2013

A theoretical model for participation by stakeholders concerned with information security issues in systems development processes

Dale Kleeman
University of Canberra, dale.kleeman@canberra.edu.au

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

ACIS 2013 Principal Sponsor

A theoretical model for participation by stakeholders concerned with information security issues in systems development processes

Dale Kleeman
School of Information Systems and Accounting
University of Canberra
Email: dale.kleeman@canberra.edu.au

Abstract

After discussing the general issues with user participation in information systems development and aspect of user awareness with information security processes, this article raises a series of issues concerned with user participation with the information security aspects of the user requirements during information systems development processes. These issues are then developed into a theoretical model concerned with user participation in the elicitation of information security requirements during systems development processes. While most of these issues are known in the general systems development context, when they arise in the information security context, they are easily overlooked or neglected. The theoretical model and the associated issues presented are candidates further research work within the information security domain.

Keywords

Information security, user awareness, user participation, user requirements

INTRODUCTION

It is sometimes claimed that information security measures, implemented within information systems and business processes, are just another form of user requirements, in much the same way that the functional aspects of these systems and processes are user requirements (Baskerville 1993; Gerber and von Solm 2005). Increasingly, over time, within information systems practice we have been seeing users take a more active role in the specification and design of the functional requirements, but the same is often not the case for the information security measures. Information security is often perceived of as a technical problem during systems development and security policy formulation, where the major inputs to policy and requirements specification come from technical and information security staff – this security-centric approach frequently minimises the contribution from users in business areas, contrasting with this increased level of user involvement with the functional requirements.

Confidentiality, integrity and availability (CIA) of information are central to information security and this paper will take a broad view of the information security term, encompassing these elements as they play out with information and the associated systems and technology. Taking integrity as an example of these CIA elements, it is the users who need a certain degree of accuracy or completeness with the data in their systems in order to take the actions that they do with the outputs of these systems. The information security staff are rarely, if ever, acting on the functional outputs of these systems, so would have little appreciation for the degree of accuracy needed in the data, and consequently, would be very poorly placed to specify the requirements around this or any of the other components of integrity. Similar comments could be made in relation to the confidentiality and availability of information within these systems.

With this in mind, this paper presents a case for greater user involvement in specifying the requirements for information security measures. The paper will start with a brief look at the general issues around user involvement in systems development, and then follow this up with a discussion around information security related aspects of user involvement and awareness. This will then lead in to the development of a theoretical model concerned with user participation with information security issues within ISD projects. The model is currently work in progress, with the discussion identifying a range of issues that could be areas for further research.

USER INVOLVEMENT IN SYSTEMS DEVELOPMENT REQUIREMENTS

The issue of user involvement in systems development activities has been an area of major interest in IS research since the early days of the discipline (Barki and Hartwick 1989; He and King 2008; Hirschheim 1983; Iivari et al. 2010; King and Cleland 1971). An aspect of this interest is a concern with high rates of project failure, with one of the dimensions of this failure being poor understanding of user requirements (often because of poor user participation practices), and the developed system (if completed) not being what was required by the user

community. Deficiencies around requirements specification is now often claimed as the greatest single cause of failures of software projects (Hansen and Lyytinen 2010). This connection between some level of user participation and the elicitation of quality user requirements, or even more broadly, overall project success has been the subject of more recent IS research. As an example, Harris and Weistroffer (2009) survey much of the relevant literature in this area and use this to establish a strong connection between levels of user participation and project success.

In a meta-analysis of 82 empirical studies on user participation, He and King (2008) conclude "that user participation is somewhat beneficial in ISD" and "its effects on ISD attitudinal/behavioural outcomes were found to be significant and moderately strong in magnitude; its effects on productivity outcomes, albeit significant, were found to be limited with small effect sizes". They note, however, that "the overall modest effect of user participation suggests that user participation alone may not be sufficient to predict the success of ISD projects, especially when productivity outcomes are of research interest". They then conclude that this has "strong implications for ISD practitioners . . . if system acceptance is the ultimate goal, user participation should be designed to induce more psychological involvement . . . among potential users".

