things*. http://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber-physical-systems.html.

DiMase, Daniel, Zachary A Collier, Kenneth Heffner, and Igor Linkov. 2015. “Systems Engineering Framework for Cyber Physical Security and Resilience.” *Environment Systems and Decisions* 35 (2): 291–300. doi:10.1007/s10669-015-9540-y.

Evans, Peter C, and Marco Annunziata. 2012. “Industrial Internet: Pushing the Boundaries of Minds and Machines.” General Electric. https://www.ge.com/docs/chapters/Industrial_Internet.pdf.

Francalanza, E, J Borg, and C Constantinescu. 2017. “A Knowledge-Based Tool for Designing Cyber Physical Production Systems.” *Computers in Industry* 84: 39–58. doi:https://doi.org/10.1016/j.compind.2016.08.001.

Gershenfeld, Neil A. 1999. *When Things Start to Think*. New York, NY, USA: Henry Holt. https://books.google.com/books?hl=en&lr=&id=J8GLAwAAQBAJ&oi=fnd&pg=PP2&dq=When+Things+Start+to+Think&ots=8HHfEEuYYh&sig=vSgqQS_0PtX0cH_E_d0uDVTYlCI#v=onepage&q=When Things Start to Think&f=false.

Gordon, Lawrence A., and Martin P. Loeb. 2002. “The Economics of Information Security Investment.” *ACM Transactions on Information and System Security* 5 (4). ACM: 438–57. doi:10.1145/581271.581274.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions.” *Future Generation Computer Systems* 29 (7): 1645–60. doi:10.1016/j.future.2013.01.010.

Hofmann, Erik, and Marco Rüsch. 2017. “Industry 4.0 and the Current Status as Well as Future Prospects on Logistics.” *Computers in Industry* 89: 23–34. doi:10.1016/j.compind.2017.04.002.

Jazdi, N. 2014. “Cyber Physical Systems in the Context of Industry 4.0.” In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, 1–4. IEEE. doi:10.1109/AQTR.2014.6857843.

Kambatla, Karthik, Giorgos Kollias, Vipin Kumar, and Ananth Grama. 2014. “Trends in Big Data Analytics.” *J. Parallel Distrib. Comput* 74: 2561–73. doi:10.1016/j.jpdc.2014.01.003.

Khalid, Azfar, Pierre Kirisci, Zeashan Hameed Khan, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. 2018. “Security Framework for Industrial Collaborative Robotic Cyber-Physical Systems.” *Computers in Industry* 97: 132–45. doi:https://doi.org/10.1016/j.compind.2018.02.009.

Kirkpatrick, Keith. 2013. “Software-Defined Networking.” *Communications of the ACM* 56 (9). ACM: 16. doi:10.1145/2500468.2500473.

Koch, Robert, and Gabi Rodosek. 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*. 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.

Lee, Jay, Behrad Bagheri, and Hung-An Kao. 2015. “A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems.” *Manufacturing Letters*. Vol. 3.

doi:10.1016/j.mfglet.2014.12.001.

Leitão, Paulo, Armando Walter Colombo, and Stamatis Karnouskos. 2016. “Industrial Automation Based on Cyber-Physical Systems Technologies: Prototype Implementations and Challenges.” *Computers in Industry* 81: 11–25. doi:10.1016/j.compind.2015.08.004.

Leonard, Thomas C. 2008. “Richard H. Thaler, Cass R. Sunstein, Nudge: Improving Decisions about Health, Wealth, and Happiness.” *Constitutional Political Economy* 19 (4): 356–60. doi:10.1007/s10602-008-9056-2.

Lewis, David, and Darren Brigder. 2004. “Market Researchers Make Increasing Use of Brain Imaging.” *Advances in Clinical Neuroscience and Rehabilitation* 5 (3): 36–37. http://www.acnr.co.uk/pdfs/volume5issue3/v5i3specfeat.pdf.

Lipman Paul. 2017. “New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking.” https://www.prnewswire.com/news-releases/new-reaper-iot-botnet-leaves-378-million-iot-devices-potentially-vulnerable-to-hacking-300542019.html.

Longstaff, T.A., and Y.Y. Haimes. 2002. “A Holistic Roadmap for Survivable Infrastructure Systems.” *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 32 (2): 260–68. doi:10.1109/TSMCA.2002.1021113.

Marwedel, Peter, and Michael Engel. 2016. “Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions.” In , 1–30. Springer International Publishing. doi:10.1007/978-3-319-26869-9_1.

Meulen, van der Rob. 2017. “Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.” Egham.

https://www.gartner.com/newsroom/id/3598917.

Morgan, Steve. 2017. “Gartner: Worldwide Information Security Spending to Hit $93B in 2018.” https://www.csoonline.com/article/3219165/it-careers/gartner-worldwide-information-security-spending-to-hit-93b-in-2018.html.

