Research Proposal Outline

James Hines

Transcript for the audio-narrated slide presentation

Slide 1 - Start slide

This presentation outlines the research proposal for the MSc CyberSecurity Capstone Project

Slide 2 - Project Title

The Title of this project is: A Simplified Cyber Risk And Financial Impact Quantification (CRAFIQ) analysis for supporting Cyber defence planning, Decisions and monitoring. Also shortened to **CRAFIQ** analysis during parts of this presentation.

Slide 3 - What is the Research Problem.

As cyber security develops within Small and Medium Enterprises (SMEs), so does the need for cyber risk professionals, who will be able to communicate quantitative findings to help SMEs make decisions while planning for an improvement in their security posture.

Usually, SMEs often **lack the budget and expertise** to have a dedicated Cyber Risk Officer, who is solely responsible for creating quantitative risk analysis to support the CISOs decisions in **planning and implementing** cyber defence measures.

According to a survey carried out by Hubbard & Seiersen (2016), **75 percent** of those working in Cyber security agreed, that a probabilistic approach **should** eventually be implemented in the near future. **However**, the same survey also revealed that 68 percent of those **same** individuals preferred a softer approach to full quantification.

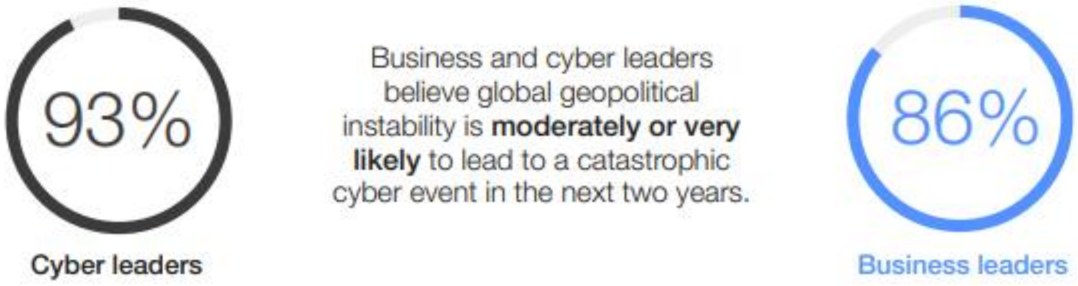
If we take a look at an example of why a softer approach for quantification **may** have been suggested, then being faced with something like this formula below (formula 1.), to apply a risk measure, to cyber security investments, could be daunting for a large majority of individuals.

$$CyRAROC = \frac{\Delta E[L] - I_0 + i * CyVaR(\alpha)}{CyVaR(\alpha)}$$

Formula 1. Source (Orlando, 2021)

Slide 4 - What is the Significance and Contribution to the discipline.

So, what is the significance and contribution to the discipline? Looking at figure 1. According to the world economic forum (2023), 93% of cyber leaders and 86% of business leaders from 151 global organisations, across 32 countries, representing 22 industries had expressed their concerns of geopolitical instability, **leading** to a catastrophic cyber event by **2025**.



Business and cyber leaders believe global geopolitical instability is **moderately or very likely** to lead to a catastrophic cyber event in the next two years.

Figure 1. World economic forum survey. Source WEF (2023).

We should consider that these figures are expressed by **large** businesses who tend to have budgets and expertise to help defend **against** cyber events. But, small and medium businesses are also at a high risk of being hit with a cyber-attack, due to weak controls while also having less resources in place to survive a malicious attack (Allianz Risk Barometer, 2023).

Slide 5

<u>What</u> <u>is then the significance of a simplified CRAFIQ analysis and</u> **<u>How</u>** <u>could it contribute to the discipline?</u>

<u>Slide 6</u>

Let's look at the **What**. If we take a look at Figure 2. , we can see that, Cyber incidents and Business interruption are the two most important business risks selected from a survey with 2,712 respondents. The simplified CRAFIQ analysis can be correlated to those two main risks.

Cyber incidents will fall within the Cyber Risk (CR) section of CRAFIQ and Business interruptions will fall within the Financial Impact (FI) section of CRAFIQ.