There is much complexity around the nature of user participation and what forms of participation are important within ISD and IT projects. This complexity ranges from issues around the nature of the participation effort through to the nature of the projects themselves, and includes the following factors:

- the nature of the user participation – this can range from simple involvement (such as just being consulted) through to more active participation (such as taking on project roles), and is also concerned with the types of activities and the amount of participation that this might entail;
- the level of expertise brought by the users to the participation context, and their degree of involvement;
- whether users are in-house or external to the organisation, the geographic distribution of users, and even just the overall large numbers of potential users in some projects, along with the diversity of requirements sources;
- the heterogeneous nature of some user communities, with some systems being used by highly diverse users, some with high level skills ranging down to others who may be quite IT-illiterate;
- the variety of systems developmental approaches and modes (in house, purchased, COTS-based developments, traditional versus agile, etc.) and the complexity of the system being considered;
- the increasing use of inter-organisational systems, and also the need for standardised systems within organisations and across multiple organisations such as franchises.

The broad issues with this area of research have been well summarised in a number of papers, including: Hansen et al. (2009); He and King (2008); Iivari et al. (2010); and Markus and Mao (2004).

Markus and Mao (2004) identify three main issues from the literature that had previously been identified as contributing to project success:

- ***buy-in*** by participants, where the psychological impacts of the participation leads to participants becoming more committed to the systems they have helped develop;
- ***system quality*** issues, where participation by users can improve the quality of the system requirements as specified; and
- ***emergent interactions***, where the good relationships potentially produced from the process are conducive to participants being more willing to share requirements information and developers being more willing to incorporate these requirements into systems.

In the discussion that follows, Markus and Mao explore a range of unresolved issues with each of these explanations and the possible implications of these issues on the IS participation theory and research. They then propose a new theoretical foundation with a series of propositions leading to a model depicting a range of emergent causal processes, elements of which are illustrated in figure 1 below.

In the discussion of this model (described in figure 1), they posit that, while there are causal relationships, as depicted on the diagram, these are "*neither necessary nor sufficient* for success . . . they are *not sufficient* for success, because good requirements are not always transformed into good products and good products are not always used with the hoped-for results . . . they are also *not necessary* for success, because it is sometimes possible for gifted (or lucky) developers to craft excellent solutions" (Markus and Mao 2004, pp. 537/8).

However the overall picture of user participation is not all positive, with He and King (2008) noting that a "growing body of qualitative research has identified possible obstacles, drawbacks, or even negative effects

arising from the practice of user participation, such as user-developer conflict, communication gaps, communication lapses, and increased ISD workload". This would suggest that there is a need for some caution with the view that all user participation in information systems development will produce useful outcomes.

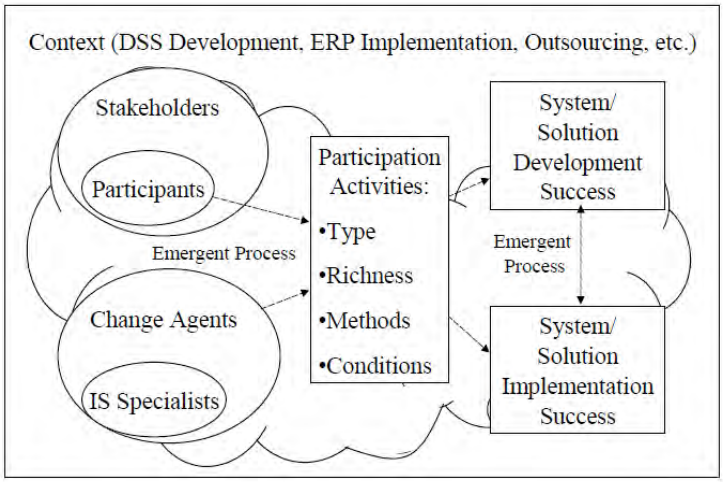

Figure 1 Updated IS Participation Theory elements (Figure 5, Markus and Mao, 2004, p 537)

Despite these reservations, it is clear from the body of literature in this area, that there is a substantive case for some level of user participation in establishing general information systems requirements, and within ISD projects generally.

