RMPP Unit 3 – Seminar 2 Preparation

In this seminar, we will be focusing on LO 3 "Evaluate critically existing literature, research design and methodology for the chosen topic." One way this is done is by conducting a peer review of existing literature on a particular subject.
In preparation for this week's seminar, you will need to source at least 2 papers in a Computing field of your choice that utilise the two different types of research methods to achieve their goal/research aims. Now answer the following questions (please provide justifications for your answers) and be prepared to discuss them in the session:

- *Familiarise yourself with the purpose, problem, objective or research question of each paper. Are they in line with your experience or thoughts on the topic, contributing to the collective body of knowledge in this area?*
- *Is the research methodology utilised in each paper appropriate for the stated purpose or question?*
- *In terms of data collection and analysis, is this also appropriate for the stated purpose or question? (We will discuss this further in upcoming units.)*
- *Does each paper support its claims and conclusions with explicit arguments or evidence?*
- *How would you enhance the work/paper?*

The first paper relates to qualitative methods in cybersecurity research (Fujs et al., 2019) to establish which types of qualitative methods are most used and in conjunction with which topics. As the problem is not clearly defined, exploratory research has been used.

Research in cybersecurity is deemed popular with a large body of research available, however Fujs et al. (2019) there is no study that has provided an insight into which research methods are being commonly used and how. Therefore the paper aims to provide an overview of qualitative methods used and evaluate reporting used on the research methods. The intended audience is aimed at cybersecurity researchers to benefit their practice and gain an adequate level of research.

The general personal assumption would be that quantitative research methods may be more common due to the rigour of data collected and the likelihood of being accessed for further work or publications. However, this paper offers greater breadth and depth by exploring social and behavioural areas in cybersecurity (Fujs et al., 2019) and offering to reason why phishing attempts occur.

The piece offers an overview of methods such as observation, interview, Delphi method, case study, action research and grounded theory. The research was based on a search through bibliographic databases. With this being a literature review, it was useful; however, there were limitations.

Research can be considered slightly dated, and the work covered is only two years' worth of literature. Also, the search queries were limited as 'cybersecurity' is a general

term, and more explicit terminology could have been used to yield more results. Furthermore, the use of only three databases also showed a limitation.

This paper made some valuable findings that researchers can be aware of, such as that data collection and analysis should be more rigorous. Also, topics like secure software development are identified as an area for attention.

The qualitative methods used are interviews, case studies and observations. To enhance this paper, as interviews were the most common method, perhaps research more profoundly into the practice of these and investigate how they may differ depending on the area or level of focus.

The second paper identifies a quantitative research method named CSeCRM Cybersecurity Culture Research Methodology to measure cybersecurity culture (Veiga, 2016). The method aims to be an instrument with meaningful results for researchers to make predictions from the data obtained. Questionnaires were given to employees over three weeks to validate the designed model, and statistical analysis was then conducted.

The literature review was helpful as it assessed the cybersecurity culture. Frameworks within an organisation support reduced risk and the assessment data to target cyber awareness and employee training. The risk of human factors can be minimised, and the assessment can be an annual benchmark to track progress.

However, there is also a limitation in this area, as there is more rigour to the risk of human behaviour and insider threat. Also, as stated by Veiga (2016), including structural equation modelling (SEM) would build more links between the variables considered and make a standardised approach across all the levels (individual, organisational, national and international). To enhance this paper, conducting the research is a broader industry scale as this was solely focused on an international finance organisation.

Fujs, D., Mihelic, A. & Vrhovec, S. (2019). *The power of interpretation: Qualitative methods in cybersecurity research*.

Veiga, A. D. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI Computing Conference (SAI), 13-15 July 2016 2016. 1006-1015.