Nicolescu, Razvan, Michael Huth, Petar Radanliev, and David De Roure. 2018a. “State of The Art in IoT - Beyond Economic Value.” London. https://iotuk.org.uk/wp-content/uploads/2018/08/State-of-the-Art-in-IoT-–-Beyond-Economic-Value2.pdf.

———. 2018b. “Mapping the Values of IoT.” *Journal of Information Technology*, March. Palgrave Macmillan UK, 1–16. doi:10.1057/s41265-018-0054-1.

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

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

Orojloo, Hamed, and Mohammad Abdollahi Azgomi. 2017. “A Game-Theoretic Approach to Model and Quantify the Security of Cyber-Physical Systems.” *Computers in Industry* 88: 44–57. doi:https://doi.org/10.1016/j.compind.2017.03.007.

Ouyang, Jian, Shiding Lin, Song Jiang, Zhenyu Hou, Yong Wang, Yuanzheng Wang, Jian Ouyang, et al. 2014. “SDF: Software-Defined Flash for Web-Scale Internet Storage Systems.” In *Proceedings of the 19th International Conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS ’14*, 42:471–84. New

York, New York, USA: ACM Press. doi:10.1145/2541940.2541959.

Penas, Olivia, Régis Plateaux, Stanislao Patalano, and Moncef Hammadi. 2017. “Multi-Scale Approach from Mechatronic to Cyber-Physical Systems for the Design of Manufacturing Systems.” *Computers in Industry* 86: 52–69. doi:https://doi.org/10.1016/j.compind.2016.12.001.

Radanliev, P., C.D. De Roure, .R.C. Nurse, R. Nicolescu, M. Huth, C Cannady, R.M. Montalvo, et al. 2018. “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*, 2018:41 (6 pp.)-41 (6 pp.). London: IET. doi:10.1049/cp.2018.0041.

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

Radanliev, P., D. De Roure, R. Nicolescu, and M. Huth. 2019. “A Reference Architecture for Integrating the Industrial Internet of Things in the Industry 4.0.” *Working Paper.* Oxford.

Radanliev, Petar. 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.

———. 2015. “Architectures for Green-Field Supply Chain Integration.” *Journal of Supply Chain and Operations Management* 13 (2). GB.

https://www.csupom.com/uploads/1/1/4/8/114895679/2015n5p5.pdf.

Radanliev, Petar, David Charles De Roure, Jason R.C. Nurse, Pete Burnap, Eirini Anthi, Uchenna Ani, Omar Santos, and Rafael Mantilla Montalvo. 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.* Oxford.

Radanliev, Petar, David Charles De Roure, Jason R.C. Nurse, Rafael Mantilla Montalvo, and Pete Burnap. 2019a. "Standardisation of Cyber Risk Impact Assessment for the Internet of Things (IoT)." *Working Paper.*

———. 2019b. "The Industrial Internet-of-Things in the Industry 4.0 Supply Chains of Small and Medium Sized Enterprises." *Working Paper.* Oxford.

Radanliev, Petar, David Charles De Roure, Jason R.C. Nurse, Rafael Mantilla Montalvo, Pete Burnap, David Charles De Roure, Jason R.C. Nurse, Rafael Mantilla Montalvo, and Stacy Cannady. 2019. "Design Principles for Cyber Risk Impact Assessment from Internet of Things (IoT)." *Working Paper.* Oxford.

Radanliev, Petar, David De Roure, Carsten Maple, Razvan Nicolescu, Jason Nurse, and Uchenna Anie. 2019. "Cyber Risk in IoT Systems." *Journal of Cyber Policy*, 1–27. doi:10.13140/RG.2.2.29652.86404.

Radanliev, Petar, David De Roure, Jason Nurse, Peter Burnap, and Rafael Mantilla Montalvo. 2019. "Methodology for Designing Decision Support Supply Chain Systems for Visualising and Mitigating Cyber Risk from IoT Technologies." *Working Paper.* Oxford.

Radanliev, Petar, Dave De Roure, Jason R.C. Nurse, Razvan Nicolescu, Michael Huth, Stacy

Cannady, and Rafael Mantilla Montalvo. 2019. “Cyber Risk Impact Assessment – Discussion on Assessing the Risk from the IoT to the Digital Economy.” Oxford.

———. 2019. “New Developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – Discussion on Future Developments in the Industrial Internet of Things and Industry 4.0.” Oxford.

Radanliev, Petar, David C. De Roure, Jason R.C. Nurse, Rafael Mantilla Montalvo, and Peter Burnap. 2019. “Supply Chain Design for the Industrial Internet of Things and the Industry 4.0.” Oxford.

Radanliev, Petar, David Charles De Roure, Jason R.C. Nurse, Pete Burnap, Eirini Anthi, Uchenna Ani, La’Treall Maddox, Omar Santos, and Rafael Mantilla Montalvo. 2019. “Cyber Risk from IoT Technologies in the Supply Chain – Discussion on Supply Chains Decision Support System for the Digital Economy.” Oxford.