INFORMATION SECURITY USER INVOLVEMENT AND AWARENESS

When considering the issue of user participation with information security issues within projects, and the potential for user-centric approaches, it is useful to look at broader user involvement in, and awareness of, information security. Most of the current references and texts deal with this mainly through the need for users to be aware of information security issues so that they can enforce the relevant countermeasures and detect various intrusions or breaches of security mechanisms. That is, they establish the key role of users as important participants in information security, rather than as designers of the security requirements. This is the main form of awareness promoted in some of the current texts such as Merkow and Breithaupt (2006); Slay and Koronios (2006); Volonino and Robinson (2004); Whitman and Mattord (2010); and Whitman and Mattord (2011).

Rainer et al. (2007) also note that managerial issues are high on the list of issues that information security professionals need to be aware of. They point out the need for business managers and information security professionals to move more toward each other on the spectrum – where business managers need to become more aware of information security technical issues and information security professionals needing to become more aware of business management issues. Despite this, they fail to deal with the question of whether business managers should be more involved in specifying information security policy and information security requirements for developing systems, as the primary focus in the article appears to be concerned with management support for information security including low funding and the justification for security expenditures.

Tracey (2007) makes a case for making security "the default thinking mode" in today's organisations and suggests that this can be accomplished through "including security in business decision-making process" and using organisational procedures to enforce this, but again, the emphasis appears to be mainly concerned developing a security culture that will help to improve the effectiveness of the existing security measures.

Siponen and Vance (2010) discuss the issue of employee's failure to comply with information security policies, and their application of neutralisation techniques as a means of rationalising this behaviour. Relating back to research in other areas where neutralisation techniques are applied (Greenberg 1990, as quoted in Siponen and Vance 2010), they suggest that seminars and education play a key role in inhibiting employees' attempts to use techniques of neutralisation, and use this to justify the need for employee education. The implication from this research is that user education needs to focus on the rationale underpinning the information security measures, so that the users are informed of: what the measures are that they need to comply with; how they work; and what they are meant to achieve with respect to the business processes that the users are engaged with.

This is connected to a debate that seems to have surfaced in some security circles related to the extent of transparency to users for any security measures. This is discussed in various papers, but Dourish et al. (2004) gives a good summary of the issues, with his definition of "transparency" being that security measures are

invisible to the users and with these users relying on assurances from their system administrators that their work will meet appropriate security standards.

Dourish et al. (2004) note that while transparent structures free the user of the need to understand the technical concepts behind the security mechanisms, they form the view that security mechanisms should be visible to the users as it allows them to "see how to manipulate their security environment when the unexpected happens or when a computer system requires troubleshooting". However, concerns may arise in situations where users lack the expertise to competently manipulate their security environment and, as such, may potentially leave themselves exposed to significant threats that arise from unintentionally leaving their security environment in a weakened state. This becomes quite evident in the discussion of a study (Whitten and Tygar (1999) as quoted in Dourish et al. (2004)) showing the difficulty users had in successfully using PGP software to encrypt/decrypt their email, but no resolutions to this problem are provided in the Dourish paper.

These arguments are further developed by DiGioia and Dourish (2005) where they note that "what 'secure' means at any given moment is a determination that only an end user can make" and that "attempts to make systems inherently secure, then, are problematic because they presuppose what 'secure' might be, taking that decision out of the users' hands". This "transparent" approach to security appears to be associated with security-centric approaches, and the implication in these two articles is that these approaches have problems that can lead to flawed security in many cases.

With these points in mind, this raises a question around the issue of user awareness of the security mechanisms operating in their environment. The questions that Dourish et al. 2004 were interested in related to users' perceptions of security and how they know systems are secure enough for them and their work. It seems that they would be unable to answer that question if their awareness of security in their environment was low, and in these situations they would be relying heavily on the assurances given by the technical experts that adequate protection mechanisms had been put in place. In addition, Siponen and Vance (2010) would also suggest that they are less likely to comply with security measures in these circumstances.

However, this brings up a conundrum – if the technical experts had not consulted with users about their security requirements, then it is likely that some users would be uneasy that the experts actually knew what levels of security were actually required, and thus would lack the confidence that these experts had provided appropriate levels of protection. Whereas, if the experts had consulted with users about their requirements then they would have a higher level of awareness than this minimal level noted above.

