Qualitative and Quantitative Assessment Approaches in Spears & Barki (2010)

1. Qualitative Methods:

The qualitative methods employed by Spears and Barki (2010) allowed for a detailed understanding of user roles in SRM. Recent studies emphasise the importance of qualitative approaches in exploring user involvement in IS security. For example, Myers (2019) highlights that qualitative methods such as interviews and case studies are instrumental in understanding the contextual and cultural factors that influence organisational security behaviour. Despite the value of qualitative approaches, there are challenges, such as social desirability bias, as King and Brooks (2017) discussed, which can influence the data collected through interviews. Triangulating these findings with other methods like document analysis or observational data can help reduce biases.

Spears and Barki (2010) leveraged qualitative methods to identify themes from interviews, which are foundational in building a grounded theoretical model, an approach still valued today for exploring emerging phenomena in IS security (Trauth, 2001). Despite this, more observational techniques could enhance findings by providing real-world verification of self-reported data.

Benefits: Qualitative methods remain indispensable for understanding how user participation affects SRM. The study's combination of thematic analysis and semi-structured interviews offers a comprehensive view, validated by the work of Baxter and Jack (2018), who continue to promote case study research to contextualise findings in specific organizational environments.

2. Quantitative Methods:

Spears and Barki (2010) used quantitative methods, such as PLS regression, to empirically validate the relationships derived from the qualitative study. However, Hair et al. (2017) suggest that Structural Equation Modelling (SEM) could provide a more nuanced understanding of complex interactions within IS security. This approach might yield more profound insights into the indirect effects of user participation on SRM outcomes.

Benefits: The strength of Spears and Barki's quantitative approach lies in its ability to generalise findings across a broader population. This approach is still relevant, as demonstrated by Bélanger and Crossler (2019), who used survey-based quantitative methods to assess security behaviour and found significant connections between user participation and improved security outcomes.

Advantages of Involving Users in the Risk Management Process

1. Improved Control Development:

Involving users in SRM improves control development by providing valuable, context-specific insights. Alshaikh et al. (2021) reaffirm Spears and Barki's (2010) findings, showing that user involvement in security control design enhances the adaptability and relevance of controls. However, they caution that user participation can lead to poorly implemented controls without proper training.

Critical Note: Barki and Hartwick (1994) noted that user participation often leads to better alignment of controls with business processes, but this can only be achieved if users are sufficiently knowledgeable about security risks and business needs.

2. Increased Organizational Awareness:

Spears and Barki (2010) argue that user participation increases awareness of security risks, a claim supported by recent studies. Cram et al. (2017) suggest that such participation fosters a security-aware culture, but they highlight that awareness alone does not guarantee long-term security. Bélanger and Crossler (2019) further contend that awareness must be followed by consistent behavioural changes to ensure lasting impact.

Critical Note: Dhillon and Moores (2001) raise the concern that security awareness programs often fade over time if not reinforced. This suggests that continuous engagement and training are essential to maintaining awareness beyond the initial stages of participation.

3. Alignment with Business Processes:

Aligning security controls with business processes, as emphasised by Spears and Barki (2010), is crucial for effective SRM. However, this alignment can sometimes be challenging. Suh and Han (2003) argue that in some cases, business goals conflict with security objectives, leading to resistance from users when security measures impede productivity.

Impact of Lack of User Access on Risk Assessment

1. Incomplete Risk Identification:

Without user participation, critical business-specific risks may go unaddressed. Alshaikh et al. (2021) highlight that users are often the first to recognise

vulnerabilities in their workflows. Spears and Barki (2010) note that user involvement helps identify risks overlooked in a purely technical assessment.

2. Poorly Aligned Controls:

Controls designed without user input are often poorly aligned with actual business processes, leading to compliance issues. D'Arcy and Herath (2011) found that poorly aligned controls tend to encourage workarounds, as employees prioritise operational efficiency over security measures. This behaviour often results in unintended security gaps. Spears and Barki (2010) emphasise the need for user engagement to ensure that security measures are both practical and supportive of the organisation's workflows, mitigating these risks.

Mitigation Strategies

1. Increased Collaboration with Auditors and Consultants:

Collaboration with auditors and consultants can help organisations address security risks when user access is limited. Siponen and Vance (2010) argue that external auditors bring a fresh perspective to security assessments, often identifying risks that internal teams may overlook due to familiarity with the system. However, Spears and Barki (2010) emphasise that while external expertise is valuable, it must be balanced with internal knowledge to ensure that risk management strategies are relevant and implementable within the specific organisational context.

