 doi:10.20944/preprints201903.0104.v1

Cyber Risk in IoT Systems

Petar Radanliev[a*], David Charles De Roure[a], Carsten Maple[b], Jason R.C. Nurse[c], Razvan Nicolescu[d], Uchenna Ani[e]

[a]*Department, University, City, Country;* [b]*Department, University, City, Country*

[a]*Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, petar.radanliev@oerc.ox.ac.uk, david.deroure@oerc.ox.ac.uk;* [b]*WMG Cyber Security Centre, University of Warwick, carsten.maple@warwick.ac.uk;* [c]*School of Computing, University of Kent, UK, j.r.c.nurse@kent.ac.uk;* [d]*Imperial College London, UK, r.nicolescu@imperial.ac.uk;* [e]*STEaPP, Faculty of Engineering Science, University College London, u.ani@ucl.ac.uk*

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

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 and the University of North Carolina.

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

 doi:10.20944/preprints201903.0104.v1

Abstract

In this paper we present an understanding of cyber risks in the Internet of Things (IoT), we explain why it is important to understand what IoT cyber risks are and how we can use risk assessment and risk management approaches to deal with these challenges. We introduce the most effective ways of doing Risk assessment and Risk Management of IoT risk. As part of our research, we also developed methodologies to assess and manage risk in this emerging environment. This paper will take you through our research and we will explain: what we mean by the IoT; what we mean by risk and risk in the IoT; why risk assessment and risk management are important; the IoT risk management for incident response and recovery; what open questions on IoT risk assessment and risk management remain.

Keywords: cyber risk; Internet of Things; cyber risk impact assessment; cyber risk estimation; cyber risk insurance

1. Introduction - Defining the Internet of Things (IoT)

The Internet of Things (IoT) represents the idea of networked objects communicating their data which can be controlled across other objects, systems and servers. Communication between objects, networks and humans involves conscious and/or unconscious actions from one IoT agent or device to another IoT agent or device. This differentiates the IoT from the Internet, the automation and the reduction of human input, which is a requirement for the Internet to function. The development of IoT has given us opportunities for social and economic interaction in a wide number of areas such as supply chain management, social media, medicine and energy consumption (for example, smart health devices). IoT provides advanced connectivity that goes beyond machine-to-machine (M2M) communications and applies to a diversity of protocols, domains, and applications. All of this is very exciting, but with new technologies comes new types of risks, and current risk assessment and risk management methods haven't been designed to anticipate or predict what these may be.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

2. Defining what is IoT risk

Risk is all around us, and governments, businesses and individuals engage in risk-based decisions countless times every day. Risk can generally be regarded as the potential for some event to occur, be it positive or negative. For example, let's consider an individual risk like drinking alcohol; we know the negative medical effects and the associated cost to the NHS alcohol consumption has, yet it is considered by many as a positive social event and people continue drinking despite the risks to their health. If we think about businesses, they face strategic, compliance, operational, financial and reputational risks on a regular basis, all of which could affect their profitability or ability to function.

However, this paper is about the IoT and currently, many businesses are looking to adopt new forms of technology (such as the IoT, Blockchain and Artificial Intelligence) to increase the efficiency and effectiveness of their services. This opens them up to the risks that come along with these technologies. While these technologies have the potential to improve their productivity, there is also the potential for the business to be exposed to a series of technical, ethical, security and privacy risks – it is these aspects of IoT that we will focus on in this paper.

To properly understand risk, and by extension risk in the IoT, we need to consider its main components. An organisation's assets form the basis for risk. By assets, we mean something the organisation values, so it could be a product it makes, it could be an app they have developed, or it could be data or information about their customers. From this, we can see that there are many different types of asset, and that the harm or damage to an asset will come in different forms - how this damage or harm could happen can occur in different ways, and we call these threats. Threats are those actions that target assets to cause some negative result (for example, remember the ransomware attacks on the NHS in 2017?); threat events will also have some likelihood or