This suggests, that for some users at least, there is a need to have a reasonable level of awareness about security mechanisms in their environment and, as a minimum, this is likely to be partly developed through appropriate consultation mechanisms. It could be argued that the more involved users are in establishing their security environment, the more aware they will become of these issues, and thus, more confident that the environment will be properly constituted to meet their needs in this area. This involvement should be more with the higher levels of security requirements along with regular feedback against performance measures, than at a detailed technical specification.

To be involved at the technical levels would require significant technical skills that could only be gained through time consuming training activities and well beyond the level of effort most users would want to put into this activity. However, the higher level requirements specification and review activities could be achieved with much less effort on their part. In many ways, this is consistent with the specification of other, more traditional, elements of user requirements, where the users may not have, or even desire, the detailed technical knowledge for these specifications, but do want to be directly involved in their high level specification.

This broad discussion now leads to a possible theoretical model concerned with user participation with information security issues within information systems development projects.

A THEORETICAL MODEL OF USER PARTICIPATION WITH INFORMATION SECURITY ISSUES WITHIN ISD PROJECTS

In order to understand these issues, it is important that there is some discussion around what is meant by "improved information security outcomes". This discussion then leads into the elaboration of a range of aspects that relate to user participation in ISD projects. Each of these aspects produces a series of major issues that contribute to a theoretical model.

A reasonable definition of what is meant by improved information security outcomes in business processes would be the implementation of appropriate, cost effective information security countermeasures (or controls) that are commensurate with the levels of risks that the business process is exposed to. A range of measures can have an important impact on achieving these outcomes, including issues such as: the use of risk analysis practices to achieve an understanding across the organisation of the relevant risks; the establishment of requirements for controls to mitigate these risks, and the actual implementation of these controls; and the conformance with the

controls by the participants in the business process, this being connected to levels of awareness, senior management support, and having an appropriate security culture within the organisation.

A question arising from this is whether there is a relationship between well specified information security requirements, and business processes that have better information security outcomes. Associated with this, there is also the need to consider whether there may be trade-offs between efforts to specify the information security controls and the risk reduction this may promote.

User awareness

The earlier discussion on user awareness noted the connection between user awareness of information security measures (what they are, how they work, what they are meant to achieve) and improved information security outcomes. Spears and Barki (2010) establish some evidence of this connection between user awareness and more effective information security measures, noting the important role played by users in the implementation of these measures within business processes, and connecting levels of awareness with the effectiveness of the implementation of these measures. Spears and Barki also note that user participation in "security risk management" (SRM) has significant benefits for improving levels of user awareness. An implication that can be drawn from this is that user participation in the specification of information security requirements during systems development is likely to have a similar outcome with respect to user awareness.

The earlier discussion concerning application of neutralisation techniques by employees raised by Siponen and Vance (2010) is evidence of the important role played by seminars and education in inhibiting employees' failure to comply with information security policies. This user education needs to focus on the rationale underpinning the information security measures, so that the users are informed of what the measures are that they need to comply with, how they work, and what they are meant to achieve with respect to the business processes that the users are engaged with.

This first issue would appear to be well established by this evidence, but it is important to the overall theoretical model, so will be stated here.

Issue 1: Improving levels of user awareness of information security issues leads to improved information security outcomes. User should be made aware of what the information security measures are, how they work, and what they are meant to achieve.

Participants

When discussing participative practices for the development and specification of information security requirements, there is a need to consider who the actors will be in such processes, and what roles these actors will have in the various participation activities.

At the business process end of things, there are a range of users who would need to be considered as candidates for the participation processes:

- hands-on users – these may be internal (employees) or external to the organisation;
- managers in business process work areas;
- executive champions.

In relation to the executive champions, Markus and Mao (2004) make the point with respect to general systems development participative practices, that top management support is a form of user participation. The information security literature also establishes the importance of top management support for general information security outcomes. Examples of this include Volonino and Robinson (2004, pp. 57-59), and Smith and Jamison (2006). Both CoBIT 5 (ISACA 2012) and the ISO27000 series standards also put a strong emphasis on senior management involvement as being important to achieving appropriate information security outcomes. For example, managements' responsibility for the information security management system is noted in section 5.1 of ISO27001 and 6.1.1 of ISO27002. CoBIT 5 (p 22 of the framework document) has a list of important questions for those involved in governance, including "is the information I am processing well secured?"

