Information Security Perceptions of Users, Levels of Engagement and Developer Resistance

Dale Kleeman
School of Information Technology and Systems
University of Canberra
Canberra, Australia
Email: dale.kleeeman@canberra.edu.au

Abstract

This paper reports on a case study considering the propensity for a range of stakeholders to engage with information security issues during a major development project as part of a project considering the user involvement with the elicitation of information security requirements. Also examined were the attitudes of IT managers and project team members.

The research found that many users have an interest in being involved with information security issue, but their concerns meant they would need to be supported during any information security requirements gathering process. While business areas were interested in being involved, there was resistance from developers and this would require careful management. It was found that most users had a simplistic view of information security, largely limited to issues around access privileges.

Keywords: information security; user awareness, user participation, user requirements

1 Introduction

Information security research and literature has generally followed the views from practice where users are frequently seen as a weak link in the implementation of information security measures and their role in the overall information security system should be minimised if possible. This is evident in information systems security development approaches, both in the research literature and in practice, where users generally do not have a role in the security requirements elicitation process. This situation appears contrary to the more general information systems development literature where participative practices have become commonplace.

This study recognises the critical role that users can play in information security, and reports on a case study concerned with the implementation of an Electronic Document and Records Management System (EDRMS) in a public sector organisation. Issues concerned with user involvement in the elicitation of the information security requirements were explored using interview and document analysis.

The main research question with this work looking at the EDRMS case study was to consider the propensity and willingness for a range of stakeholders to engage with information security issues during a major development project. The case study also examined the attitudes of IT managers and project team members to user involvement in information security and the nature of these perspectives, particularly as they impacted on participatory practices in the development and specification of information security requirements. Users perception of information security and the impacts of information security measures on their work were also considered.

The motivations for this work stem from the patchy record of information security awareness and education programs and the desire to explore whether engagement with user area staff during development can have an impact on outcomes in this area through increased buy-in to the resultant security measures and improved understanding by all stakeholders of security requirements.

2 Background and review of the literature

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 IS research. As an example, Harris and Weistroffer (2009) surveyed much of the relevant literature in this area and use this to establish a strong connection between levels of user participation and project success. It is not the intent here to fully survey these issues, except to note that they are also relevant to the elicitation of information security requirements.

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 user awareness of and involvement in 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 (2014); Whitman and Mattord (2017); and academic literature such as Safa et al (2016).

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. 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 with the emphasis being mainly concerned with

developing a security culture that will help to improve the effectiveness of the existing security measures.

Information security awareness and training has also been extensively explored with the view that outcomes for organisations are patchy, at best, with increasing numbers of breaches being reported, even in organisations with information security training and awareness programs in place (Mahfuth et al 2017; Alshaikh et al 2018). Alshaikh et al note that "this trend may indicate that many current security training and awareness programs are not as effective as they should be".

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. 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.

DiGioia and Dourish (2005) 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 raises a question around the issue of user awareness of the security mechanisms operating in their environment. The transparency 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.

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.

Kleeman (2013) proposed a model for participation by stakeholders concerned with information security issues in systems development processes with the suggestion that this would positively impact on user awareness and ownership of information security control measures. The buy-in ensuing from this participation would then help to overcome many of the compliance issues identified by Siponen and Vance (2010).

3 Research approach

This paper reports on case study work involving a project for the implementation of an EDRMS in a local public sector organisation with approximately 1000 employees. The project is referred to as the 'E-records project', and the system is called the 'E-records' system in this paper. The E-records project was considered from a case study perspective, where the processes around the implementation of the E-records system would be used as a vehicle to understand issues associated with user engagement with aspects of information security.

The case study was considered through a multifaceted approach, including:

- the collection and assessment of a range of documents relating to the project;
- the participation by the researcher in various project related activities, including steering committee meetings; and
- interviewing a series of people involved in the project, including project team members, IT managers, and representatives of a range of user areas.

Documents reviewed during the research effort with the E-records project included:

- documents relating to the initial funding and establishment of the project, including the business case and a statement of requirements;
- various tender preparation and evaluation documents
- steering committee progress reports;
- various outputs from the business analysis processes, including detailed analysis of the workflows around document processing and a range of 'workflow maps'.

