UNIT 2 SEMINAR PREPARATION - USER PARTICIPATION IN THE RISK MANAGEMENT PROCESS

HOW DID THE AUTHORS USE BOTH QUALITATIVE AND QUANTITATIVE ASSESSMENT APPROACHES?

Spears & Barki (2010) collated, analysed and integrated both qualitative and quantitative to examine user participation in security risk management. After conducting interviews with one sample of informants having experience in organisational compliance with the Sarbanes-Oxley Act of 2002, the three user participation theories described by Markus and Mao (2004) were used to construct a process model as a framework for analysis. Thereafter, quantitative method (survey) using a different sample was used to test the theoretical model derived from the qualitative study.

WHAT BENEFITS DID EACH APPROACH YIELD?

Qualitative

1. Provided a rich understanding of the activities, behaviors, and assignments that define user participation in the context of SRM for regulatory compliance.
2. Allowed a process model to be constructed by applying the three user participation theories described by Markus and Mao (2004) as a framework for analysis.

Quantitative

1. Clarity (more precise definition) of theoretical concepts
2. Reveals theoretical relationships that may have been missed in qualitative study

WHAT DO THE AUTHORS LIST AS THE ADVANTAGES OF INVOLVING USERS IN THE RISK MANAGEMENT PROCESS?

1. **Organisational security controls (i.e., policies, procedures, safeguards, and countermeasures that prevent, detect, or minimize an IS security breach) can only be effective to the extent that people handling the information in their day-to-day jobs (e.g., functional business users) are aware of those measures and adhere to them.**
2. **Security controls need to be aligned with business objectives to be effective. Such alignment requires an understanding of the relative value of information, how information is used within and across business processes, and at what nodes within a process sensitive information is most vulnerable. User participation in IS security risk analysis and control design can provide needed business knowledge, thus contributing to more effective security measures.**

BASED ON THE FINDINGS OF THE RESEARCH,

HOW WILL THE LACK OF USER ACCESS AFFECT THE RISK ASSESSMENT YOU WILL CARRY OUT AS PART OF YOUR ASSESSMENT?

WILL IT AFFECT THE CHOICE OF QUALITATIVE VS. QUANTITATIVE ASSESSMENT METHODS YOU UTILISE?

HOW MIGHT YOU MITIGATE ANY ISSUES ENCOUNTERED?

1. **Poor access control can expose the organisation to unauthorized access of data and programs, fraud, or the shutdown of computer services.**
2. **No. The choice of either qualitative or quantitative assessment depends on available data and context. Quantitative assessment is preferred when testing or confirming a theory or hypothesis while qualitative assessment is suitable when seeking for understanding of concepts, thoughts or experiences.**
3. **Emplacement of physical, procedural and technical controls.**

References

Markus M and Mao J (2004). Participation in Development and Implementation - Updating an Old, Tired Concept for Today's IS Contexts, Journal of the Association for Information. Available from https://aisel.aisnet.org/jais/vol5/iss11/14/ [Assessed 30 August 2022]

Spears, J. & Barki, H., (2010). User participation in information systems risk management. Available from: https://www-jstor-org.uniessexlib.idm.oclc.org/stable/pdf/25750689.pdf?refreqid=excelsior%3A6a87aa557d27a29300e45939cf76cf05&ab_segments=&origin=&acceptTC=1 [Assessed 30 August 2022]