With respect to the other, non-executive participants, information systems development processes will usually impact on many more stakeholders than can effectively participate in a development process generally, and specifically the development of the information security requirements. There are also situations where some of the stakeholders are just not able to participate, even if there was capacity to accommodate them in the processes – for example, many of the external stakeholders are not even identified at the time of the development. As any connection between participation in the process and the raising of user awareness of information security measures will be restricted to those who have actually participated at some stage, and that increasing levels of awareness are connected with improving information security outcomes, then there would need to be

consideration around the lack of participation for some of the actors in the business process, and how this situation might be remedied.

Noting that not all stakeholders will be selected for the various participation activities, there is then the question of which participants are selected, and also an issue of whether these will be "good participants". Should there be a combination of managerial and hands-on users? How will the issue of top management support impact on levels of participation, and on which participants are selected for the various participation roles in the project? Will the levels of top management support also impact on how seriously those selected take the participation activities?

Research in the general systems development context indicates that it is important to distinguish between operational and managerial users when it comes to participation related activities, and that their roles in the participation activities might be different, with consequent differing impacts on systems development success (Markus and Mao 2004, p 528; Barki et al. 2001). Markus and Mao (2004) (quoting Akkermans and van Helden 2002) indicated that "participation [by lower level staff] and top management support are mutually reinforcing tactics".

Translating this into the information security context raises a number of questions. Which end user participants should be selected for participation in information security related activities? What impact will top management support have on these activities and selection of participants, and will it improve the relationship between this participation and information security outcomes?

There is also the issue of subsequent evolution of the system, after implementation, and the potential impacts of staff turnover. Staff with useful levels of awareness will move on from the situation at some stage, and new staff will enter, where they have not had the opportunity to participate in the specification of the information security requirements. As a consequence, alternative approaches will be needed for these two groups of staff (those who are left out of the initial participation processes, and those who subsequently join a situation where they play a role with the business processes). This suggests that a useful output from the development processes may well be materials that could be used to support any ongoing awareness efforts.

Issue 2: Information security participation activities are more likely to result in improved information security outcomes when a greater number of stakeholders are involved in the process, and these stakeholder groups should include operational users and local management personnel from the affected business processes. Careful consideration is needed around the selection of participants for appropriate outcomes to be achieved.

Issue 3: Concern and interest by executive champions for information security issues will increase the likelihood of useful engagement with these issues by business process members (operation users and their managers) in any systems development effort. This interest will also increase the likelihood that those selected for the participation activities will take that role seriously.

Issue 4: Local managers from business processes can make an ongoing contribution to information security outcomes after implementation if they are supported by appropriate awareness and education materials produced during the development processes.

Business analysts

On the developer side of things, there are also issues. Should the normal systems developers, such as the business analysts (BAs) be undertaking all the participation work, or should an additional group of BAs with specific information security expertise be brought in to undertake the information security related work? The earlier discussion indicated that having two separate groups of BAs will lead to the separation of the information security requirements from the other requirements gathering processes, and will have a potential for reversion to security-centric approaches, where information security requirements are not considered mainstream, and user engagement around these issues is neglected. By having the one group of BAs doing all of this work, it will strengthen the case that these information security issues are normal mainstream issues, and that it is appropriate for users to engage with these aspects during requirements gathering.

A further issue also arises with this as to the approaches that are taken around participation practices, and the skills that the relevant BAs may actually have in the area of engaging in meaningful ways with the end users on information security issues.

Issue 5: Integrating information security requirements gathering into the normal work of business analysts will improve information security outcomes. Business analysts will need to have an effective process that enables them to explicitly focus on information security requirements during the requirements gathering process.

Types of involvement

General participation in systems development activities raises a question about the different types of involvement, with the possibility of different participation outcomes. These are enumerated in Markus and Mao (2004), and include:

- ***Solution design*** – participation in the various phases of the development lifecycle, such as requirements generation, design, development, and testing;
- ***Solution implementation*** – participation in post-development system implementation, such as acceptance testing, installation of the system and conversion activities, planning and execution of training, and post implementation evaluation of the system and its performance; and
- ***Project management*** – participation in various project management activities, such as project reporting, liaising activities, and undertaking the formal project management role.

