Standardisation of Cyber Risk Impact Assessment For The Internet of Things (IoT)

S.Madhuri[1], N.Vidya[2], Rooma Zainab Ferdouse[3]
[1, 2, 3] Princeton Institute of technology

Abstract- *In this research article, we explore the use of a design process for adapting existing cyber risk assessment standards to allow the calculation of economic impact from IoT cyber risk. The paper presents a new model that includes a design process with new risk assessment vectors, specific for IoT cyber risk. To design new risk assessment vectors for IoT, the study applied a range of methodologies, including literature review, empirical study and comparative study, followed by theoretical analysis and grounded theory. An epistemological framework emerges from applying the constructivist grounded theory methodology to draw on knowledge from existing cyber risk frameworks, models and methodologies. This framework presents the current gaps in cyber risk standards and policies, and defines the design principles of future cyber risk impact assessment. The core contribution of the article therefore, being the presentation of a new model for impact assessment of IoT cyber risk.*

Keywords- Cyber risk; Internet of Things cyber risk; Internet of Things risk vectors; Standardisation of cyber risk assessment; Economic impact assessment.

I. INTRODUCTION

The evolution of IoT represents multiple categories of cyberphysical systems, 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 IoT, while simultaneously harnessing its economic value, requires systematic consideration of multiple factors, including: privacy, ethics, trust, reliability, acceptability and security. Such a systematic approach would go far to ensure the integrity, confidentiality, and availability of the data contained in IoT devices and services. Cyber security has been recognised as a critical national policy issue. by many countries Economic impact of cyber risk and cyber security importance is growing as the integration of IoT connected devices into smart manufacturing and supply, cities, intelligent transport systems, smart grids and more aspects of modern life, including banking, finance, autonomous cars and personal medical devices. 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 minimize cyber risk that accompanies IoT deployments. This answer must be partially addressed by economic analysis, such as cost and frequency analysis of cyber-attacks. 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.

The research problem investigated in this paper is 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, the 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' could be somewhat misleading. Even governments advocate security standards ex. standards like ISA 99, or C2M2 [1], [2] 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 research methodology in this paper proposes combining the Cyber VaR, NIST and FAIR frameworks 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, cyberphysical 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. A interruption in services delivered by a smart grid or smart city would impact many businesses, agencies and individuals.

II. RESEARCH METHODOLOGY

This section outlines the research methodology applied in the research. The section starts with detailing the models applied and adapted. Then the complexities of designing a new impact assessment model are discussed. Finally, the early models are compared with most research modelling approaches to define the rationale for the research methodology applied. Economic impact frameworks and modelsThe Cyber Value-at-Risk (CyVaR) framework has been promoted for standardisation of language, models and methods [43] which has been further developed by Deloitte (2016). This framework represents the first attempt to understand the economic impact of cyber risk for individual organisations [25]

The first unifying economic framework encompassing the cross-disciplinary field of 'Cybernomics' proposed measurement units for cyber risk [26]. Multidisciplinary methodologies are applied, along with established risk measurement methods to define individual risk units: e.g. MicroMort (MM) for measuring medical risk, Value-at-Risk (VaR) for measuring market risk for measuring cyber risk [26]. The main weakness of this framework is that it has not been tested or validated with real data. It has taken years to validate VaR and decades to validate MM due to the time required for data collection. Other cyber value analysis methods have advanced to calculate the cost of different cyber-attack types, 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 [25] 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' [22]. This is of great concern especially in sharing cyber risk in critical infrastructure [25], because critical infrastructure is vital for a strong digital economy [29]. Complexities in building economic impact theoretical model There are multiple problems in building one theoretical model that would rule all of the complexities discussed. There are additional complexities that 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 [25]. Therefore, the economic value of digital assets has to reflect their economic functions first before their value can be properly assigned [26].

Table 1 lists a number of cyber risk management methodologies as used or proposed in industry and academia.
Qualitative Methods

1) The IT Infrastructure Library (ITIL)
2) Control Objectives for Information and
Related Technology (COBIT)
3) ISO/IEC 27005:2011
4) Information Security Forum (ISF) Simplified
Process for Risk Identification (SPRINT)
and Simple to Apply Risk Analysis (SARA)
5) Operational Critical Threat and Vulnerability
Evaluation (OCTAVE)
6) NIST Special Publication 800-53
7) NIST Special Publication 800-37
8) ISO/IEC 31000:2009
9) Consultative, Objective and Bi-functional Risk Analysis (COBRA)
10) Construct a platform for Risk Analysis of Security Critical Systems (CORAS)
11) Business Process: Information Risk Management (BPIRM) Quantitative Methods
12) Information Security Risk Analysis Method (ISRAM)
13) Central computer and Telecommunication Agency Risk Analysis and Management Method (CRAMM)
14) BSI Guide- RuSecure- Based on
15) BS7799 Standard
16) Cost-Of-Risk Analysis (CORA)

Existing cyber risk frameworks and methodologies are constrained by a number of limitations. 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 [26]. Furthermore, cyber risk assessment methodologies have created an inconsistency in measuring cyber risk, because of the absence of a common point of reference [26]. Comparison of early and more recent models on the economic impact of

cyber risk 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' , 'optimal amount to invest' , 'risk averseness' , 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. Because the motivation for cyber risk can be different than purely financial (ex. espionage), and yet still creating economic impact.

III. DISCUSSION

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

IV. CONCLUSION

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 paper informs on how one may assess economic impact with mathematical formalisms. The multiple complexities explained in the study, in terms of calculating the economic impact of IoT cyber risk, also lead to the conclusion that impact can only be assessed with new risk metrics, and a new valuation method specific for the new risk metrics, combined with new regulatory framework and standardisation IoT data bases with new risk vectors as defined in the form of International IoT Asset Classification (IIoTAC) and Key IoT Cyber Risk Factors (KIoTCRF). This paper 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 paper combined common basic terminology, common approaches and incorporated existing standards into a new model for calculating the economic impact of IoT cyber risk**.**

REFERENCES

[1] U.S. Department of Energy, "Energy Sector Cybersecurity Framework Implementation Guidance," 2015.

[2] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2) | Department of Energy," Washington, DC, 2014.

[3] K. Ashton, "In the real world, things matter more than ideas," *RFID J.*, vol. 22, no. 7, 2011.

[4] N. A. Gershenfeld, *When things start to think*. New York, NY, USA: Henry Holt, 1999.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[6] Allen and Hamilton, "Cyber Power Index: Findings and Methodology," McLean, Virginia, 2014.

[7] P. Marwedel and M. Engel, "Cyber-Physical systems: Opportunities, Challenges and (Some) Solutions," Springer International Publishing, 2016, pp. 1–30.

[8] G. Anderson, "The Economic Impact of Technology Infrastructure for Smart Manufacturing," *NIST Econ. Anal. Briefs*, vol. 4, 2016.

[9] 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.).

[10] 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.

[11] 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.

[12] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, O. Santos, and R. M. Montalvo, "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," Oxford, 2019.