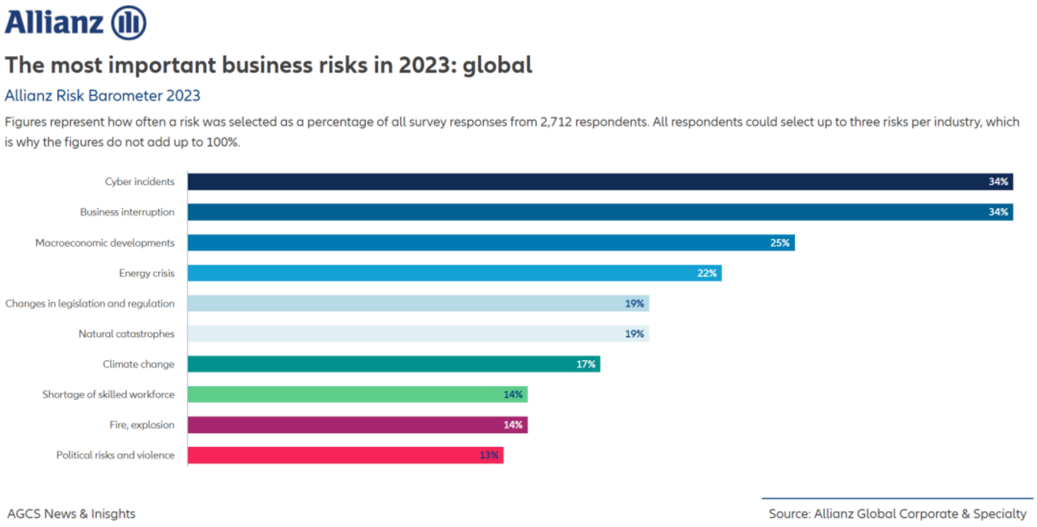


Figure 2. The most important business risks in 2023: Global. Source (Allianz Risk Barometer (2023)

Slide 7

So, if we go back to the **what**. What this analysis will aim to do is to simplify the process of being able to **quantify** financial impact from observing the potential cyber risks in an SME, then present the results in a **format** which is expected at senior and boardroom level, to support cyber defence planning, decisions and monitoring.

This idea of "**simplifying** quantification", is also supported by Strupczewski (2021) who suggests that a **reason** for Cyber risk quantification analysis not being more broadly used is because of its **complexity.**

To get an idea and understand part of the complexity, According to BSI (2017:21) the **interpretation** of statistical results generally involves uncertainties and also **depends** under which framework the statistics had been generated.

That said, to ensure that the analysis can be defended, it is important that the simplified method still utilises threat frequency, loss magnitude and Vulnerability (Freund & Jones, 2015).

Therefore, the hybrid analysis combination consisting of a process such as: a pre-qualitative questionnaire, a simplified CRAFIQ analysis followed by a post-qualitative questionnaire should encapsulate the required information that is relevant for SME's and presented in a clear, relatable and repeatable form.

Slide 8

How could it contribute to the discipline?

By attempting to create a simplified cyber risk and financial impact quantification analysis, that aims, to not **just** provide results in a format which, senior management and boardroom level managers prefer to be presented with, **but**, with a slimmed down, **simplified** version of quantification, then individuals may be more likely to attempt to implement a cyber risk quantification approach.

A simplified version, could also encourage more individuals to adopt a quantitative approach.

It could also be a motivational steppingstone into deeper cyber quantification methods

Slide 9 - The Research Question.

The Research question. Is it possible that:, by performing a **simplified** Cyber risk and financial impact quantification analysis, that it could support Cyber defence planning, decisions and monitoring within an SME?.

Slide 10 - Aims and Objectives

Aims: To develop a 3-phase data collection process by:

1. Firstly, By creating two qualitative questionnaires
    a. Pre-analysis questionnaire
    b. Post-analysis questionnaire

2. Secondly, To create a **simplified** Cyber Risk and Financial Impact (CRAFIQ) Analysis that can be used in a SME

Slide 11

Objectives:

1. Use the pre-analysis questionnaire to:
    a. Discover the current security posture thoughts
    b. Discover their future cybersecurity opinions and mindset
2. Use CRAFIQ analysis to:
    a. Quantify the security posture and risks to an SME
    b. Promote awareness of the status quo
    c. Encourage broader usage of quantifying cyber risk and financial impact
    d. Create a stepping stone for users to move onto deeper quantification methods such as FAIR
3. Use the Post-analysis questionnaire to discover if the CRAFIQ analysis:
    a. Had changed their thoughts on current security posture
    b. Increase support for the planning of improved cyber defence decisions.

The data collected via the 3-phase process will then be analysed and presented in a final report to show any changes in answers between the pre-questionnaire and Post-questionnaire

Slide 12 - Key literature related to the project.

If we first want to understand what cyber risk is, then a good, clear description to begin with has been quoted by Egan et al (2019). Egan et al (2019) stated that “Cyber risk is the risk of any financial loss, disruption or negative reputational impact because of a failure in information technology systems; whether through people, process or technology.”

