1. Introduction

This e-Portfolio consolidates the evidence of my academic and professional learning throughout the Research Methods and Professional Practice module. It demonstrates how I have applied research principles, ethical governance, and quantitative analysis within real-world cybersecurity management.

The purpose of this narrative is to showcase how theoretical knowledge has been transformed into practical, ethical, and analytical competence. Each section aligns with the module's learning outcomes—appraising professional and ethical issues, evaluating research methodology, and developing independent critical enquiry.

The structure mirrors my development: beginning with the application of knowledge through ethical and statistical exercises, moving to independent work through literature and proposal evaluation, and culminating in professional growth reflected in the Skills Matrix and Action Plan. The portfolio illustrates how reflective practice, guided by Rolfe et al.'s (2001) What? So What? Now What? model, transformed my perspective from technical practitioner to research-oriented cybersecurity professional.

.

2. Application of Knowledge

1. Ethics and Professional Conduct

The early stages of the module focused on the ethical foundations of computing research. In Unit 1, the Malware Disruption Case presented a moral dilemma involving an internet service provider deploying retaliatory malware to disable a botnet. Using the ACM Code of Ethics (2018) and BCS Code of Conduct (2024), I assessed the situation through the principles of beneficence, non-maleficence, and respect for privacy.

This exercise emphasised that even when intentions are good, actions must remain within legal and ethical boundaries. I concluded that the ISP's behaviour breached principles of due process and user consent. The discussion highlighted the fine balance between proactive defence and unlawful intrusion. In my professional practice, these insights reinforced the importance of ensuring that every security response complies with institutional policy and data-protection law.

The collaborative ethics discussion further improved my communication and analytical reasoning. Engaging with peers exposed me to diverse viewpoints—technical, legal, and moral—helping me appreciate that cybersecurity decisions are rarely binary. The case taught me that ethical reasoning strengthens rather than limits operational efficiency because it builds organisational trust and accountability.

2. Privacy and Data Governance

In Unit 4, the Beth and Ricardo Case extended ethical reasoning into the domain of data protection. Analysing how a researcher mishandled sensitive records illustrated the importance of informed consent, data minimisation, and purpose limitation under GDPR (2018) principles.

Through this case, I realised that ethical research requires both technical safeguards and procedural governance. I connected this directly to professional data-governance processes, implementing stronger anonymisation controls to protect personal information.

Further examples such as Cambridge Analytica's political profiling and Google Street View's Wi-Fi collection were analysed in Unit 5, exposing how organisations can misuse data under the guise of innovation. Reflecting on these cases helped me reinforce the need for ethical transparency and continuous consent in any data-driven cybersecurity project..

3. Statistical and Analytical Application

Units 7 to 9 advanced my quantitative-research competence. I completed inferential-statistics exercises using Excel datasets. Key analyses included:

- Paired t-Test (Con1 vs Con2): $t = 2.875$, $p = 0.01834$ → significant difference
- Independent t-Test (Diet A vs Diet B): $t = 3.072$, $p = 0.00275$ → significant
- Chi-square Test (Area × Brand): $p = 0.19276$ → no significant association

These results taught me how to distinguish statistical significance from practical relevance and how sampling influences generalisability.

Visualisation exercises in Unit 8 (bar, line, and scatter charts) enhanced my ability to present data clearly—skills directly transferable to cybersecurity performance reporting. In Unit 9, validity and generalisability activities reinforced the need for representative data. I now interpret performance metrics through this same lens, ensuring conclusions are evidence-based and statistically defensible.

Through these ethical and analytical components, I developed the intellectual discipline to evaluate evidence critically and apply research logic to practical cybersecurity scenarios.

3. Independent Work

Independent work was demonstrated most prominently through the Literature Review and Research Proposal assignments. Initially, my literature review lacked methodological precision; feedback highlighted the need to differentiate between systematic and narrative approaches. Revisiting the structure, I re-organised my sources around clear research questions and methodological categories, which enhanced coherence and analytical depth.

The revised review focused on “Cloud Security Risks in Higher Education Institutions (HEIs)”, synthesising works such as ENISA (2023) on cloud risk management and Alazab et al. (2024) on phishing-detection frameworks. I identified a gap in empirical studies linking risk governance with academic data environments, leading to my proposal for a CyBOK-based Framework for Managing Cloud Risks in HEIs.