Markus and Mao (2004) also make a significant note about the quality of the participation experience that is provided to participants, and their degree of psychological involvement in the participation activities. They illustrate this with the following example:

> *"One can participate in development either by responding in 20 minutes to a questionnaire about requirements or by joining an ERP system configuration team that meets full-time for many months. The level of personal investment in system development and implementation success is infinitely greater in the second case, as is participants' ability to influence system quality."* (Markus and Mao 2004, p 532)

They also go on to note that " 'true participation' involves the ability to make or influence design decisions . . . . which not all participation activities give equally."

Bringing this back to the information security context, particularly in the light of this statement, raises the question about whether participation in some of the development activities is likely to produce better information security outcomes than the participation in other activities. Markus and Mao (2004) assert that participation around solution design, particularly in relation to specifying requirements, is likely to produce outcomes related to system quality, whereas participation in solution implementation activities is more likely to produce outcomes with system acceptance. They also assert that:

> *"we believe that participating in a planning or decision-making role (e.g., designing training programs) provides a richer participation experience than participating in an operational role (e.g., training others or being trained)."* (Markus and Mao 2004, p 532)

While these participation practices still need to be considered in the general ISD context, some of these types of participation are not quite as relevant to the broader issue of information security and associated requirements gathering, and for this it is suggested that this could be limited to a number of key areas of participation, including:

- in the solution design area, information security requirements generation and (possibly) design;
- in the solution implementation area, acceptance testing of security requirements, conversion of data, the planning and execution of training, and post implementation evaluation of the system and its performance.

It is quite likely that any participation concerning information security issues in both of these areas will have an impact on information security awareness, however, the more that this is "true participation" involving the ability to influence decisions and to help with design, the more likely this will lead to outcomes with greater potential for buy-in, with a consequent reduction in the neutralisation behaviour as discussed by Siponen and Vance (2010).

Further consideration also needs to be given to the extent to which this participation in information security related activities should be integrated with other systems development participation activities. The broad context of information security requirements being a subset of other system requirements would suggest that these should be integrated to some degree, however, even within this integration, it is important that there is some explicit mention of the information security context, as this would be seen as being strongly connected to the process of raising awareness of these issues with the participants.

Issue 6: Information security participation activities should be integrated with other user participation activities, as much as is possible, however, it is important for information security to receive explicit attention during these participation activities.

Issue 7: The richer the information security participation activities, the more likely this will impact positively on overall information security outcomes. Participation activities are likely to be richer when participants devote

ongoing time to project teams and have the ability to influence decision making with respect to information security requirements and design.

Issue 8: The elicitation of information requirements is likely to be more successful when it is supported by an explicit process concerned with information security issues.

Choice of participation methods

There are a multitude of ways in which the participation of the various actors can be conducted, ranging from a simple process where the BAs ask the users about a range of requirements, including their information security needs, through to full blown participative practices, where some users play a very active role on the project team over a period of time. Given the comments above about integrating this effort with information security matters into the other efforts around user participation in a systems development, the nature of this participation should be broadly consistent with other project based participative practices, but a question could be asked about which of these practices is likely to lead to better outcomes with respect to the information security needs.

Marcus and Mao (2004) discuss a range of other factors around general participation methods, including the artefacts that are used to engage with users (for example, various prototyping techniques; and system design representations of a technical or non-technical nature) and issues around facilitation, location, and financial incentives for participation. All of these issues would also be relevant to some degree with the information security requirements.

This question of participation methods is perhaps even more significant in the information security context (as distinct from the functional requirements context), as participants and developers are likely to have a general lack of familiarity with information security issues and a possible inclination to leave these matters to the information security specialists. This would then have the potential for many important areas of information security to be easily overlooked in the event of a poor process.

As an example, anecdotal experience would indicate that when many people from a background other than IT or information security are asked about information security, they immediately think that this matter is just about access controls and confidentiality of information, with little perception that information security extends into others significant areas. If these perceptions are carried through into a process where participation around information security matters was poorly organised, then the outcomes of the process are likely to focus heavily on these issues of who can access what, and what information needs to be kept confidential, with a consequent neglect of other important issues.

Issue 9: Supporting business analysts dealing with information security issues with materials that identify all information security issues relevant to end users will facilitate the elicitation of more comprehensive information security requirements.