The researcher also participated as a member of the Project Reference Group. This role on the Reference Group provided background to the project which enabled it to be seen as a suitable candidate for the research effort, and the selection of this project for the research effort was then discussed with the key players within the project before proceeding with the research activity. Staff consulted about this selection of the project included the head of IT Management, the project owner from within IT Management, and the Corporate Records Information Manager. After agreement had been reached around the selection of the project for the research effort, the ethics approval was received for the research project.

Interviews were conducted with a total of 18 staff members of the organisation. The interviews were conducted in a semi-structured manner with a range of concepts used to seed the conversation. Answers provided by the participants were then used to determine the direction and extent of the interview. After the collection of basic demographic data (gender, age range, nature of work position), the following themes were covered in most of the interviews:

- the extent of any general awareness of information security issues and knowledge of any relevant organisation policy and standards (such as AS4360 and the ISO27000 series);
- the extent to which participants had previously participated in specifying general functional requirements on ISD projects, and had previously participated in specifying information security requirements;
- an exploration around whether any information security measures have adversely interfered with the performance of any aspects of their work; and
- the desire and motivation to be involved in establishing information security requirements with future IT projects.

The interviews were recorded, transcribed and edited to provide the data for this analysis. They were then coded using a simple coding mechanism, with key issues from each interview tabulated and used for data analysis.

Interviewees have been identified with codes that represent the work area in which they were based. Staff from the ICT area were labelled ICT1-5; the finance department FN1-4; and the two other user areas AC1-4 and ST1-5.

4 Findings from the case study

This section describes the issues that have emerged from the analysis of the various documents and interview data. These issues have some interesting implications for information security practice in organisations. The major issues arising from the analysis that are reported on in this paper include:

- motivations of users to be involved with information security
- information security perceptions of users, and
- information security measures adversely interfering with the performance of work.

4.1 Motivations of users to be involved with information security

All of the interviews with staff from user areas produced useful comments on desire of users to be involved with information security issues during requirements gathering processes. It was clear from these comments that many users have an interest in being involved with information security issue, at least to some degree, but have significant limitations around time, and to a lesser extent, concerns about their expertise. This may mean that they would be happy to be involved to the extent of being consulted, but would be unlikely to want to commit significant amount of time to the process. Also, if the consultation processes had some formal structure to them – perhaps in the form of group workshops, with involvement driven by the more senior staff – then people would likely feel much more comfortable to be involved, in contrast to individual one on one involvement.

It was also clear from these comments that users would need to be adequately supported during any information security requirements gathering processes. If they were just asked 'what information

security measures do you want in your systems?' then it is unlikely they would be able to produce a comprehensive answer, or even feel confident that they were able to answer such questions. However, if there were supporting materials that outlined a range of measures (expressed at a relatively conceptual level) that were likely to be the kinds of information security controls relevant to a user context, then they would be much better placed to engage with this information security requirements gathering process.

Looking at other evidence around these issues, most interviews included questions about the desire and motivation of interviewees to be involved in establishing information security requirements with future IT projects and their willingness to be involved in workshops concerned with eliciting information security control requirements with the E-records system.

Interviewees provided a mix of responses when asked about their desires to be involved in establishing information security requirements with ten respondents expressing an interest or a strong desire to be involved, six respondents were not all that interested, one who was ambivalent about this, and one not responding to this question.

However, there was quite a different response to a question about whether the interviewees would be willing to participate in a one- to two-hour workshop facilitated by the researcher that would help with the eliciting of information security requirements around the implementation of the E-records system. With the 13 respondents from outside of the ICT department, only one said they were not interested in participating in these workshops and a few others expressed some concern about whether they knew enough in order for them to be able to make a useful contribution. Two other respondents expressed some reservations based on their time availability, but if the arrangements fitted in with their other priorities they were interested in being involved.

This indicates that there were some respondents who were not interested in being involved with specifying information security requirements, but were happy to participate in workshops that were mainly focussed on eliciting specific information security requirements. The interview data suggested this willingness to engage with the issues through the workshop process was a way of getting involved without being threatened, particularly around low levels of information security knowledge.

It was also quite clear that those with less desire and motivation to be involved with these issues were further down the hierarchy in the organisational structures. Those in more managerial positions, or those more connected with IT issues in their work generally, were more interested and motivated to be involved and saw the need for users to be involved with these issues.

