Reflective Analysis on Research Methods and Professional Practice

This reflection critically examines my learning trajectory within the Research Methods and Professional Practice module, using the What? – So What? – Now What? framework (Rolfe et al., 2001). As a senior Cybersecurity Professional, my initial approach focused heavily on operational pragmatism and GRC compliance. The module fundamentally reshaped my analytical and methodological rigour, leading to four key developments: epistemological reframing, critical appraisal skills, enhanced statistical literacy, and the integrated design of my mixed-methods research proposal on a Hybrid AI–Human Framework.

Key Learning Outcomes

The module's structured approach facilitated a significant evolution in my professional and academic capabilities:

Learning Outcome	Artefact	Reflection
Reflect on ethical and professional issues in computing	Menlo Report application (Unit 1) and proposal ethics section.	Embedded Beneficence and Justice principles (Finn & Shilton, 2023) to ensure research design maximises benefit, minimises harm, and includes diverse stakeholder perspectives.
Critical Evaluation of Research Paradigms	The Epistemological Shift (Unit 3) and Peer Review of Zero-Trust Architecture papers.	Challenged the default positivist stance, recognising the vital role of interpretivism and socio-technical factors (Saxe, 2018; Saunders et al., 2023) in understanding security culture.
Apply statistical techniques to research problems	Inferential Statistics Worksheets and analysis of threat detection times.	Transcended statistical anxiety to gain practical insight into p-values and confidence intervals, enabling a critical evaluation of data-driven security claims (Benavoli & Mangili, 2023).
Synthesising a Mixed-Methods Research Design	Research Proposal: 'A Hybrid AI–Human Framework for Mitigating Security Vulnerabilities...'.	Demonstrated the ability to design a coherent, mixed-methods study, aligning philosophical stance with analytical techniques to address a complex, real-world socio-technical gap (Creswell

		& Creswell, 2023).

WHAT? (Description of Key Learning)

The module's structure challenged entrenched professional biases and expanded my methodological toolkit.

1. Epistemological and Ontological Reframing

Professionally, my reliance on SIEM (Security Information and Event Management) metrics and KPIs fostered a strong positivist orientation. Unit 3 revealed the limitations of this stance, especially concerning the human element. The interpretivist perspective, emphasising subjective reality, became compelling for analysing security culture and incident post-mortems, highlighting that security "truth" is a complex product of socio-technical factors (Aljuhani & Slay, 2024; Saxe, 2018). This shift was crucial for viewing security as more than a deterministic technical problem (Saunders et al., 2023).

2. Peer Review and Critical Appraisal

The peer review activity on AI security papers required rigorous assessment of methodological alignment and validity (Fink, 2023). This immediately exposed my underlying bias rooted in a prioritisation of quantifiable data. Critiquing a qualitative, thematic study forced me to recognise the depth of insight qualitative methods provide regarding adoption barriers and human trust. This direct engagement fostered active, critical interrogation of research, mirroring the ethical responsibility of a research-informed practitioner.

3. Confronting Statistical Anxiety

Focusing on inferential statistics (t-tests, p-values, confidence intervals) initially caused cognitive dissonance. Overcoming this transformed my practice: I moved from relying on automated dashboards to becoming an active interrogator of data validity and reliability, directly aligning with the Beneficence principle of the Menlo Report (Finn & Shilton, 2023). This struggle exposed an over-reliance on automated tools which, if unchecked, compromises the ability to scrutinise data-driven security decisions (Benavoli & Mangili, 2023).

4. Synthesising the Research Proposal

The culminating task involved synthesising learning into the research proposal, *'A Hybrid AI–Human Framework for Mitigating Security Vulnerabilities'*. This required identifying a precise research gap and justifying a mixed-methods design (Creswell & Creswell, 2023), combining

quantitative analysis with qualitative interviews. Crucially, I applied a socio-technical security lens (Saxe, 2018), framing the technical (AI robustness) and human (oversight) layers as inseparable research elements, connecting academic methodology directly to complex, real-world governance challenges (Yin, 2018).

SO WHAT? (Analysis of Significance)

My shift from absolute positivism to a pragmatic acceptance of mixed-methods aligns with the contemporary complexity of cybersecurity, where quantifiable metrics and nuanced cultural factors both drive risk (Aljuhani & Slay, 2024; Bryman, 2016). Qualitative insights reveal the governance and procedural dimensions crucial for resilient systems (Saunders et al., 2023). This expansion reinforces the Justice principle of the Menlo Report (Finn & Shilton, 2023), ensuring security governance reflects a full spectrum of stakeholder perspectives.