Issue 10: Processes concerned with participation in information security issues should be oriented around user engagement with the elicitation process. These processes should also recognise a multiplicity of interests among user groups and types (operational and managerial), and should be appropriate for the non-specialist information security knowledge of participants, focusing on non-technical aspects of information security.

The developed theoretical model

The preceding discussion can be used to represent these concepts diagrammatically by adapting the Marcus and Mao model presented in figure 1. Figure 2 shows the interrelationships between some of the key concepts that have been raised and is annotated with numbers for each of the issues that have been identified. This figure, together with the 10 issues that have been identified in the preceding discussion, represents a theoretical model to describe the relationships between participation by various actors in a systems development process, and improved information security outcomes that may arise as a result of this participation.

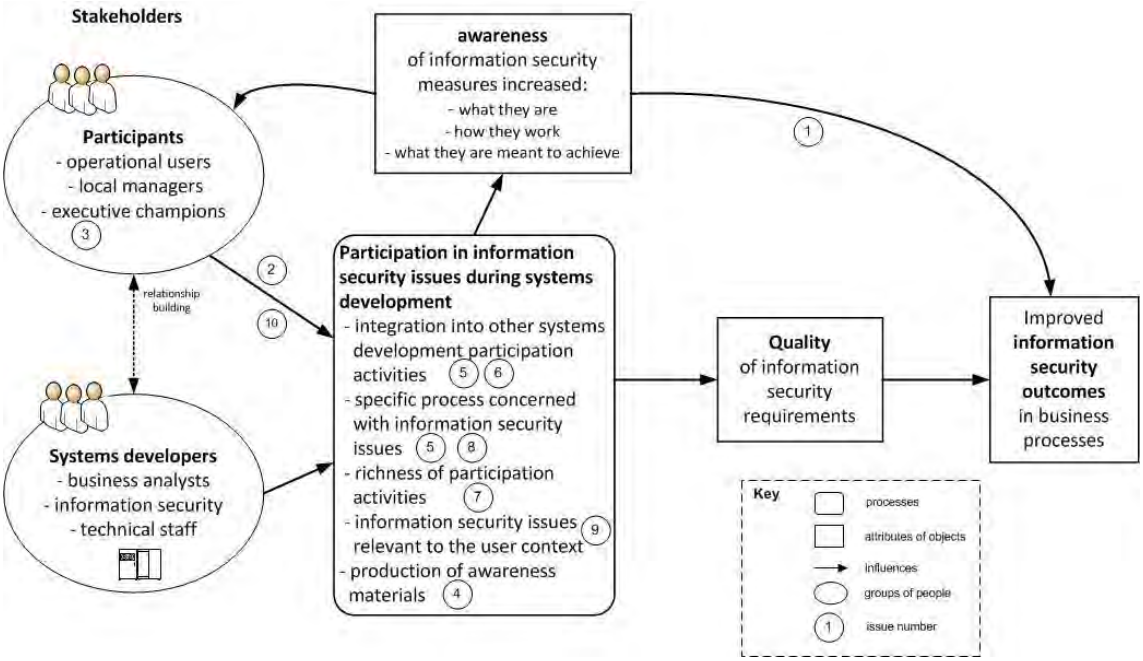

Figure 2: A proposed theoretical model connecting participation by stakeholders with information security issues in systems development situations to improved information security outcomes.

CONCLUSION

This article has raised a series of issues concerned with user participation with information security aspects of the user requirements during information systems development processes. While most of these issues are known in the general systems development context, when they arise in the information security context, they are easily overlooked or neglected. These issues are then developed into a theoretical model concerned with user participation in the elicitation of information security requirements during systems development processes. Some of these issues are already supported by existing research within the information security literature, while others are yet to be actively considered and are good candidates for further research work. As many of these issues are more qualitative in nature, it is likely that the research will need to be of a more qualitative nature, such as action research or interpretive case study.

A theoretical model has been presented and could be used as a basis for consolidating research effort into user participation into information security practices. Associated with this would be a further research question as to the extent to which users are prepared to spend time on such activities within an information systems development and security context.

REFERENCES

Barki, H., and Hartwick, J. 1989. "Rethinking the Concept of User Involvement," *MIS Quarterly*, March 1989, pp 53-63.

