Research Methods and Professional Practice

End of Module Reflective Assignment

https://github.com/mohmmedh1/Research-Methods/blob/main/README.md

Contents

1. Introduction

This reflective piece critically evaluates my learning journey throughout the Research Methods and Professional Practice (RMPP_PCOM7E) module. Applying Rolfe et al.'s (2001) model (What? – So What? – Now What?), I analyse the evolution of my academic, analytical, and ethical competencies and their integration within professional cybersecurity practice.

The reflection demonstrates how structured academic inquiry reshaped my understanding of research design, critical analysis, and professional accountability. It evidences my transformation from a technically focused practitioner into a reflective researcher capable of synthesising ethical reasoning with data-driven decision-making—an essential skill for advanced cybersecurity leadership.

2. WHAT – Description of Learning Experience

Initially, my approach to cybersecurity research was primarily technical and operational, centred on incident response and network defence. This module, however, introduced the philosophical, ethical, and methodological foundations required for credible and reproducible research.

In Unit 1, the Malware Disruption case challenged my ethical reasoning. Analysing the ISP Rogue Services incident through the ACM and BCS Codes of Conduct illustrated that professional judgement requires balancing legal, moral, and societal responsibilities. This experience grounded later reflections on accountability and informed consent, echoing the principles of Respect, Beneficence, Justice, and Accountability outlined in the Menlo Report (Finn & Shilton, 2023).

Across Units 2–4, I refined my ability to translate broad cybersecurity topics into structured research questions and literature reviews. Developing my review on Cloud Security Risks in Higher Education Institutions revealed a lack of empirical studies within regional data-sovereignty contexts—an identified research gap that informs my future dissertation. Peer-review activities strengthened my analytical precision, encouraging evidence-based argumentation over intuition.

In Units 5 and 6, I deepened my understanding of research ethics in data collection. Examining the Cambridge Analytica and TikTok survey cases exposed the consequences of unethical data handling and reinforced the necessity of privacy-by-design—principles I now advocate within MBZUH governance frameworks.

Finally, Units 7–9 expanded my quantitative and inferential-statistics competence. Conducting t-tests, chi-square analyses, and variance evaluations advanced my capability to interpret correlations and causation. Data-visualisation tasks further enhanced my ability to communicate findings effectively; skills now reflected in my cybersecurity incident-trend dashboards.

Collectively, these experiences cultivated a deeper appreciation of how academic rigour underpins ethical and reliable cybersecurity research.

3. SO, WHAT – Critical Interpretation and Analysis

This module initiated a paradigm shift from operational execution to evidence-based critical inquiry. I began questioning not only what occurs in cybersecurity phenomena but also why and how these occur within socio-technical and ethical systems.

Understanding the scientific method (Anderson & Hepburn, 2020) illuminated parallels between research design and SOC analysis—both require observation, hypothesis formulation, and systematic evaluation. This mindset now informs how I validate threat-intelligence sources and assess false-positive anomalies.

The study of research ethics redefined my professional values. Applying the Menlo principles encouraged reflection on proportionality, harm mitigation, and fairness when processing sensitive data. I subsequently integrated anonymisation protocols and controlled retention policies into MBZUH investigations to safeguard user privacy.

A major area of growth involved enhancing critical-thinking and time-management abilities. Balancing work commitments with academic demands required strategic planning and prioritisation matrices. This discipline improved not only my academic output but also operational efficiency, enabling me to manage concurrent security initiatives with reduced stress.

Engaging with diverse research methodologies enriched my analytical flexibility. Quantitative approaches offered empirical validation, whereas qualitative methods revealed behavioural and organisational insights—an essential synergy in cybersecurity research. My evaluation of AI-driven SOC automation combined statistical precision with ethical appraisal, addressing algorithmic bias in decision-support systems.

My statistical literacy matured substantially. Interpreting confidence intervals and effect sizes shifted my perspective from numerical reporting to conceptual understanding. I now treat data as an evolving narrative, applying inferential reasoning to performance metrics for XDR, NDR, and EDR technologies.

Emotionally, transitioning from practitioner to researcher required resilience and humility. Constructive tutor and peer feedback became a driver of academic maturity, helping me view critique as a tool for iterative improvement rather than personal evaluation.

4. NOW WHAT – Future Application and Action Plan

The competencies developed in this module will shape both my academic research and professional leadership. Academically, the methodological discipline established here provides the foundation for my upcoming MSc dissertation, which will propose a CyBOK-based framework for mitigating cloud-security risks in UAE Higher Education. The rigour achieved in sampling, ethics, and validity will ensure credible and publishable outcomes.

Professionally, I will embed a research-informed decision-making approach within MBZUH's Digital Infrastructure Division. Quantitative trend analysis will inform SOC dashboards, while qualitative insights from staff interviews will refine compliance strategies. This mixed-methods approach aligns with organisational resilience objectives and national digital-trust frameworks.