There were a number of responses relating to the establishment of information security requirements that were of note:

- AC1, who had significant information security and project management experience, expressed strong views about the need to consult with user groups about a range of issues, including information security issues.
- AC4, who also had had some IT audit experience noted that 'security to me has always been just another requirement'.
- ST1, a manager from a business area, expressed a strong interest in issues around access controls and business continuity, and while he wanted to be involved in most of this, had low expectations that he could have a much influence over the business continuity of the E-records system. One of the comments he made was 'motivation stems from self-interest'.
- AC2 noted that she was probably not interested in being involved in establishing information security requirements but has 'sat there in awe at some of the decisions that have been made'.
- ICT5, a respondent from IT Management noted that he had significant previous involvement with establishing information security requirements with a range of IT systems and processes, but with respect to the E-records project, stated that 'I must admit I would probably be happy <not being involved> until I found that it prevented some functionality that I deemed necessary, or that it exposed me to a risk that wasn't acceptable'.
- ST2 noted that 'I liked being involved to the extent that I was, or am, but beyond that probably not' (due largely to workload and time factors). He subsequently talked about information security issues he was currently involved with around access to the student records system which suggested a much deeper level of interest.
- ST5, a lower level member of staff indicated that she was not all that interested in being involved, except with regard to some very specific issues. She gave the impression of being a bit overwhelmed by all of this.

- Some of the comments from the Finance area included FN1 saying: 'Yes, I think everyone realises that they are important, but I am sure they all think, crikey, I hope someone else picks up the ball with this and runs with it and gets the process in place. I don't think anybody here regards this as a trivial issue, but I suppose taking responsibility for it is another thing, but I think that has really been forced upon us now as a result of the audit findings, so it is something that we have to embrace'; and FN3 saying 'Really, really keen to be involved'.

4.2 User engagement with information security and developer resistance

It was evident from the work in this case study that user areas were generally interested in engaging with information security issues, but it was apparent that they had been given few opportunities to do this prior to the interviews being conducted. Two of the user areas considered in the study had already been through the requirements-gathering phase of the project prior to this point, where the general user requirements had been discussed with representatives from these areas and system specification documents produced. Comments made by interviewees indicated that information security was not a topic in the requirements-gathering process and this was confirmed by members of the project team.

The E-records project team expressed the view that allowing the users some degree of control over the access privileges of documents that they had lodged in the E-records system would provide them with an opportunity to engage with the information security issues at a local level, and this meant that it was not necessary to comprehensively deal with this issue during the requirements-gathering phase. This view was also clear when the workflow maps from these areas were examined (these documents contained the detailed outputs of the business analysis processes in these two user areas). There was little in these documents about information security other than some basic comments about access controls and many of the interviews also indicated that there had only been superficial consultation with user areas around information security and access controls within the E-records project if at all.

It was therefore clear from these user requirements documents and the discussions with representatives from these user areas that ICT had made critical decisions around many of these matters without any significant user area involvement. Elements of this were also evident in the interviews with ICT1, ICT2 and ICT3 – key members of the E-records project team. Other informal discussions with the E-records project manager supported this view. The consultation that had occurred related mainly to the basic issues around access controls, essentially concerned with who would have access to what data items, with little, if any consideration given to the overall access control policy and the process issues with the administration and maintenance of access controls over time.

To illustrate this matter, there were a range of policy issues where user input could have provided some useful benefits. One example was within the E-records system where there were questions about whether access security policy should be set by the group or the individual. This question arose in a number of the interviews and it was evident in project discussions and documentation that the E-records project team had made a decision about this without any user consultation.

This example can be demonstrated by an analogy to an academic situation where access to teaching materials may be at issue. In this situation an individual academic may wish to restrict access to the teaching materials used in delivering a teaching unit, whereas the academic's discipline group may have a view that all teaching materials should be made available to the other academics within the group. Views highlighting the relative importance of individual and group access were expressed during interviews with staff from a range of user areas.

This is likely to lead to a tension between the individuals' desires and actions, and what is potentially desired by the group. Without any active discussion around this issue within user groups, it is quite likely that no group policy would be set (which appeared to be the outcome within the E-records project). This could lead to a situation where individuals end up with the control to do what they want, and more often than not, limiting access to records under their control. Retrieving this situation subsequently to a group policy setting could then prove problematic.

