RISCS

CYBER RISK QUANTIFICATION RESEARCH PROJECT

Executive Summary

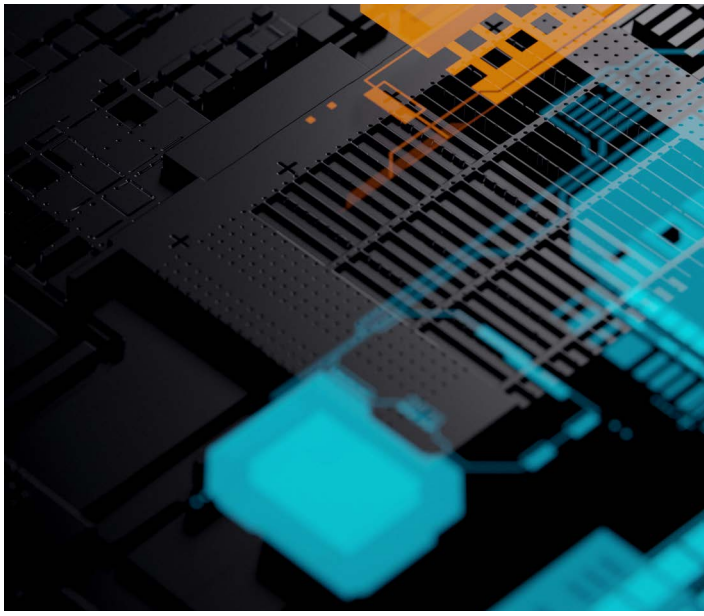
PROJECT TEAM:
Alpesh Bhudia, Anna Cartwright, Edward Cartwright, Frank Cremer, Tom Meurs, Phillip Samson, Jacob Seifert, Darren Shannon, and Barry Sheehan.

VERSION 1.0
05/08/24

OXFORD BROOKES UNIVERSITY
DE MONTFORT UNIVERSITY LEICESTER
UNIVERSITY OF LEICESTER
UNIVERSITY OF LIMERICK OLLSCOIL LUIMNIGH

Executive Summary

Cyber risk quantification provides a means to measure, and subsequently communicate and manage, the risk to an organisation from cyber attack or breach. It is a means to identify optimal investment opportunities and communicate cybersecurity investment returns in ways that are familiar to boards. Our RISCS Cyber Risk Quantification Project provides a comprehensive analysis of the current state of cyber risk quantification. It addresses the methodologies, use cases, and challenges associated with cyber risk quantification, including its application to specific challenge areas and the feasibility of a standardised model for costing cybersecurity incidents. The report offers insights and strategic recommendations for organisations to effectively measure, manage, and communicate cyber risks. Our key findings can be summarized as follows.



The General Risk Cyber Quantification Landscape

1. **There are a large number of cyber risk quantification approaches currently in use:** We identified 137 standards, guidelines, and frameworks and 81 risk assessment methods. It is inevitably hard for organisations to navigate such a complex environment and determine what approach to use.

2. **Quantification approaches differ across several dimensions:** They differ in terms of, e.g. the amount of information needed to inform the quantification process, the complexity of the assessment, and type of output. There is little evidence on the comparative effectiveness of different approaches nor an agreed benchmark for comparing approaches.

3. **Quantification should be responsive to the needs of the organisation:** Cyber risk quantification should be a continuously ongoing process with input from across the organisation including, e.g. finance and HR. Organisations should look to develop in-house expertise to facilitate quantification, even if also using external expertise.

Cyber Risk Quantification in the Context of Specific Challenge Areas

4. **Aggregate Risk:** There is no standardised approach for quantifying cyber risk at an aggregate level for sectors or industries. Aggregate risk can be modelled using either *bottom-up* methodologies, which quantify risk for representative organisations, or *top-down* methodologies, which analyse aggregate-level threats and contagion networks. Approaches need to carefully take account of economic and technological spillovers between organisations as well as correlated risks.

5. **Critical Infrastructure:** Sectors like nuclear, finance, and health require improved cyber risk quantification approaches tailored to their unique risk profiles and threat landscapes. Current risk management expertise in these sectors focuses on component failure from known risks and does not map well to analysing external threats in a rapidly changing environment.

6. **Cost-Benefit Analysis:** Cyber risk quantification can be used to analyse the cost-benefit trade-off of cybersecurity programs. Care, however, should be exercised in using past data to estimate returns to investment. Analysis of the returns to cyber security investment must take account of the threat level an organisation faces and take on board expert input.

7. **Market Dynamics:** The market for cyber risk quantification tools can lead to aggregate risks due to information asymmetry. The market could become dominated by low quality cyber risk quantification tools that promise more than they deliver.

A Standard Method for Costing Cyber Security Incidents

8. **Taxonomy of Harms:** A comprehensive taxonomy of cyber harms, including physical, economic, psychological, reputational, and societal harms, is essential for estimating all the costs of a cyber incident. Reliable taxonomies exist in the academic literature.

9. **Established Methods:** Methods like Monte Carlo simulations are well-established for estimating the costs of a cyber incident. Such methods face challenges due to over-reliance on historical data and capturing only some of the relevant harms (with focus on costs that are more easily measured).

10. **Standard Model Recommendations:** A standard model of cyber costing should be based on a set of core principles that allow for transparency and an accurate estimation of costs:

    a. Define the scope and purpose of the costing exercise.
    b. Ensure transparency and flexibility in assumptions.
    c. Provide clear guidance and ensure reproducibility.
    d. Involve input from across the organisation.
    e. Reflect on the organisation's resource capacity.
    f. Include both tangible and intangible costs.
    g. Recognise the dynamic flow of costs over time.
    h. Use appropriate measures of economic opportunity cost.

Where to Next in Terms of Research?

Future research should look in more detail at the practical implementation of cyber risk quantification within organisations. Ideally comparing different methods and how they evolve over time. Evaluation of implementation will also allow ready identification of data gaps and how they can be filled.

The Data Challenge

Effective cyber risk quantification requires detailed and consistent data. Key challenges include enhancing the diversity and relevance of data sources, standardising data collection and reporting methodologies, and linking security controls with cyber risk outcomes. Often data within an organisation exists but needs to be appropriately fed into the quantification exercise, hence the need for multiple parts of the organisation to be involved in cyber risk quantification.

Conclusion

The RISCS Cyber Risk Quantification Project underscores the importance of a versatile, multi-pronged approach to cyber risk quantification. The adoption of methods must consider organisational context, expert judgment, and quantifiable data to navigate the complexities of cyber risk in an increasingly digital world. The project calls for ongoing research, improved data collection, and developing in-house expertise to enhance cyber risk management.