Seminar 2 Workshop Activity

A: How did the authors use both Qualitative and Quantitative assessment approaches? What benefits did each approach yield?

Spears and Barki (2010) used qualitative analysis to create a base level of understanding on the nature of user participation in the context of security and risk management (SRM). This was deemed necessary due to previous studies being predominantly focused on users as a weak link, rather than on how users can positively affect the development of SRM processes. Quantitative analysis was then performed using the results.

The qualitative analysis consisted of interviewing people in 5 businesses with some oversight over security or risk processes or had some relationship to compliance with the Sarbanes-Oxley (SOX) act of 2022. The interviews broadly investigated what information security (IS) activities were performed by users of these companies and how the interviewees felt the quality of IS was affected as a result. Overall, the feeling of the participants was that the more user's interacted with the SRM processes, the more they understood the purpose of SRM controls, reducing risk.

The quantitative analysis began with a survey of businesses that comply with SOX, on user involvement, SRM control development and performance. Responders gave a value between 1 and 7 on various aspects of the three areas. Variation in responses was then evaluated using the partial least squares (PLS) modelling approach to find the interoperability of the three areas. The results validated the findings of the qualitative analysis; user participation does improve company awareness and process around SRM.

Subsequent work by Marc, Arena and Peljhan (2023) supports the findings with their own quantitative analysis, again using a survey and PLS modelling. They found that interactivity with risk management systems (RMS) had positive correlation with RMS design and effectiveness.

References

Spears, J. L. and Barki, H. (2010) ‘User Participation in Information Systems Security Risk Management’, *MIS Quarterly*, 34(3), pp. 503–22. Available at: https://doi.org/10.2307/25750689

Marc, M., Arena, M. and Peljhan, D. (2023) ‘The role of interactive style of use in improving risk management effectiveness’, *Risk Management*, 25(9). Available at: https://doi.org/10.1057/s41283-023-00114-4

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

The article by Kalogiannidis et al. (2024) describes multiple uses for AI- powered data analytics in a risk management and business continuity capacity, including:

- New threat detection – Things can change quickly in dynamic corporate environments; AI is much quicker at identifying new attack patterns than traditional models. It can then evaluate these patterns and help define new strategies to prevent or mitigate them.
- Real-time Monitoring – AI can utilise data to track variables, allowing strategies to be adapted at the earliest opportunity. This is extremely useful in incident response, as logs, incoming traffic, processing requests can all be parsed in rapid time, so if an incident occurs a response can be immediately deployed.
- Predictive Modelling – AI's ability to process a large volume of data makes predictive models much faster, less error prone and completely unbiased. This can be used in risk forecasts, warehouse and equipment management etc. AI is also capable of handling data that would be impossible to process by humans, allowing insights previously inaccessible.

Aljohani (2023) made similar conclusions and implemented various case studies in which AI-driven analytics were used practically in various businesses, highlighting its adaptability. The studies were successful, although the need to balance complexity and efficiency of models was highlighted, so that the technology can be implemented in regular businesses in the long-term.

References

Aljohani, A. (2023) ‘Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility’, *Sustainability*, 15(20), 15088. Available at: https://doi.org/10.3390/su152015088

Kalogiannidis et al. (2024) ‘The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece’, *Risks*, 12(2), 19. Available at: https://doi.org/10.3390/risks12020019

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

Kalogiannidis et al. (2024) strongly promotes the use of NLP in risk management strategies, finding it speeds up risk assessment and makes it more precise. NLP's ability to parse large volumes of human language data leads to deeper and more effective insights. However, it was noted that although NLP does have a positive impact on business continuity, there are other necessary factors.

However, to gain a more holistic analysis of data for use in risk analysis, other technologies must be used to determine insights from statistical / numerical data, visual data, inputs from sensors, and for creating data that can be used to simulate situational risk. These technologies include:

- Machine Learning – Used to sort through historical data to enhance decision-making and make predictions. Aljohani (2023) found that using a combination of machine learning and predictive analytics led to a more proactive form of risk analysis, ultimately leading to more agile decision-making. Shi et al. (2022) consider machine learning an improvement over statistical based methods, and the subset of deep learning to be the most effective and accurate method of analysing risk in this way.
- Computer Vision – Analysis of visual data such as recordings, photos and live video. Can be used for real time monitoring of events for safety and liability purposes. Lan, Awolusi and Cai (2024) researched using computer vision for improving worker safety at steel mills and returned positive results, albeit with some limitations.

- Generative AI – Can create its own datasets that simulate real life data, to perform analysis free of concerns about data privacy and compliance regulations. Nadella et al. (2025) tested a framework based on this principle and reported improved threat detection, high levels of accuracy and recall, adaptability across domains and effective data privacy safeguards.

References

Aljohani, A. (2023) 'Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility', *Sustainability*, 15(20), 15088. Available at: https://doi.org/10.3390/su152015088

Kalogiannidis et al. (2024) 'The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece', *Risks*, 12(2), 19. Available at: https://doi.org/10.3390/risks12020019

Lan, R., Awolusi, I. and Cai, J. (2024) 'Computer Vision for Safety Management in the Steel Industry', *AI*, 5(3), pp. 1192-1215. Available at: https://doi.org/10.3390/ai5030058

Nadella et al. (2025) 'Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management', *Computers*, 14(2), 55. Available at: https://doi.org/10.3390/computers14020055

Shi et al. (2022) 'Machine-learning driven credit risk: a systemic review', *Neural Computing and Applications,* 34, pp. 14327-14339. Available at: https://doi.org/10.1007/s00521-022-07472-2