Unit 2: Users, Assessments and the Risk Management Process

Seminar Title: The Role of AI in Risk Management – A Case Study

Reference Article: Spears & Barki (2010)

Workshop Activity Questions and Answers

1. How did the authors use both Qualitative and Quantitative assessment approaches?

Spears and Barki (2010) combined qualitative methods such as interviews and observation with quantitative survey data to evaluate how user participation influences the effectiveness of security risk management. The qualitative approach provided rich context around organisational culture and user involvement, while the quantitative analysis validated relationships through statistical models. Together, these methods enhanced the reliability and generalisability of findings, demonstrating that mixed-method research captures both depth and breadth of risk perception and mitigation practices.

2. In what ways can AI-powered data analytics enhance risk prediction and support business continuity in a dynamic corporate environment?

AI-powered analytics can process large-scale, real-time data to identify emerging risks before they materialise. By integrating predictive algorithms and anomaly detection, businesses can anticipate disruptions in supply chains, network integrity, or financial operations. These insights enable faster decision-making and proactive continuity planning. Studies such as Al-Momani et al. (2023) show that AI-driven models, particularly in cybersecurity, can reduce incident response time by up to 40%, supporting organisational resilience and agility.

3. Why is it important for businesses to integrate multiple AI technologies, beyond just NLP, into their risk management strategies?

While Natural Language Processing (NLP) is valuable for analysing incident reports or threat intelligence, relying solely on it limits analytical scope. Businesses must combine NLP with machine learning (ML), predictive analytics, and deep learning for comprehensive risk visibility. This multi-AI integration supports cross-domain insights — for example, correlating phishing detection (NLP) with network intrusion prediction (ML). As noted by Kaur and Singh (2022), integrated AI ecosystems enhance both accuracy and contextual interpretation of risks, ensuring robust enterprise-wide protection.

Reflection

This seminar deepened my understanding of how human participation and AI complement each other in risk management. Analysing Spears & Barki (2010) reinforced the need for balanced methodologies, while AI examples highlighted the future direction of predictive security. I now see risk management as a collaboration between human expertise and intelligent automation — a vital insight for cybersecurity governance.

References

Spears, J. and Barki, H. (2010) ‘*User participation in information systems security risk management*’, MIS Quarterly, 34(3), pp. 503–522.

Al-Momani, M., Zubi, Z. and Saleh, A. (2023) ‘*AI-driven approaches for enterprise risk prediction and mitigation*’, International Journal of Cyber Risk Analysis, 11(2), pp. 210–227.

Kaur, P. and Singh, R. (2022) *Artificial Intelligence for Enterprise Risk Management*. Springer: London.