Traditionally, risk assessments have been carried out in a subjective, qualitative format. Usually assigning a probability value of 1 to 5, where, for example, a value of 1 could represent a “**Not likely**” of something happening and a 5 could mean “Highly likely” that something may happen. This approach can unintentionally be biassed (Esuli et al, 2023), because it's based on feeling. A quantitative approach provides an improved and more accurate calibration of probabilities (Esuli et al , 2023).

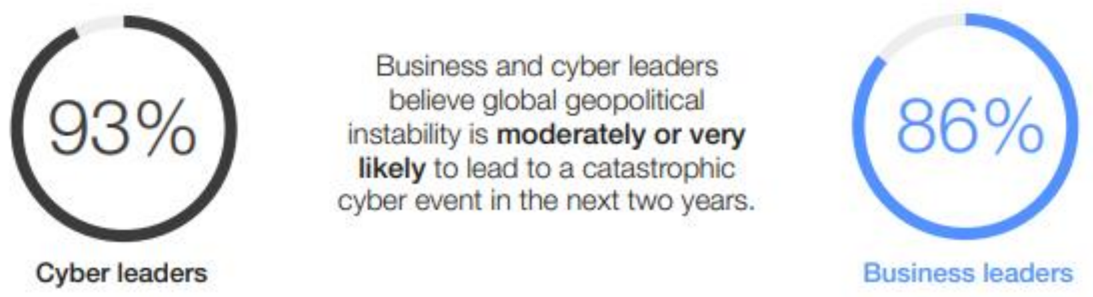
Regarding quantification, although based on mathematical models such as statistical probabilistic models, Bayesian, monte carlo simulations and markov chain analysis, the approach to risk quantification appears dynamic **depending** on **what data** you wish to observe.

An example of a dynamic approach is perception-based quantification, which is a method that can directly model subjectivity of beliefs (Wang, 2018). However, Hubbard & Seierson (2023: 157) state that “very few people are natural calibrated estimators” which is another name for subjective probability assignment, an area of research within decision psychology.

<u>Slide 13</u>

Although Hubbard & Seierson (2023) and Wang (2018) have differing opinions about the abilities of taking subjective values to create quantifiable value, both opinions could still be correct depending, on the end goal, **especially** if we consider the **sequential multi-phase design** and **partially integrated mixed approach,** as explained by Saunders et al, (2019).

Support for the opinion by Wang (2018) is that it is, highly likely that **perception**-based quantification could be an approach for transferring qualitative values from a survey and converting the feedback into a quantitative value, such as in figure 4. Here, 151 organisations answered a survey and the response was then quantified from their belief.



Business and cyber leaders believe global geopolitical instability is **moderately or very likely** to lead to a catastrophic cyber event in the next two years.

Figure 4. World economic forum survey. Source WEF(2023)

Therefore, with this same example given in figure 4, the opinion expressed by Hubbard & Seierson (2023) may also be correct on the basis **that** a large proportion of those who answered this survey may be incorrect, due to **their** individual lack of ability to provide an accurate **calibrated estimation.**

<u>Slide 14</u>

Esuli et al (2023) states that learning to quantify, admits different problems of applicative interest. We have observed how Wang (2018) and Hubbard & Seierson (2023) have opposing opinions but both opinions could still be correct. And the idea that both opinions could be correct is supported by Saunders et al (2019). A possible reason for differing opinion may be partially explained in research by Eusli et al (2023) who attribute quantification problems to various forms of quantification such as single-label quantification (SLQ), Binary quantification (BQ) and regression quantification (RQ) to name a few.

<u>Slide 15 - Methodology</u>

The methodology, of this research, still needs to be defined as part of phase 1 of the proposed activities, but what can be said so far is that:

The collection, usage and analysis of <u>Primary Data</u> will be achieved by creating the following:

<u>Two Qualitative questionnaires</u>, a pre and post questionnaire which will be answered in person:

Possibly, carry out a Narrative Analysis of the answers on the questionnaires and look at performing a descriptive analysis on all of the 3-phase process analysis feedback at the SMEs to observe if a pattern arises as a result of the CRAFIQ analysis.

One Quantitative simplified CRAFIQ Analysis.
Cyber Risk may look at the security posture of **people, processes and technology** which ties into Egan et al (2019) introduction to cyber risk.

The analyses will look at how these three areas could impact business units and what the financial impact for each business unit/entity/department could be.

