What do the authors list as the advantages of involving users in the risk management process?

Security literature often portrays system users as the "weak link" in security, which cause vulnerabilities waiting to be exploited. With their study, Spears and Barki (2010) aim to provide evidence of an opposing view. Users could instead have a valuable role in security design, and if involved in the design process, can make a positive impact.

As a foundation for their study, the authors cite three underlying theories to explain how user involvement influences system success:

According to the *buy-in theory*, when users participate in the system design process, they are more likely to accept and adopt processes due to their psychological involvement. That is, by involving users in the risk management process, users are more inclined to accept the system and view processes as personally relevant (Markus and Mao 2004).

The *system quality theory* states that when users participate in the system's development, management and developers become better informed about business needs, which in turn results in higher quality and more successful systems (Markus and Mao 2004).

Last, the *emergent interactions theory* associates system success with relationships that develop between users and IS professionals when users participate in the development process. According to Markus and Mao (2004), the nature of these relationships has a direct impact on success. If there is a "good" relationship between users and developers, developers are more likely to consider business needs in the system design. However, a "bad" relationship that includes disputes and conflicts is more likely to result in a negative outcome (Markus and Mao, 2004).

Spears and Barki (2010) have found support for all three theories in a security context as well. Within their qualitative analysis, it was found that as users participated in security risk management, the topic became more relevant to their respective business processes. Organizational awareness of security risks and controls increased, and security controls were more aligned with the business context. Regarding the system quality theory, it was found that improvements were made in the design and implementation of IS security controls and their respective performance. Interestingly, control performance was found to be improved, not necessarily solely because of the users' knowledge, but because users were also being held accountable to perform assigned security tasks. Evidence of emergent interactions was also found at the staff level and at the senior management level. "New, or in some cases stronger, interactions between users and IS personnel had

been recently formed to manage IS security at all five companies." (Spears and Barki, 2010: 514).

As a takeaway, it is beneficial to involve system users with the risk management process. Decision-makers and security managers can utilise the domain and business expertise of the user base to further add value. User participation raises organizational awareness of security risks and controls within business processes, which in turn contributes to more effective security control development and performance.

Reference List

Markus, M. L. & Mao, J.-Y. (2004) Participation in Development and Implementation? Updating an Old, Tired Concept for Today's IS Contexts. *Journal of the Association for Information Systems* 5(11-12): 514-544.

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly* 34(3): 503-520. Available at: https://www.researchgate.net/publication/220259994_User_Participation_in_Information_Systems_Security_Risk_Management [Accessed 2 February 2021].