2. Use of Proxy Interviews:

When direct user access is unavailable, proxy interviews with managers or team leaders can offer valuable insights. Goucher et al. (2020) found that while proxy interviews are helpful, supplementing them with process data ensures a more accurate

reflection of user behaviour. Spears and Barki (2010) also suggest that this can be a helpful alternative, though it is not a perfect substitute for direct engagement.

3. Surveys and Questionnaires:

Surveys and questionnaires are commonly used when face-to-face interviews are not feasible. D'Arcy and Herath (2011) emphasise that while surveys are effective for gathering large amounts of data, combining them with interactive methods like workshops can yield more actionable insights. Workshops and focus groups encourage deeper engagement from participants, enabling them to explore complex security behaviours and practices in a more open format. Spears and Barki (2010) highlighted the utility of surveys in capturing broad patterns of user participation across organisations, though they also acknowledged that more dynamic methods could complement traditional surveys by fostering richer discussion and user feedback.

Bibliography

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2021) An exploratory study of current information security training and awareness practices in organisations Information & Computer Security. 29(1); 1839. https://aisel.aisnet.org/hicss-51/os/practice-based_research/4/ [Accessed 08/09/2024]

Barki, H. and Hartwick, J. (1994) Explaining the role of user participation in information system use, Management Science. 40(4); 440465 https://pubsonline.informs.org/doi/abs/10.1287/mnsc.40.4.440 [Accessed 08/09/2024]

Baxter, P. and Jack, S. (2018) Qualitative case study methodology: Study design and implementation for novice researchers The Qualitative Report. 13(4); 544559 https://www.academia.edu/download/40131683/case_study_ecmple.pdf [Accessed 08/09/2024]

Cram, W.A., Proudfoot, J.G., and D'Arcy, J. (2017) Organisational information security policies: A review and research framework European Journal of Information Systems. 26(6); 605641 https://doi-org.uniessexlib.idm.oclc.org/10.1057/s41303-017-0059-9 [Accessed 10/08/2024]

Dhillon, G. and Moores, T. (2001) Information systems security management in the new millennium. *Communications of the ACM* 44(9); 125128 https://dl.acm.org/doi/fullHtml/10.1145/341852.341877 [Accessed 09/07/2024]

Siponen, M. and Vance, A. (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3); 487-502 https://doi.org/10.2307/25750688 [Accessed 09/08/2024]

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2017) A Primer on Partial Least Squares Structural Equation Modeling. (PLSSEM) 2nd edn Thousand Oaks: Sage Publications https://doi.org/10.1080/1743727X.2015.1005806 [Accessed 09/08/2024]

King, N. and Brooks, J. (2017) Template Analysis for Business and Management Students. London: Sage Publications. https://web-p-ebscohost-com.uniessexlib.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=4&sid=daf6b4f0-48ff-4715-9f48-620824cb2ad1%40redis [Accessed 09/08/2024]

Siponen, M., Mahmood, M.A. and Pahnila, S. (2018) Employees' adherence to information security policies: An integrative model and empirical tests, MIS Quarterly 42(1); 1030 https://doi.org/10.1016/j.im.2013.08.006 [Accessed 10/08/2024]

Spears, J.L. and Barki, H. (2010) User participation in information systems security risk management. MIS Quarterly, 34(3); 503522 https://www.jstor.org/stable/25750689 [Accessed 09/08/2024]

Suh, B. and Han, I. (2003) The IS risk analysis based on a business model, Information & Management. 41(2); 149158 https://doi.org/10.1016/S0378-7206(03)00044-2 [Accessed 09/08/2024]

Myers, M.D. (2019) Qualitative Research in Business and Management. 3rd edn. London: Sage Publications https://doi-org.uniessexlib.idm.oclc.org/10.1108/11766090910989536 [Accessed 10/08/2024]

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2021) An exploratory study of current information security training and awareness practices in organisations, *Information & Computer Security* 29(1); 18-39 https://aisel.aisnet.org/hicss-51/os/practice-based_research/4/ [Accessed 10/08/2024]

D'Arcy, J. and Herath, T. (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings European Journal of Information Systems. 20(6); 643-658 https://doi.org/10.1057/ejis.2011.23 [Accessed 10/08/2024]

Spears, J.L. and Barki, H. (2010) User participation in information systems security risk management. *MIS Quarterly*, 34(3); 503-522 https://doi.org/10.2307/25750689 [Accessed 11/09/2024]