Slide 16
The 5-Phase methodology will be to perform the pre-questionaire, then the CRAFIQ analysis, Then present CRAFIQ analysis results to the decision makers, carryout the post questionnaire, analyse the 3-phase process documentation and wrap up with a second presentation of the 3-phase process results.

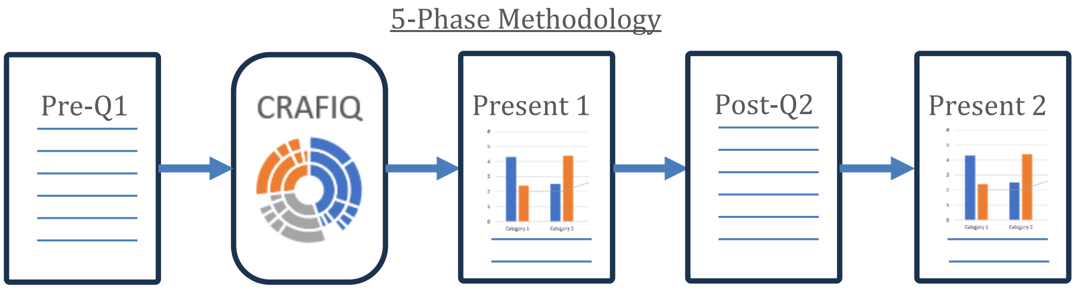


Figure 5. 5-Phase Methodology. Source (Hines, 2023)

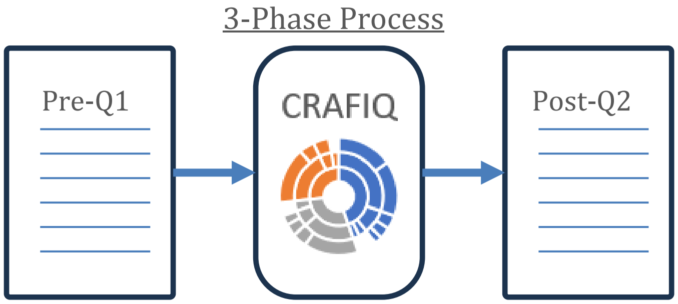


Figure 6. 3-Phase Process of collecting data. Source (Hines, 2023)

Slide 17 - Research Design
The research design will utilise the sequential multi-phase design using mixed methods which allows a dynamic approach (Saunders et al, 2019:182).

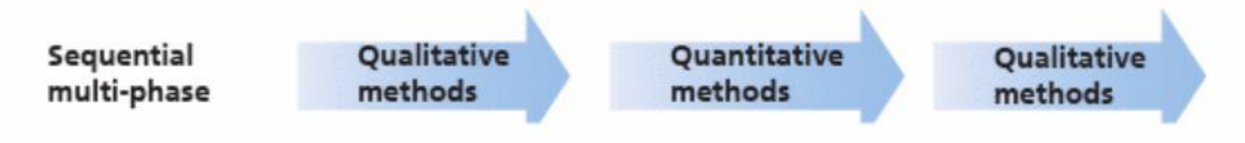


Figure 7. Mixed methods research design. Source (Saunders et al. 2019)

According to Saunders et al (2019:183) using the partially integrated mixed approach allows the researcher to use qualitative and quantitative methods at particular stages of the research. This approach will fit to the 3-phase process described in the methodology slide as well as in the aims and objectives slides.

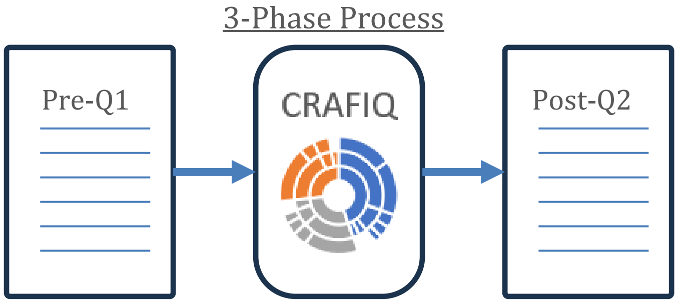


Figure 8. 3-Phase Process of collecting data. Source (Hines, 2023)

Slide 18 - Ethical considerations and risk assessment

Ethical considerations and confidentiality must be a priority from a compliance and legal perspective, but also out of respect.
Personal information of people needs to be protected, maybe assigning anonymous numbering.
An informed consent form should also be created for participants (Dawson, 2015).

Risk Assessment and mitigation should ensure that any information about a business process, systems, security posture and know-how should not be identifiable to a business name or individual who is participating in the research. Also important that care should be taken to not increase the probability of a security incident or breach.