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

probability of success. Therefore, we think that risk is the probability that a threat event will occur and result in negative impact on or harm of an asset. An IoT-based example of this is the probability of a phishing attack on a connected corporate device occurring, like a company laptop or a smart phone, which then causes several IoT sensors to be infected with malware and consequently the disruption of a manufacturing plant's production line. While there are many application domains for the IoT, such as Connected and Autonomous Vehicles, Health and Well-being, Industry 4.0 and Smart Grid, for organisations to consider cyber security risk solely in the context of their particular domain would give misinformed results, since the IoT is an ecosystem with platforms and services shared by different application domains [1]. In the following table, we explore the main cyber risks that many businesses face. We use the term 'cyber risk' in line with the Institute for Risk Management definition of:

"Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."

https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

Type of Risk	Definition	Key Words	Example
Ethical	An action that falls short of what is considered morally right or outside of a professional standard. So, an ethical risk for an institution is the unintended harm caused by an unethical action.	Integrity, honesty, fraud, moral, standards, compliance, misconduct	Volkswagen develop and install software to cheat diesel emissions tests. This compromises organisation and industry standards and results in massive reputational and financial losses.
Privacy	Most information about people is digitised. Keeping this private and confidential is important. So, a privacy risk is when there is a temporary or permanent loss of control over data that may causes some form of harm to the individual and the business, organisation or government that holds the data.	Trust, transparency, data, confidentiality, cyberattack, hacking, data breach, phishing, pharming, ransomware, spam	In May 2014 145 million eBay customers have their names, addresses, date of birth and passwords accessed. Yahoo was the victim of a massive data breach in 2013-2014. In 2017 they finally admitted that all 3 billion user accounts had been compromised.
Security	This is to do with vulnerabilities and gaps in security programmes and systems. These vulnerabilities	Vulnerability, weakness, protection, attacks,	In October 2016 the Mirai Botnet launched a DDoS attack on DYN which led to parts of the internet

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

	can be exploited in order to gain access to assets causing damage, harm or loss. Types of attack include physical, network, software and encryption attacks.	breaches, DDoS (distributed denial of service), botnets, malware, virus	going down and affected Twitter, Netflix, CNN, Reddit (along with many others) Building management systems were attacked in a Finnish town of Lappeenranta, causing the heating in two buildings to fail.
Technical	The failure of hardware or software due to poor design, construction or evaluation.	Compliance, regulation, testing, evaluation	It was recently discovered that computer chips produced in the last 20 years all contain fundamental security flaws. Depending on the particular flaw variation on the chip, such as Spectre and Meltdown[1].

Table 1: Defining the types of cyber risk from IoT systems

1.1 Defining what is IoT risk assessment

Understanding what is meant by risk is only the first step when we are considering the potential risks in IoT. The next step is to be able to assess the risk, which involves the tasks of; Identifying (or defining) the risk this is the action of developing a clear understanding of what organisational IoT assets are targeted by which threats, and what harm could happen if those attacks are successful.

Estimating the risk; this step aims to measure the IoT risk based on the likelihood of the threat occurring and the impact on the organisation's IoT infrastructure if it does occur. These measures can be qualitative (e.g., ratings using the levels, high, medium and low) or quantitative (e.g., based on mathematical estimations and calculations). Prioritising the risk; once we have a list of the risks and each one has been estimated, the next step is to prioritise the risks. This essentially provides a ranking of the risks based on their estimated levels. We consider these three steps as the best process of IoT risk

[1] See https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html for a further discussion of Spectre and Meltdown.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

assessment. Figure 1, below, sets this out, and also demonstrates that this is a continuous process [2].

Figure 1: The risk assessment process

1.2 Defining what is IoT risk management

Risk management builds on the risk assessment process described above. While risk management techniques are well developed and used in a variety of areas, there remains a significant challenge in managing risk in certain application domains. There are four basic way to handle risk:

- IoT risk mitigation – this involves either reducing the likelihood of the risk happening or reducing the impact of the risk. In IoT risk management, this might include implementing IoT risk controls;
- IoT risk transfer – this involves outsourcing the risk to a third-party. In this instance, via cyber insurance for example;
- IoT risk avoidance – this involves removing the risk. An example would be to remove the IoT asset where the risk has originated; and
- IoT risk acceptance – this involves accepting the risk as it stands, due to either the risk falling within the organisational risk appetite or the aggregated risk being sufficiently within the accepted risk levels.

The type of treatment selected for each risk is based on its estimated level, the costs associated with the treatment, and the organisation's overall tolerance for risk [3]. In the IoT, these factors are constantly changing and therefore, form one of the unique challenges when managing risks in dynamic IoT environments [4].