Barki, H., Rivard, S., and Talbot, J. 2001. "An Integrative Contingency Model of Software Project Risk Management," *Journal of Management Information Systems* (17:4), pp 37-70.

Baskerville, R. 1993. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys (CSUR)* (25:4), December 1993, pp 375-414.

DiGioia, P., and Dourish, P. 2005. "Social Navigation as a Model for Usable Security," in: *Proceedings of the 2005 symposium on Usable privacy and security*. Pittsburgh, Pennsylvania: ACM Press.

Dourish, P., Grinter, R.E., Flor, J.D.d.l., and Joseph, M. 2004. "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem," *Personal Ubiquitous Computing* (8:6), November 2004, pp 391-401.

Gerber, M., and von Solms, R. 2005. "Management of Risk in the Information Age," *Computers & Security* (24:1), pp 16-30.

Hansen, S., Berente, N., and Lyytinen, K. 2009. "Requirements in the 21st Century: Current Practice and Emerging Trends," *Design Requirements Engineering: A Ten-Year Perspective*, pp 44-87.

Hansen, S., and Lyytinen, K. 2010. "Challenges in Contemporary Requirements Practice," in: *43rd Hawaii International Conference on System Sciences (HICSS), 2010* IEEE, pp. 1-11.

Harris, M.A., and Weistroffer, H.R. 2009. "A New Look at the Relationship between User Involvement in Systems Development and System Success," *Communications of the Association for Information Systems* (24:42), pp 739-756.

He, J., and King, W.R. 2008. "The Role of User Participation in Information Systems Development: Implications from a Meta-Analysis," *Journal of Management Information Systems* (25:1), pp 301-331.

Hirschheim, R.A. 1983. "Assessing Participative Systems Design: Some Conclusions from an Exploratory Study," *Information & Management* (6:6), pp 317-327.

Iivari, J., Isomäki, H., and Pekkola, S. 2010. "The User–the Great Unknown of Systems Development: Reasons, Forms, Challenges, Experiences and Intellectual Contributions of User Involvement," *Information systems journal* (20:2), pp 109-117.

ISACA. 2012. *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT*. ISACA.

King, W.R., and Cleland, D.I. 1971. "Manager-Analyst Teamwork in MIS: Cooperation Vital in Systems Design," *Business Horizons* (14:2), pp 59-68.

Markus, M.L., and 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), pp 514-544.

Merkow, M.S., and Breithaupt, J. 2006. *Information Security Principles and Practices*. Upper Saddle River, New Jersey: Pearson, Prentice Hall.

Rainer Jr, R.K., Marshall, T.E., Knapp, K.J., and Montgomery, G.H. 2007. "Do Information Security Professionals and Business Managers View Information Security Issues Differently?," *Information Systems Security* (16:2), pp 100-108.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp 487-502.

Slay, J., and Koronios, A. 2006. *Information Technology Security & Risk Management*. Milton, Qld: John Wiley & Sons Australia Ltd.

Smith, S., and Jamieson, R. 2006. "Determining Key Factors in E-Government Information System Security," *Information systems management* (23:2), pp 23-32.

Spears, J., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *Management Information Systems Quarterly* (34:3), pp 503-522.

Standards Australia. 2006. *AS/NZS ISO/IEC 27001:2006 Information Technology - Security Techniques - Information Security Management Systems - Requirements*. Sydney: Standards Australia/Standards New Zealand.

Standards Australia. 2006. *AS/NZS ISO/IEC 27002:2006 Information Technology - Security Techniques - Code of Practice for Information Security Management*. Sydney: Standards Australia International/Standards New Zealand.

Tracy, R.P. 2007. "IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards," *Information Systems Security* (16:2), pp 114-122.

Volonino, L., and Robinson, S.R. 2004. *Principles and Practice of Information Security : Protecting Computers from Hackers and Lawyers*, (1st ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.

Whitman, M.E., and Mattord, H.J. 2010. *Management of Information Security*, (3rd ed.). Cengage Learning.

Whitman, M.E., and Mattord, H.J. 2011. *Roadmap to Information Security: For IT and Infosec Managers*. Boston, MA: Cengage Learning.

COPYRIGHT