Improved time management and critical reasoning will continue guiding my response to complex cyber incidents. Implementing structured reflection cycles during post-incident reviews now ensures continuous improvement and knowledge transfer. These practices have already enhanced incident-resolution times and reduced escalation frequency.

Ethically, I will continue championing data-governance maturity across MBZUH, ensuring alignment with GDPR, UAE Data Protection Law, and BCS ethical codes. Lessons from historical misuse cases, such as Cambridge Analytica and Google Street View, reinforce my advocacy for informed consent, necessity, and proportionality in all data-processing activities.

Looking forward, I plan to disseminate my findings through a peer-reviewed journal article and to pursue CISSP certification by 2026, bridging scholarly research with professional credibility. This dual pathway positions me as a reflective cybersecurity leader who applies academic reasoning to real-world governance challenges.

5. Learning Outcomes & Evidence

- LO1 – Professional, legal, and ethical issues: Demonstrated through analysis of the Malware Disruption case and GDPR-aligned reflections.
- LO2 – Principles of academic investigation: Evidenced in the literature-review and research-proposal submissions.
- LO3 – Critical evaluation of research design: Applied in comparing quantitative and qualitative paradigms within cybersecurity studies.
- LO4 – Statistical and analytical competency: Proven through hypothesis testing, validity assessment, and visualisation exercises.

All artefacts, worksheets, and reflections are archived in my GitHub e-Portfolio (Units 1–11), evidencing incremental learning across the module.

6. Team Reflection

Collaborating within a culturally diverse cohort illuminated how background and experience shape perceptions of ethical risk. Participation in Collaborative Discussions 1 and 2 honed my communication and analytical skills. Engaging with differing viewpoints challenged cognitive bias and improved my argumentation structure.

Applying Edmondson's (2018) principles of psychological safety, I promoted balanced participation, ensuring all contributions were respected. This process enhanced interpersonal awareness, conflict-resolution skills, and emotional intelligence. It mirrored MBZUH's SOC team dynamics, where cross-functional collaboration is critical for effective incident response. Implementing similar facilitation techniques professionally has improved meeting efficiency and reduced escalation time by approximately 20%, demonstrating direct transfer of academic learning to workplace practice.

7. Academic Integrity & Citations

Throughout this module, I fully adhered to the University of Essex Online (2025) Academic Integrity Policy, maintaining transparency, originality, and accurate referencing. Where digital or AI-assisted tools were utilised for idea structuring, outputs were critically verified and rewritten in my own academic language to preserve authenticity.

This vigilance has strengthened my professional accountability in governance documentation and audit trails. Additionally, I implemented a personal Data Ethics Checklist to ensure that sensitive information within MBZUH risk registers complies with institutional privacy and regulatory requirements.

8. Conclusion

The Research Methods and Professional Practice module has been transformative, bridging academic methodology with professional cybersecurity operations. It equipped me with the ability to design ethical studies, apply quantitative reasoning, and engage in continuous critical reflection. The integration of these capabilities has redefined how I lead investigations, evaluate evidence, and support ethical governance.

By combining scholarly inquiry with applied cybersecurity practice, I now approach every technical challenge as an opportunity for systematic, reflective innovation—embodying the ethos of lifelong learning central to postgraduate education.

Overall, the module significantly enhanced my critical thinking, reflective reasoning, and time management capabilities. These competencies now underpin my academic research and professional leadership approach, ensuring that each decision I make is evidence-driven, ethically grounded, and strategically timed.

9. Evidence of Individual Contributions

All artefacts in the GitHub e-Portfolio represent my independent work, supported by formative tutor feedback and verifiable through timestamped submissions. Screenshots, statistical outputs, and reflection logs provide transparent evidence of individual engagement and achievement.

10. References

Anderson, H. & Hepburn, B. (2020) ‘Scientific Method’, *The Stanford Encyclopedia of Philosophy (Winter 2020 Edition).* Available at: https://plato.stanford.edu/entries/scientific-method/

Edmondson, A. (2018) *The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth.* Hoboken: Wiley.

Finn, M. & Shilton, K. (2023) ‘Ethics governance development: The case of the Menlo Report’, *Social Studies of Science*, 53(3), pp. 315–340. Available at: https://journals.sagepub.com/home/sss

Rolfe, G., Freshwater, D. & Jasper, M. (2001) *Critical Reflection in Nursing and the Helping Professions: A User’s Guide.* Basingstoke: Palgrave Macmillan.

University of Essex Online (2025) *Research Methods and Professional Practice Module Resources.* Colchester: University of Essex Online.

Mohammed Bin Zayed University for Humanities (MBZUH) (2025) *Institutional Website.* Available at: https://www.mbzuh.ac.ae