2 Defining how IoT transform the nature of risk

IoT represents interconnected technologies continuously communicating and sharing data. This technology creates serious safety risks and ethical concerns. For example, IoT devices can outlive humans, so the questions arises; who owns the data on an IoT device if and when the owner dies? Another example might be where smart meter information can be used to see when householders are at home; or if an autonomous car is on a collision course, does it protect the driver or the pedestrian, or a child in the car or child on the road? While the ethical questions triggered by the IoT are intriguing, currently we only have philosophical debates with no real answers, and as stated previously, the focus of this book is the economic impact of IoT cyber risk. In this and following sections, we discuss the related IoT risk assessment approaches that have been used to date, and discuss how we think these approaches can be adapted to assess the impact of IoT cyber risk.

3 Defining how to perform risk assessment for IoT systems

One of the main difficulties of the IoT is that it is developing at a faster rate than other technologies, and governments have not been able to catch up with standards and security regulations. We found that there are, currently, no risk assessment standards to govern companies in assessing the new types of risk before implementing IoT technologies and solutions [5].In the present climate, given the lack of unified global standards and regulations, businesses are pursuing economic profits from IoT solutions,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

but when it gets to understanding the risk to their operations, businesses are often just hoping for the best [6].

3.1 Analysis of cyber risk assessment approaches

As part of our research, we did an analysis of the existing cyber risk assessment approaches [6]–[13] so we could give basic guidance on how to develop a unified approach to risk assessment. In summary, a majority of the cyber security frameworks today apply qualitative approaches to measuring cyber risk (e.g. OCTAVE, TARA, NIST). Quantitative approaches are mostly present in the cyber security models (e.g. Risk Lens).

Name	Author(s) or Institution	What is it	Type
OCTAVE	Caralli, Stevens, Young, & Wilson, 2007	This is a standardised questionnaire that can be applied to investigate and categorise recovery impact areas. However, the OCTAVE method is complex and takes time to understand	Qualitative
TARA	Wynn et al., 2011	This is a predictive framework that enables targeting of the most crucial exposures, as opposed to promoting the defence of all possible vulnerabilities	Qualitative
CVSS (Common Vulnerability Scoring System)	First (2017) https://www.first.org/cvss/	A scoring system "that provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity". It is relatively easy to use and translate results although, the calculator is based on experts' opinion and do not represent an ultimate precision, the calculator represents a guiding point.	Qualitative
Exostar System	Exostar LLC https://www.exostar.com see also Shaw, Takanti, Zullo, 2017	This system enables enterprises to assess, measure, and mitigate risk across multi-tier partner and supplier networks and determines the gaps between cybersecurity posture and regulatory compliance.	Qualitative
Capability Maturity Model Integration (CMMI)	CMMI Institute https://cmmiinstitute.com	This 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.	Qualitative

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

NIST Cybersecurity Framework	National Institute of Standards and Technology (2016) available here: https://www.nist.gov/cyberframework	This is a framework based on an extensive use of acronyms, which can be confusing and require a detailed understanding of the standards referred to in the acronyms. At present, the NIST framework is documented, not an automated tool.	Qualitative
ISO/IEC 27001	International Organization for Standardization https://www.iso.org/home.html	This risk management framework promotes standardisation of cyber risk and reflects international experience and knowledge. It is based on voluntary shared knowledge and is consensus based.	Qualitative
RiskLens	RiskLens https://www.risklens.com	This is a quantitative assessment method based on FAIR (Factor Analysis of Information Risk) and "provides a model for understanding, analyzing and quantifying information risk in financial terms".	Quantitative
CyVaR (Cyber Value at Risk)	Cyberpoint LLC https://www.cyberpointllc.com/cyvar/index.html	This presents a method to quantitatively assess risk with Monte Carlo simulations. CyVaR needs to be adapted and modified to include units of measurement for IoT cyber risk vectors.	Quantitative
FAIR	FAIR Institute https://www.fairinstitute.org	This model promotes a quantitative, risk based, acceptable level of loss exposure.	Quantitative

Table 2: Analysis of cyber risk assessment approaches

3.2 Defining new IoT Risk Assessment approach with Dependency Modelling

Given the diversity of cyber risk assessment approaches, to develop a unified cyber risk assessment approach for IoT risk, we need to start looking at the dependencies. To achieve that, we could apply a so-called dependency modelling approach [14]–[19].