While having local control of access does allow users to engage with aspects of information security, there is no doubt that individual access control settings are only a small part of the information security picture, particularly around administration and maintenance of these settings. Most user areas would be quite unprepared to deal with these issues once the system came online, leaving many of these issues to surface through use. Some of these matters could prove quite problematic to deal with after the fact, with a likely consequence of leaving the system with poorer information security

controls than would be desirable, or possible if these issues had been tackled during the development phase.

While it would be difficult to quantify the return on these efforts, it is likely that the relatively small additional effort in engaging with the users on information security issues during the requirements gathering phase would have produced significantly better outcomes with the information security measures following implementation. This engagement could have been easily integrated with discussions about other functional requirements.

A further example arose in the E-records implementation that illustrates aspects of this issue, particularly around the developers' reluctance to engage with users. There was a difference between the attitudes of the organisation's records manager and that of IT services to information access policies. Implementation of these views, one way or another could have a significant impact on whether information security measures impacted on users and their ability to do their work (as discussed below).

The records manager was of the view that users should start with access to everything, unless there is a case made around the need to restrict things (in which case they would be denied access to these things), whereas the development team approach was to only give access to anything where there was a need – essentially, a least privilege approach to access controls.

There also appeared to be a difference between how the records manager and other members of the E-records project team found out about requirements in these areas. The records manager appeared to have a greater sensitivity to the user perspective, whereas the E-records project team members appeared to be applying principles about this matter from their experience and had not consulted with the records manager or other relevant users.

While differences such as these will invariably exist with most projects, there did not appear be any structured process for resolving such differences. It was also apparent that the resolution of this problem, which was to implement the least privilege option, was likely to have been heavily driven by the opinions of the IT security function – a situation that often occurs when the lack of formal processes with these matters is evident.

These examples around the interactions between business analysts (and other members of the E-records project team) with users show a significant reluctance on their part to engage with users on eliciting information security requirements. The project manager also placed low value on outcomes from the proposed workshops intended to elicit information security requirements and is further confirmation of this developer resistance to user participative practices, particularly as they relate to information security.

Some of this resistance, particularly at the project manager level, could be attributed to the need to complete projects on time, and the perception that user participative practices are likely have an impact in this area, however, it was also apparent that there were perceptions that users generally had little knowledge of information security and were unlikely to make much of a contribution to appropriate information security controls. It was also evident that there were entrenched practices in this area, possibly driven by a lack of information security knowledge by business analysts. Changing these practices in this area could be problematic and may require careful management.

4.3 General perceptions on information security

In analysing and coding the interview data, consideration was given to how the various interviewees perceived the information security domain, and how they interpreted questions about information security.

It was clear that with almost all of the interviewees (from both user and IT areas), the immediate issues of concern when the topic of information security was raised was that of access controls, with a particular emphasis around who could have access to what data. Consideration of the broader aspects of access controls was rarely evident in the responses from any of those interviewed – this included the ongoing dynamics and administration around access controls (including process issues and the way in which access controls are implemented and modified). Within the information security domain, these issues are often seen as being as important as the initial decisions around who should have what level of access to the various data items.

Six of the interviewees broadened their view of information security to other areas, including data integrity and availability (the 'I' and the 'A' from the confidentiality, integrity and availability (CIA) model) when prompted by the interviewer. The emphasis here was mostly on the availability issue,

with a number of these interviewees directly impacted by an earlier incident when a critical system was unavailable for more than five days at a peak processing time, with this incident being referred to by some of the interviewees. This increased awareness is consistent with findings in the information security literature that one of the factors impacting on security awareness is experience with previous adverse events (for example, Smith and Jamieson 2006).

Only three of the interviewees demonstrated a very broad view of all of the elements of the CIA model without any prompting from the interviewer – these three interviewees included two senior staff from the IT area (ICT4 and ICT5) along with one user area respondent with a strong background in IT and information security (AC1).

On the whole, this did not mean that the majority of the interviewees were completely unaware of these other (non-access control related) issues, it was just that they did not automatically associate them with the information security domain, and potentially, in most cases, considered these other areas to be largely outside of the users areas sphere of influence, these being things that should mostly be left to the IT or information security experts.

It was clear from this discussion that users can have a simplistic view of information security despite the basic training on information security that most staff receive. While this is not surprising given their general lack of expertise with these matters, it can have an impact when business analysts are engaging with users around their requirements for information security. Supporting users with material that broadened these perceptions could prove helpful during an information security elicitation process.