Radanliev, Petar, Hefin Rowlands, and Andrew Thomas. 2014. “Supply Chain Paradox: Green-Field Architecture for Sustainable Strategy Formulation.” In *Cardiff: Sustainable Design and Manufacturing 2014, Part 2, International Conference*, edited by R. Setchi, R.J. Howlett, M Naim, and H. Seinz, 839–50. Cardiff: Future Technology Press.

Rajkumar, Ragunathan, Insup Lee, Lui Sha, and John Stankovic. 2010. “Cyber-Physical Systems: The Next Computing Revolution.” In *Proceedings of the 47th Design Automation Conference on - DAC ’10*, 731. New York, New York, USA: ACM Press. doi:10.1145/1837274.1837461.

RiskLens. 2017. “Risk Analytics Platform | FAIR Platform Management.” https://www.risklens.com/platform.

Rodewald, Gus, 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*, 139. New York, New York, USA: ACM Press. doi:10.1145/1107622.1107654.

Roumani, Mehrnaz Akbari, Chun Che Fung, Shri Rai, and Hong Xie. 2016. "Value Analysis of Cyber Security Based on Attack Types." *ITMSOC Transactions on Innovation & Business Engineering* 01: 34–39. http://www.itmsoc.org.

Ruan, Keyun. 2017. "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk." *Computers & Security* 65: 77–89. doi:10.1016/j.cose.2016.10.009.

Ruffle, S.J., G. Bowman, F. Caccioli, A.W. Coburn, S. Kelly, B. Leslie, and D Ralph. 2014. "Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe." *Cambridge Risk Framework Series; Centre for Risk Studies, University of Cambridge.* https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/ccrs_cyber_catastrophe_scenario_october_2014.pdf.

Rutter, Tamsin. 2015. "The Rise of Nudge – the Unit Helping Politicians to Fathom Human Behavior." *The Guardian* 7 (23): 2015. https://www.theguardian.com/public-leaders-network/2015/jul/23/rise-nudge-unit-politicians-human-behaviour.

Savage, Ken. 2017. "IoT Devices Are Hacking Your Data & Stealing Your Privacy - Infographic." https://www.pwnieexpress.com/blog/iot-devices-attack-vector-infographic.

Shackelford, Scott J. 2016. "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk." *Chapman Law Review* 19: 412–45.

http://heinonline.org/HOL/Page?handle=hein.journals/chlr19&id=469&div=26&collection=journals.

Sicari, Sabrina, Stephen Hailes, Damla Turgut, Sanaa Sharafeddine, and Uday B. Desai. 2013. "Security, Privacy and Trust Management in the Internet of Things Era – SePriT." *Ad Hoc Networks* 11 (8). Elsevier: 2623–24. doi:10.1016/J.ADHOC.2013.06.006.

Skroupa, Christopher. 2017. "The Cost Of Cyber Breach - How Much Your Company Should Budget." *Forbes*, April 19. https://www.forbes.com/sites/christopherskroupa/2017/04/19/the-cost-of-cyber-breach-how-much-your-company-should-budget/#ad618d6ce746.

Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., H. Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, D. Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, B. Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, A. Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, R. Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, Thompson Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., and P.S. R.J., Westbury. 2018. "Internet of Things Realising the Potential of a Trusted Smart World." London. www.raeng.org.uk/internetofthings.

U.S. Department of Energy. 2014. "Cybersecurity Capability Maturity Model (C2M2) | Department of Energy." Washington, DC. https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity.

———. 2015. "Energy Sector Cybersecurity Framework Implementation Guidance." https://energy.gov/sites/prod/files/2015/01/f19/Energy Sector Cybersecurity Framework Implementation Guidance_FINAL_01-05-15.pdf.

Wahlster, Wolfgang, Johannes Helbig, Ariane Hellinger, M A Veronika Stumpf, Joaquín Blasco, Helen Galloway, and Heilmeyerundsernau Gestaltung. 2013. "Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0." Federal Ministry of Educationand Research. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf.

Wark, Tim, Peter Corke, Pavan Sikka, Lasse Klingbeil, Ying Guo, Chris Crossman, Phil Valencia, Dave Swain, and Greg Bishop-Hurley. 2007. "Transforming Agriculture through Pervasive Wireless Sensor Networks." *IEEE Pervasive Computing* 6 (2): 50–57. doi:10.1109/MPRV.2007.47.

World Economic Forum. 2015. "Partnering for Cyber Resilience Towards the Quantification of Cyber Threats." Geneva. http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. 2014. "A Survey on Trust Management for Internet of Things." *Journal of Network and Computer Applications* 42 (June). Academic Press: 120–34. doi:10.1016/J.JNCA.2014.01.014.