Interactions within IoT can be seen as complex, tightly coupled relationship structures amongst the systems, sub-systems and components. The proper functioning of one or more sub-systems rely to some degree upon another system's proper functionality(ies). Therefore, there is a dependency relationship between them that can either be direct (a first order) or indirect (a higher order) [20]. For example, normal functions for components and services on the application layer (that is, the front end of the IoT

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

architecture, which may be the user interface that displays received information to the user) of the IoT typically depend on the normal functioning of transmission of data (the network layer), and the perception layer (which perceives the physical properties of things). If a service on a perception layer is impaired, it can affect the functioning of the connected service on the network or application layers. This suggests an entire risk landscape that is not about the failure of one specific IoT component, but the failure of other IoT components (devices or services) due to abnormal impacts on a component they depend on. This dependency amongst IoT sub-systems can also cause impacts or failures to cascade from one affected system or component onto another; aggravating the impacts [21].

4 Defining IoT risk management for incident response and recovery

Risk management is a separate process that follows on from risk assessment and is predominately focused on recovery, business continuity, mitigation of risk, and eventually risk acceptance. In the following section, we give an overview of the steps involved in incident response and recovery. We end this section with a discussion of cyber insurance, which represents a method for risk transference for companies.

4.1 Incident Response and Recovery

Incidence response and recovery (IR&R) for IoT typically adopts similar approaches already common to digital and computing systems. Key phases of an incident response and recovery procedure for IoT systems include planning, detection, analysis and response formulation, containment, eradication, recovery, and post-incident activity. The diagram in Figure 2 (below) illustrates this process.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

Figure 2: Security Incident Response Approach

The Planning phase, or Incident Response (IR) Preparation, involves activities that work to make sure that IoT-User organisations are in a state of readiness for the prompt handling of incidents. Example activities include;

(1) Setting and training IoT incident response teams;

(2) Defining appropriate security response and escalation policies;

(3) Forensic evidence management in line with relevant security guidelines and practices;

(4) Awareness and response strategies to common security threats such as Denial of Service, Worms/Trojans, Phishing, web-based and web application attacks, insider threat, exploit kits, information leakage, and identity theft [13], [22].

However, the scope and number of questions that need consideration and answers have only increased in the process of planning for an effective response to IoT security incidents compared to traditional IT systems. For example, let's think about a self-driving vehicle that crashes and kills a pedestrian. The car relies on radar sensors to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

detect obstacles, which evidently can fail, resulting in a crash. This is a complex human-machine system relying on many different systems owned by a variety of enterprises. A good solution path would include viewing IoT incident response considering the mission process of the IoT devices and system. This can support understanding of how malicious actors might exploit the normal infrastructure (device or system) functionality failures and impacts to hide malicious actions. Greater understanding can be achieved through ensuring that security experts responsible for securing the operations of IoT systems clearly understand the threat models that drive the systems [23]. Security experts also need to be conscious and responsive to the dynamic states of the security threats to provide effective response actions [24].

The primary aim of incidence response is to discover and stop security threats and their effects on IT systems and there are several conventional IR methodologies and frameworks that can be adapted for IoT [5], [24]. While it may not be feasible to prevent all security compromises in IoT, effective response and management of threats are needed, which must be built on well-structured and holistic incidence response plans and procedures.

- The Detection phase of IR emphasizes the importance of promptly recognizing the beginning of what is considered a ‘threat’ in an IoT system for which critical decisions and actions are required. Since IoT relies on cloud-hosted infrastructures and often includes limited-functionality devices (from an events and log management perspective), it is necessary to include in the infrastructure monitoring design, a capacity to capture instrumentations data directly from IoT devices, as well as from supporting cloud service providers [23], [25]. IoT devices use trusted credentials for exchanges which when compromised can

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

result in significant vertical and horizontal impacts across the system. Only complex monitoring as described above can provide timely visibility necessary to spur timely decisions and responses. There is an increasingly important and significant role for computational intelligence in supporting risk assessment, through identifying risk, capitalising on opportunities and gaining a deep understanding of a business with reports, dashboards, visualisations and analysis of information [13].