4.4 Information security measures adversely interfering with the performance of work

Interviewees were also asked about whether any previous experience with information security measures had had adverse impacts with the performance of their work.

15 interviewees responded to questions on whether information security measures had interfered with their work in some ways and 12 of these interviewees noted a range of incidents where this was the case. In five of these interviews, the cases were relatively minor, with seven others noting significant incidents, with most of these being issues around access to data. It was also apparent that some information security measures were seen as an unnecessary hindrance and are sometimes only implemented because of external requirements and compliance factors.

With the other three interviewees who responded to this question, incidents of the opposite nature were noted. In these cases, the lack of security related measures had caused some issues with either their work or that of the organisations where they were located at the time. There was also some interest from some user area managers in improving elements of information security in order to allow for the implementation of a range of automated processes that had the potential to improve things, either for themselves or for the users of the services they provide. There did not appear to be any strong connection with the responses in this area and other facets of the data.

It is clear from the responses that there is a mixed view about aspects of information security with only a minimal association between the response and the role of the user in the organisation.

It is evident from this discussion that information security measures can impact on the performance of work, and this can sometimes create negative perceptions about such measures. There was also some evidence that those who had been involved in the implementation of information security measures had a more positive perception of such measures. While restrictive measures are necessary at times, engaging with users on their security requirements could be one way to raise awareness of these measures and help to counter negative perceptions about the impact of information security measures on the performance of work.

5 Conclusion

This paper has described the E-records case study and the information security issues that have emerged from the analysis of the data that was collected. The major issues arising from the E-records case study help inform the considerations around end user involvement in the elicitation of information security requirements and include:

Motivations of users to be involved with information security

Many users have an interest in being involved with information security issues, at least to some degree, but have significant limitations around time, and to a lesser extent, concerns about their expertise. It is likely they would be happy to be involved to the extent of being consulted, but would be unlikely to want to commit significant amount of time to the process. Users would also need to be adequately supported during any information security requirements gathering processes.

User engagement with information security during requirements gathering and developer resistance

Business areas are generally interested in engaging with information security issues, but opportunities to do this could be compromised by the resistance from developers to such processes. The relatively small additional effort in engaging with the users on information security issues during the requirements gathering phase could produce significantly better outcomes with the information security measures following implementation; however, developer resistance to these processes could be problematic and may require careful management.

Information security perceptions of users

Users generally had a fairly simplistic view of information security, which was largely limited to issues such as the allocation of access privileges. Supporting users with material that broadened these perceptions could prove helpful during an information security elicitation process.

Information security measures adversely interfering with the performance of work

It was clear that information security measures can impact on the performance of work, and this can sometimes create negative perceptions about such measures. While restrictive measures are necessary at times, engaging with users on their security requirements could be one way to raise awareness of these measures and help to counter negative perceptions about the impact of information security measures on the performance of work.

This series of issues that have arisen from this case study work stand as interesting findings on aspects of information security, and also have implications for information security practice.

6 References

Alshaikh, M., Maynard, S. B., Ahmad, A., and Chang, S. 2018. "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," *51st Hawaii International Conference on System Sciences (HICSS)*.

Barki, H., and Hartwick, J. 1989. "Rethinking the Concept of User Involvement," *MIS Quarterly* (13:1), pp. 53-63.

DiGioia, P., and Dourish, P. 2005. "Social Navigation as a Model for Usable Security," *2005 Symposium on usable privacy and security*, Pittsburgh, Pennsylvania: ACM Press, pp. 101-108.

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

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.

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.

Kleeman, D. 2013. "A Theoretical Model for Participation by Stakeholders Concerned with Information Security Issues in Systems Development Processes," *24th Australasian Conference on Information Systems*, Melbourne, Australia, pp. 1-10.

Mahfuth, A., Yussof, S., Baker, A. A., and Ali, N. a. 2017. "A Systematic Literature Review: Information Security Culture," *Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on*: IEEE, pp. 1-6.

Merkow, M. S., and Breithaupt, J. 2014. *Information Security Principles and Practices*, (2nd ed.). Pearson.

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.

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.

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.

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

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

Whitman, M. E., and Mattord, H. J. 2017. *Management of Information Security*, (5th ed.). Stamford, CT: Cenage Learning.

Copyright