The peer review process, informed by systematic review principles (Gough et al., 2017), fostered a heightened axiological consciousness. My discomfort with qualitative assessment exposed an unexamined bias I am now actively addressing. This critical appraisal of research design directly mirrors the rigour required for presenting robust, defensible recommendations to executive leadership.

Conquering statistical anxiety was a professional necessity. Sound statistical literacy is essential for assessing the robustness of research claims (Benavoli & Mangili, 2023). My enhanced understanding of inferential statistics allows me to critically evaluate the significance of security claims, directly supporting the Beneficence principle (Finn & Shilton, 2023) by maximising organisational benefit through reliable, validated decision-making.

The research proposal served as a proof of concept. The ability to design a holistic, mixed-methods study, justifying the approach based on the specific research question (Creswell & Creswell, 2023; Yin, 2018), is directly transferable to the strategic planning of security programmes, where technical implementation must be framed by governance, human factors, and measurable outcomes.

NOW WHAT? (Actionable Steps)

The module has established a new trajectory, cementing my role as a research-informed security strategist.

A SWOT analysis

SWOT%20Analysis%
20-%20Research%20

Professional Development Actions

1. Integrating Research into Practice: I plan to apply mixed-methods evaluations in future assessments of security tools, combining quantitative performance metrics with structured practitioner feedback (Saunders et al., 2023).
2. Enhancing Statistical Proficiency: I will undertake a short course in statistics (e.g., Python/SPSS) and PowerBI training to enable inferential statistical visualisation of organisational risk metrics and reanalyse module datasets.
3. Embedding Ethical Practices: Drawing on the Menlo Report (Finn & Shilton, 2023), I will audit AI security governance programmes for fairness, inclusivity, and adherence to Justice and Beneficence principles.
4. Academic Engagement: I aim to disseminate dissertation findings through professional forums such as the ISACA Journal to bridge academic-practice gaps and contribute thought leadership.
5. Sustained Reflective Practice: I will integrate the Rolfe et al. (2001) model into a quarterly Continuing Professional Development (CPD) review cycle for major GRC (Governance, Risk and Compliance) programme deliveries (University of Edinburgh, n.d.).

Personal Development Plan

PDP%20-%20Resear
ch%20Methods%20a

Conclusion

The Research Methods and Professional Practice module has been transformative, bridging academic methodologies and professional cybersecurity practice. Through epistemological exploration, peer review, statistical engagement, and research design, I have evolved into a reflective, evidence-informed researcher. This foundation enables me to critically engage with emerging challenges, such as securing generative AI

systems, through socio-technical, ethical, and methodological lenses, strengthening my capacity to lead resilient cybersecurity initiatives in complex regulatory environments.

References

Aljuhani, A. and Slay, H. (2024) ‘The importance of socio-technical factors in cybersecurity research: A systematic review’, International Journal of Computer Science and Network Security, 24(1), pp. 174–182.

Benavoli, A. and Mangili, F. (2023) ‘Bayesian analysis in cybersecurity: overcoming frequentist limitations’, IEEE Transactions on Information Forensics and Security, 18, pp. 1120–1134.

Bryman, A. (2016) Social Research Methods. 5th edn. Oxford: Oxford University Press.

Creswell, J.W. and Creswell, J.D. (2023) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 6th edn. Thousand Oaks, CA: SAGE Publications.

Fink, A. (2023) Conducting Research Literature Reviews: From the Internet to Paper. 6th edn. Thousand Oaks, CA: SAGE Publications.

Finn, M. and Shilton, K. (2023) ‘Ethics governance development: The case of the Menlo Report’, Social Studies of Science, 53(3), pp. 315–340.

Gough, D., Oliver, S. and Thomas, J. (2017) An Introduction to Systematic Reviews. 2nd edn. London: SAGE Publications.

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

Saunders, M., Lewis, P. and Thornhill, A. (2023) Research Methods for Business Students. 8th edn. Harlow: Pearson Education Limited.

Saxe, J. (2018) ‘Socio-technical security: The human–machine interface’, Journal of Information Security Research, 9(2), pp. 85–97.

The University of Edinburgh (n.d.) ‘Reflector's Toolkit’. Available at: https://reflection.ed.ac.uk/reflectors-toolkit/reflecting-on-experience (Accessed: 12 October 2025).

Yin, R.K. (2018) Case Study Research and Applications: Design and Methods. 6th edn. Thousand Oaks, CA: SAGE Publications.