- Traditional security information and event management (SIEM) systems, although powerful and well-advanced for standard networks, are unable to handle the complexities involved in the IoT, where massive numbers of nodes and millions of data are involved, hence the need for newer more tailored IoT-centric systems.
- The Analysis and Response formulation phase focuses on understanding the characteristics of security threats or incidents to learn the most suitable strategy or method for handling future incidents; again, traditional systems struggle and IoT-specific digital forensic and incident response tools are necessary. In the IoT, analysis of threats should consider both system-wide and component-specific perspectives. Using effective threat intelligence tools and processes that relate to the IoT application sector is a good place to start, as threat indicators and protective patterns are often shared and made available on threat intelligence platforms [26], [27]. Examples of threat intelligence tools include:
    a). DHS Automated Indicator Sharing (AIS) which focuses on technology and energy sectors (https://www.us-cert.gov/ais);
    b). Industrial Control System (ICS) ISAC (http://ics-isac.org/blog/home/about/).

 doi:10.20944/preprints201903.0104.v1

From these, further analysis can be explored evaluating the scope of compromise, activities, timelines, and attacker identities related to certain breaches. However, recognition of the potential for attacks to employ anonymity and other anti-forensic capabilities characterised in the IoT domain, is required. Since IoT systems are data intensive, data compromise analysis with respect to confidentiality, integrity, and availability are also crucial. This can be complemented with IoT devices and gateway forensic analysis to provide acceptable proof of the breach of IoT devices and systems.

- The *Containment* phase aims to ensure prompt, interim resolution to a security incident by engaging attempts to restrict further damage to the system. Typical actions in traditional IT systems may include: disabling affected services, disconnecting or swapping out compromised devices and systems with new ones, revising access credential values such as passwords, disabling affected accounts or at worst, initiating a temporary shut-down. However, some of these activities do not happen translate to incidents in IoT systems, not least of all given the crucial importance of not disrupting critical business/mission processes within the system. What is key, is that affected devices, services, or system should be isolated from the operations IoT network as quickly as possible, while allowing for forensic analysis on affected systems.
- The *Eradication* phase leads on from the containment phase and focuses on the long-term removal of threats, and ensures that the system is no longer vulnerable to the threat. Typical activities in this phase include policy updates and independent security audits. This can be achieved in IoT systems through evaluating whether existing security policies can sufficiently address any threats

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

that have been identified; if not, security policy upgrades need to be adopted and implemented. For example, automated software/firmware updates and patching are challenging in today's IoT. It is necessary to devise and adopt policies and approaches for security patching that would provide the necessary security without disrupting operations and functionality. With reference to the need to support forensic analysis, it is desirable to track the activities of a malicious actor in a network. The IoT can benefit from gateway devices that support the establishment of logical rules for automated isolation of compromised infrastructure based on monitored commands or traffic flow patterns without alerting an active attacker on the network. In this way, the attacker's actions and activities can be observed and studied in great detail to inform decisions for necessary security improvements.

- The *Recovery* phase is the process of restoring the system to normal working order. Typical actions may include restoring systems using backups, system re-configurations, or fresh installations. It is necessary to consider these for both cloud and on-premise infrastructure and that restoration is initiated in such a way that it does not cause significant delays or disruptions for the normal operation of the IoT system.
- *Post-Incident Activity* includes a combined process of drawing together lessons from breaches, and reporting these lessons in a structured way that helps to form capability for future occurrences. Typically, this should be conducted through reflective meetings that bring together both senior executives and technical experts [7], [19]. In the reflective reviews, privacy checks, root cause analysis, and after-incident forensics can be performed in relation to the compromised system. Using root cause analysis, organisations can easily understand the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

failure of their security and determine how to strengthen the weaknesses as well as produce true assessments of what happened, how it happened, how well or poor the response went and why, and what a better response may look like in the future [5]. Overall, lessons learned should be evaluated and amended as required including the incident response plan, the network access control (NAC) plan, existing tools and resources to enhance security, deficiencies in cloud service provider's and the on-premise incidence response.