The peer-review exercise in Unit 3 was especially valuable. Providing feedback to a colleague honed my critical-evaluation skills, while receiving critique improved my awareness of research-design limitations. I incorporated suggestions by refining my sampling strategy and clarifying whether my research employed a systematic literature review (SLR) or mixed-methods approach.

This independent process mirrored real academic peer review and improved my self-reliance as a researcher. I learned to justify methodological choices—quantitative, qualitative, or mixed—based on the research aim rather than convenience. It also enhanced my ability to apply ethical-review processes, ensuring participant confidentiality and compliance with institutional research-ethics policies.

In my professional context, this independence translates to evidence-driven decision-making. When evaluating security solutions or analysing incident patterns, I now adopt the same structured methodology: define questions, collect and assess evidence, and derive conclusions transparently. This alignment of academic and operational practice reflects my growth from technician to reflective practitioner-researcher.

4. Professional Development

The final phase of the module focused on professional reflection and future planning, documented through the Professional Skills Matrix, SWOT Analysis, and Action Plan.

1. Skills Matrix and Competency Growth

Mapping my capabilities against the BCS Professional Standards and Essex Graduate Attributes clarified my strengths in technical and analytical domains: network defence,

encryption, and data analysis. It also revealed opportunities for development in academic publication, Python-based automation, and research dissemination.

This matrix demonstrated how academic study reinforces workplace performance. For example, quantitative skills gained through the module have already been applied to develop SOC performance dashboards, integrating validity checks and statistical trend analysis.

2. SWOT Analysis

The SWOT exercise provided structured self-assessment:

- Strengths: Leadership in cybersecurity operations, analytical thinking, and ethical governance.
- Weaknesses: Limited publication record and automation expertise.
- Opportunities: Pursuing CISSP certification and publishing on cloud-security frameworks.
- Threats: Rapid technological change and balancing MSc demands with full-time leadership duties.

Identifying these elements allowed me to set realistic, measurable goals that align with both institutional and academic priorities.

3. Action Plan

To convert reflection into measurable growth, I developed SMART objectives:

a) Publish a Paper on Cloud Security Risks in HEIs
   - Revise literature review, format per IEEE guidelines, submit by May 2026.
   - Outcome: peer-reviewed publication and academic visibility.

b) Achieve CISSP Certification
   - Study using ISC² materials; complete by February 2026.
   - Outcome: validated industry competence and enhanced organisational governance.

c) Improve Python for Security Automation
   - Complete Microsoft Learn course; apply automation to SOC log analysis.
   - Outcome: increased efficiency and data-driven detection.

d) Maintain GitHub e-Portfolio
   - Consolidate artefacts and reflections; update quarterly.
   - Outcome: transparent academic-professional profile.

4. Application in Practice

Implementing these goals has already begun. The structured reflection inspired new mentoring initiatives within the SOC, enabling junior analysts to apply ethical reasoning and research methods in incident response. Moreover, I now present research-style briefings during internal security meetings, integrating literature evidence and quantitative findings—a direct result of the module's influence.

This professional-development plan demonstrates that reflective practice is not a passive exercise but a continuous improvement mechanism that links academia with enterprise security operations.

5. Conclusion

The Research Methods and Professional Practice module has been transformative. It provided not only academic understanding of research design and ethics but also the tools to embed those principles into real-world cybersecurity governance.

Through applying ethical frameworks, mastering statistical techniques, and developing independent analytical thinking, I evolved into a more reflective and accountable professional. The integration of theory and practice has enhanced both my academic trajectory and my leadership in cybersecurity research.

This e-Portfolio captures that evolution: from learning about research to living research ethics and methodology daily, ensuring that future cybersecurity decisions are informed, transparent, and grounded in evidence.

6. References

ACM (2018) *Code of Ethics and Professional Conduct.* Available at: https://ethics.acm.org

Alazab, M., Awajan, A. and Mesleh, A. (2024) 'A Machine Learning Framework for Detecting Phishing Websites', *IEEE Access*, 12(6), pp. 11432–11447.

BCS (2024) *Code of Conduct.* Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct

ENISA (2023) *Cloud Security Risk Management for Public Institutions.* Athens: European Union Agency for Cybersecurity.

Finn, M. and Shilton, K. (2023) 'Ethics Governance Development: The Case of the Menlo Report', *Social Studies of Science*, 53(3), pp. 315–340.

Field, A. (2022) *Discovering Statistics Using IBM SPSS Statistics*, 6th edn. London: Sage.

Rolfe, G., Freshwater, D. and 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 Materials.* Colchester: University of Essex Online.