INDIVIDUAL REFLECTION ASSIGNMENT

Table of Contents

Overview

The purpose of this reflection is to demonstrate what I have learnt from research methods and focus on data analysis. My 14 years in IT security have helped me connect vulnerability assessment and data analysis to security monitoring in practice, and I can relate this research validity to the process. This made me realize errors in methodological rigor, bias minimization, data presentation. From now on, I will leverage research to the benefit of the field of IT security, writing structured reports, cross-checking the progress, and incorporating qualitative findings. This module trained my analytical thinking, making it clear that the proof of concept of evidence-based decision making and methodological precision is essential both within academic research as well as professional cybersecurity. Now, with the help of the Rolfe's Reflective Model, I am going to reflect on my experience.

What?

During this research methods module, I have developed a better and in depth understanding about research validity, generalizability, data analysis and visualization. Units 8 and 9 touched me since they are directly related to my work in Networking and Security for the IT industry. The study of managing routers, switches, firewalls, load balancers, vulnerability management tools, and structured the first dimension of my analytical skills that I found useful in analyzing data and validating research (Karvinen, 2023). While it is not difficult to get involved in these topics while in industry, an engagement from a research, academic perspective gave me a new and structured

approach to problem solving that I have not worked through before in my industry experience.

The discussions of validity and generalizability in Unit 9 brought me to reflect on the manner to which IT security assessments are carried out. To mention an example, in vulnerability management the validity of a test (i.e., that the security threat is real and has reproducible) is imperative. Likewise, this connotes that ensuring internal validity in research implies that while trying to establish a cause-and-effect relationship between variables, they are also controlled for the biases of the research that established the relationship. More specifically, I did not have any thought about how generalizability in research is also a mirror of real-world IT security activity. An instance is provided by vulnerability assessment in security testing, where one organization's vulnerability may not be the same for all computing networks, as well as research findings used overall may not apply to all populations (Yang *et al.* 2022).

Monitoring systems and security analytics fit perfectly well with data analysis and visualization, which was focused in Unit 8. You see, the way I typically detect security threats when I work with dashboards, alerts and logs is much the same as how researchers can use statistical tools and visualization techniques to analyze data. Nevertheless, I noticed that despite my work heavily depending on real time monitoring and rigid reporting, academic research is about methodological transparency, reproducibility and the choice of best statistical method. An important takeaway was to understand the difference in structure of data (qualitative vs quantitative) and how that affects analysis, as most of the time I have worked in my industry have been based around structured numerical data (Torma and Aschemann-Witzel, 2024).

Looking back at these learnings, I realized that there were gaps between what I have experienced in the industry and what I am supposed to do in the academic research methodology. I have a lot of experience in analyzing security threats and vulnerabilities using structured tools but have not considered the necessity of theoretical frameworks, validity tests and methodological rigor required in academic research.

The greatest learning was how important it is to minimize researcher bias. For the problem in IT security, bias could be manifested as false positives or false negatives in threat detection, which means either a lot of false alarms or something they need to be concerned with, but it slipped past their system. This is analogous to research validity where not controlling for confounding variables will result in a wrong conclusion. The concept that stood out to me as something that I could use in my field was triangulation, or the use of multiple sources or methods to validate findings (Donkoh and Mensah, 2023). Similarly, as network security involves several layers of defense mechanisms (e.g. firewalls, IDS, IPS) to be secure, research has to make use of various methodologies to be safe.

Now What?

In the future, I will use the knowledge I have gained about research methods in my professional practice. First, I will be much more critical of the validity of security reports and vulnerability assessments, not just taking the findings on their faces as correct, but thoroughly cross validating the findings. Secondly, I want to improve how I present data, so that security reports are more structured and based on evidence like how research findings are presented with reasons (Von Soest, 2023).

In addition, I have understood the importance of using a more structured approach in my professional work. IT security is about speed and a move to a research driven approach such as hypothesis testing before implementing new security protocols can lead to better risk management. I also see an opportunity to bridge the divide between qualitative and quantitative analysis in my work (van der Kleij *et al.* 2022). Although security data is primarily quantitative, having some sort of qualitative feedback can deepen understanding of security issues.

Summary

This module has been very transforming overall in my approach to solving problems and produced a sense of consciousness in requiring a strong methodological rigor, impartiality when analyzing results, and the need to communicate data effectively. Integrating these research methodologies into my IT security work helps me to make better decisions, to improve security assessments, and to help create more evidence-based cybersecurity strategies.

Reference List

Donkoh, S., and Mensah, J. (2023). Application of triangulation in qualitative research. *Journal of Applied Biotechnology and Bioengineering*, *10*(1), 6-9.

Karvinen, T. (2023). *Configuration management of distributed systems over unreliable and hostile networks* (Doctoral dissertation, University of Westminster).

Torma, G., and Aschemann-Witzel, J. (2024). Sparking stakeholder support: Creating personas for renewable energy innovation adoption based on qualitative data analysis. *Energy Research and Social Science*, *109*, 103407.

van der Kleij, R., Schraagen, J. M., Cadet, B., and Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers and Security*, *113*, 102535.

Von Soest, C. (2023). Why do we speak to experts? Reviving the strength of the expert interview method. *Perspectives on Politics*, *21*(1), 277-287.

Yang, J., Kim, Y. R., and Earwood, B. (2022, October). A study of effectiveness and problem solving on security concepts with model-eliciting activities. In *2022 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). IEEE.