IoT brings inherent cyber risks that span multiple functional sectors with varied degrees of dependencies. Further, IoT systems often operate on platforms that cut across geographical boundaries for which appropriate cyber incident response and recovery plans and strategies are required. Collaborative Incident Response and Recovery (IR&R) utilises shared threat intelligence and should evolve based upon this intelligence. This is required since the security risk landscape is continually evolving so that an incident response plan which was appropriate yesterday might not be today; a plan that seems effective today could also be ineffective tomorrow. Effective IR&R should be characterised by continuous refinements of processes and procedures [1]. This demonstrates a move from a reactive response to the management of security incidents in a way that fosters cooperation through the exchange and sharing of incidence management information among several distinct IoT-adopter organisations. Such an approach should enable both proactive and reactive capacities, and also enforce and assure trust and privacy among IoT infrastructures, and cooperating organisations.

4.2 Discussion on estimation and valuation of Cyber Risk Insurance

Cyber risk insurance represents risk transference and is categorised as a risk management operation. IoT technologies are booming and we can observe cyber risks

 doi:10.20944/preprints201903.0104.v1

worldwide, increasingly impacting physical property and challenging present notions of accountability and liability. In consequence, cyber insurance has often been investigated as a possible market-based solution to the problems of cyber security [4]. However, the cyber insurance market faces challenges in its ability to measure and assess risks and to design and manage cyber risks efficiently. Some of the major problems cyber insurers face is the lack of historical data on risks, a lack of claims data, the volatility of the rather immature IoT technology and markets and the increased scope for cyber security risks. Looking at the broader perspective, governments and the insurance industry are far from a working public-private partnership for cyber insurance [28].

The current model of cyber insurance works as a risk mitigation tool and covers the costs of losses caused by human malicious activity or natural disasters. In this context, many of the problems in the banking and financial sector and their failures of the past decade can be directly tied to model failure or overly optimistic judgments in the setting of assumptions or the parameterisation of a model [1]. Now, a new public policy has emerged in which insurance companies act as clearing houses for information, integrate different security services and provide guidance on appropriate security investments to businesses seeking liability coverage [29]. For example, new and traditional insurers can outsource important parts of the forensic investigation to different consultancies such as software or networking companies. However, recent research shows that this view of cyber insurance as a delegated policy tool has limitations in producing the anticipated coordination benefits and indeed may erode the aggregate level of security investment undertaken by targets in different insurance markets [29].

It should be recognised that the IoT represents a huge opportunity for insurers to harness and understand the right kind of data at the right time. IoT can thus represent a part of the solution to improved coverage and liability of non-tangible digital assets and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

to the dynamic nature of cyber-attacks. IoT can provide a part of response to the general agreement that there is simply not enough data to actually understand the risks and also reduce the resource allocation problems arising from incomplete information regarding parties' actions (moral hazard) and characteristics (adverse selection). However, the analysis and correlation of large IoT data sources and the use of new digital forensics and methods might not be enough sometimes. For example, despite the fact that algorithms used to calculate cyber-risk metrics can analyse and correlate vast amounts of data, the methodologies that inform actuarial models may still struggle to make sense of, and integrate, the real-time information that is available from IoT devices.

Over-reliance on modelling in cyber insurance can also conceal insidious and difficult to detect processes [5], [26], such as in case of the 'normalization of deviance [4]. The normalization of deviance defines the processes that socially organise and systematically reproduce mistakes related to complex technological solutions. In this context, IoT can help by making use data to increase transparency and predictability of such processes, understand the limitations of computational modelling and techniques and improve the assumptions that these models are based on. The constant inspection of granular IoT data and the possibility of sharing aggregates of IoT data and to increase transparency between parties can help insurers and re-insurers to understand strict liability and its sharing across parties across complex ecosystems. Parties can collaborate to prevent risks cascading and to investigate possible "black swan" events (an event that is unprecedented and unpredicted, but on reflection, was bound to happen) in relation to the use of digital devices, which are likely to increase in number, at least in the short term. Formal methods for trustworthiness assessment may then help inform insurance models for complex IoT ecosystems. Such developments would temper the proliferation of false beliefs due to over-reliance on the 'accuracy' of the

 doi:10.20944/preprints201903.0104.v1

outputs from computing models, which can lend an apparent objectivity to the results that can then justify inappropriate actions and policies [30].