Slide 19 - Timeline of proposed activities ***(Show Timeline)***

This is an “Activity network” Timeline which has been heavily adapted from Dawson (2015:73) and combined with milestone phases.

The weeks have been broken down into sections with the vertical orange lines clearly separating the blocks of weeks.

Phase 1 will have 3 activities running parallel until the end of week 12. Week 13 and 14 will focus on refining and closing the questionnaire design before moving onto establishing CRAFIQ analysis KPIs.

Phase 2 will focus on the testing of the CRAFIQ analysis and fine tuning.

Phase 3 will Implement the 3-phase analysis, followed then, by the analyses of the results from the questionnaires. Finally culminating in the write up to complete the MSc Paper and submission.

Slide 20 - Conclusion

It is worth remembering that this is not about creating a whole new process of cyber risk quantification, but it is about simplifying the analysis as a support tool for decision making. The analysis accumulates in a three phase process, which should indicate if psychological change and opinion has taken place, as a result being exposed to CRAFIQ analysis.

Improving the security posture within businesses, **especially** small and medium businesses could be challenging due to budgets and technical skills shortage. According to Morgan & Sausalito (2022), there were 3.5 million unfilled cybersecurity positions in 2021, an increase of 350% since 2013. Due to such demand and shortage of qualified personnel, it may be difficult to have the expertise for full cyber risk quantification.

With so many differing opinions on cyber risk modelling, **which** approaches to use, and **how** to use the various techniques for carrying out cyber risk quantification, it appears that a simplified, workable, adoptable form of quantification is required, that allows individuals to begin the process and gain confidence to dive deeper into a more specialised cyber quantification method.

Slide 21 - References

Allianz global corporate & specialty (2023) The most important business risks in 2023: global. Available from: https://app.23degrees.io/embed/QhJ7h3aVVhjVJjIP-bar-horizontal-the-most-important-business [Accessed on 18th August 2023]

Allianz Risk Barometer (2023) Cyber Incidents. Available from: https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html [Accessed on 18th August 2023]

BSI. (2017) BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz. *Bundesamt für Sicherheit in der Informationstechnik*. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=908032 [Accessed on 18th August.2023]

Dawson, C. (2015) Projects in computing and information systems: A student's guide. 3ed. Pearson.

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., Dee, A., Bajaj, R., Jaeger, V.-J., Katz, D., Meghen, P., Silley, M., Nasser-Probert, S., Pikinska, J., Rubin, R.

and Ang, K. (2019) Cyber operational risk scenarios for insurance companies British Actuarial Journal. *Cambridge University Press*, 24: e6. DOI: https://doi.org/10.1017/S1357321718000284. [Accessed on 16th August 2023].

Esuli, A., Fabris, A., Moreo, A., Sebastiani, F. (2023). The Case for Quantification. In: Learning to Quantify. *The Information Retrieval Series* 47. Springer. DOI: https://doi.org/10.1007/978-3-031-20467-8_1 [Accessed on 20th August 2023].

Freund, J, & Jones, J. (2015) Measuring and managing information risk: A FAIR approach. Elsevier.

Hubbard, D, & Seierson, R. (2016) How to measure anything in Cybersecurity Risk. John Wiley & Sons

Hubbard, D, & Seierson, R. (2023) How to measure anything in Cybersecurity Risk: 2ed. John Wiley & Sons

ISO. (2023) 27001 standard for Information security management systems. Available from: https://www.iso.org/standard/27001 [Accessed on 19th August 2023]

Morgan, S. & Sausalito, C. (2022) The past, present and future of cyber crime.*Cyber security ventures.* Available from: https://cybersecurityventures.com/cybersecurity-almanac-2022/ [Accessed on 19th August 2023]

Orlando, A., (2021) Cyber risk quantification: Investigating the role of cyber value at risk. *Risks*, *9*(10): 184. Available from: https://www.mdpi.com/2227-9091/9/10/184 [Accessed on 15th August 2023]

Saunders, M., Lewis, P. & Thornhill, A. (2019) Research methods for business students. Pearson education ltd. Available from: https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=5774742&ppg=205 [Accessed on 19th August 2023]

Strupczewski, G. (2021) Defining Cyber Risk. Safety Science 135: DOI https://doi.org/10.1016/j.ssci.2020.105143 [Accessed on 2nd August 2023]

Wang, Y. (2018) Trust Quantification for Networked Cyber-Physical Systems. *IEEE Internet of Things Journa*l. 5(3): 2055-2070. Available from: https://ieeexplore-ieee-org.uniessexlib.idm.oclc.org/document/8329991 [Accessed on 17th August 2023]