From a risk management point of view, one important question is; what architectural improvements of a company's IT system might increase resilience to cyber risk?. We tend to think of cyber security as pertaining to IT companies but, actually, the digitalisation is currently extending well beyond the existing IT systems to manufacturing floors and other production activities where only a few people normally associate with IT. The boundaries between IT systems and manufacturing may not be so obvious. This represents a particular challenge as, in spite of new investments in IoT and broad concerns with cyber risks, the manufacturing industry as a whole is still fragmented in its approach to managing cyber-related risks and in having the organisational ownership to do so effectively [31]. More general risks pertain to the vulnerability that IoT solutions currently have in relation to cyber-attacks and the capability of such solutions to establish and maintain different sorts of rights, such as the right to privacy. The relatively recent DDoS attacks that exploited simple but poorly secured IoT end devices, such as baby monitors with immutable default passwords, show that – on the one hand – the model of low-cost, low-security IoT solutions is not sustainable and that – on the other hand – organisations and individuals need to protect themselves through collaborations, increased transparency, re-drawing of the current accountability and liability domains, and so forth.

From a public policy point of view, it has been argued that insurers became 'de facto regulators' by establishing a minimum-security level to gain cyber coverage [13]. Indeed, there has been research trying to understand the link between security controls and cyber insurance proposal forms [28]. In this context, IoT can help shape public policies that are beneficial for the insurance sector and the society at large. For example,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2019 doi:10.20944/preprints201903.0104.v1

one important opportunity is represented by businesses using IoT to demonstrate their compliance with both national and international industry standards as well as internal policies. The challenges facing organisations in standards compliance for IoT systems are significant [6] However, insurers can design dynamic insurance policies that would not only reflect the changes in behaviour and characteristics of businesses and the contexts in which they operate, but will also allow the creation of insured ecosystems where dynamic mechanisms such as double rewarding mechanisms and adaptive incentives can be operationalized. In such ecosystems, network-specific risks could be transferred between businesses and insurers (or re-insurers) in near real time, e.g. by using smart contracts. These measures can improve some of the current challenges in cyber risk and also contribute to the improvement of existing regulation, public policies and government interventions in the cyber insurance market.

Current developments in the IoT ecosystems allow innovative ways to design cyber insurance services that would utilise IoT data in order to:

- mitigate risk management and facilitate new developments in this area, such as risk engineering;
- increase transparency and predictability of the cyber insurance processes, including near real-time evidence-based explanations meant to increase trust and reduce risks;
- increase the flexibility and adaptability of the current business environments, including the correlation of multi-model information such as risk, anomaly scores and liability;
- investigate the use of Smart Contracts to manage cyber risks within the insured environment.

 doi:10.20944/preprints201903.0104.v1

5 Conclusion

The design of a holistic model for IoT risk assessment and risk management remains a challenge. To design such a model, research should focus on: IoT economic impact, IoT machine ethics, IoT sensor networks, IoT safety, IoT cyber security and IoT equipment combined. Interdisciplinary research such as this would benefit smart city design, intelligent transport design, smart grid design and individual industries and services (e.g. commercial and industrial IoT equipment), by bridging gaps between cyber risk and economic value.

In this paper we have given you an overview of the current research on quantification of IoT cyber risk, with specific new models on this topic, such as the dependency modelling and cyber risk mitigation and transference strategies (e.g. cyber risk insurance). We refer to a number of models and risk assessment articles and technical publications that have emerged recently in the research literature. We believe that this research is useful and important, since currently there are no specific standards to govern the assessment of IoT cyber risk. So, we hope that this paper helps more people to understand and consider the many issues around risk in IoT systems and ultimately, that it can make a contribution to the design of a holistic approach to IoT risk assessment.

6 References

[1] C. Maple, “Security and privacy in the internet of things,” *J. Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017.

[2] J. R. C. Nurse, P. Radanliev, S. Creese, and D. De Roure, “Realities of Risk: ‘If you can’t understand it, you can’t properly assess it!’: The reality of assessing

 doi:10.20944/preprints201903.0104.v1

security risks in Internet of Things systems," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–9.

[3] J. R. C. Nurse and J. E. Sinclair, "Supporting the Comparison of Business-Level Security Requirements within Cross-Enterprise Service Development," Springer, Berlin, Heidelberg, 2009, pp. 61–72.

[4] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "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, vol. 2018, no. CP740, p. 3 (9 pp.)-3 (9 pp.).

[5] P. Radanliev, D. De Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the internet of things," *Comput. Ind.*, vol. 102, pp. 14–22, Nov. 2018.

[6] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "Standardisation of cyber risk impact assessment for the Internet of Things (IoT)," *Work. Pap.*, 2019.

[7] P. Radanliev, D. De Roure, J. Nurse, P. Burnap, and R. Mantilla Montalvo, "Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies," Oxford, 2019.

[8] P. Radanliev, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "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, 2019.

 doi:10.20944/preprints201903.0104.v1

[9] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises," Oxford, 2019.

[10] P. Radanliev, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, "Cyber risk impact assessment – discussion on assessing the risk from the IoT to the digital economy," Oxford, 2019.

[11] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. M. Montalvo, "Cyber risk from IoT technologies in the supply chain – discussion on supply chains decision support system for the digital economy," Oxford, 2019.

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

[13] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Maddox, O. Santos, and R. M. Montalvo, "Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment," Preprints, Oxford, 201903.0080.v1, Mar. 2019.

[14] P. Radanliev, "Architectures for Green-Field Supply Chain Integration," *J. Supply Chain Oper. Manag.*, vol. 13, no. 2, Sep. 2015.

[15] P. Radanliev, H. Rowlands, and A. Thomas, "Supply Chain Paradox: Green-field Architecture for Sustainable Strategy Formulation," in *Cardiff: Sustainable*

 doi:10.20944/preprints201903.0104.v1

Design and Manufacturing 2014, Part 2, International Conference, 2014, pp. 839–850.

[16] P. Radanliev, "Green-field Architecture for Sustainable Supply Chain Strategy Formulation," *Int. J. Supply Chain Manag.*, vol. 4, no. 2, pp. 62–67, Jun. 2015.

[17] P. Radanliev, "A conceptual framework for supply chain systems architecture and integration design based on practice and theory in the North Wales slate mining industry," British Library, 2014.

[18] P. Radanliev, "Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration," *Oper. Supply Chain Manag. An Int. J.*, vol. 9, no. 1, 2016.

[19] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, and P. Burnap, "Supply Chain Design for the Industrial Internet of Things and the Industry 4.0," Oxford, 2019.

[20] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 16–23, 2015.

[21] R. Bloomfield, L. Buzna, P. Popov, K. Salako, and D. Wright, *Stochastic modelling of the effects of interdependencies between critical infrastructure*, vol. 6027 LNCS. Springer Berlin Heidelberg, 2010.

[22] P. Burnap, Y. Cherdantseva, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A Goal-Oriented Approach to Determining and Sharing Risk Data in Distributed Interdependent Systems," *IEEE Comput.*, vol. 50, no. 4, pp. 72–79,

 doi:10.20944/preprints201903.0104.v1

2017.

[23] B. Russell and D. Van Duren, *Practical internet of things security : a practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world*. 2016.

[24] L. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, 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, T. Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., and P. S. R.J., Westbury, "Internet of Things realising the potential of a trusted smart world," London, 2018.

[25] P. Radanliev, D. De Roure, R. Nicolescu, and M. Huth, "A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0," Oxford, 2019.

[26] R. Nicolescu, M. Huth, P. Radanliev, and D. De Roure, "Mapping the values of IoT," *J. Inf. Technol.*, pp. 1–16, Mar. 2018.

[27] R. Nicolescu, M. Huth, P. Radanliev, and D. De Roure, "State of The Art in IoT - Beyond Economic Value," London, 2018.

[28] D. Woods, I. Agrafiotis, J. R. C. Nurse, and S. Creese, "Mapping the coverage of security controls in cyber insurance proposal forms," *J. Internet Serv. Appl.*, vol. 8, no. 1, p. 8, Dec. 2017.

 doi:10.20944/preprints201903.0104.v1

[29] L. Allodi and F. Massacci, “Security Events and Vulnerability Data for Cybersecurity Risk Estimation,” *Risk Anal.*, vol. 37, no. 8, pp. 1606–1627, Aug. 2017.

[30] P. Radanliev, C. D. De Roure, .R.C. Nurse, R. Nicolescu, M. Huth, C. Cannady, R. M. Montalvo, D. De Roure, J. R. C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, “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, vol. 2018, no. CP740, p. 41 (6 pp.)-41 (6 pp.).

[31] J. Buith, “Cyber Value at Risk in the Netherlands,” 2016.