December 2004

A preliminary study determine the role of organisational knowledge in computer security

Raj Gururajan
Murdoch University

Alan Thompson
Murdoch University

A preliminary study determine the role of organisational knowledge in computer security

Raj Gururajan[1] and Alan Thompson[2]
[1] Department of Information Systems, The University of Southern Queensland, QLD 4350
[2] Murdoch Business School, Murdoch University, Perth, WA 6150
email: gururaja@usq.edu.au

ABSRACT

Prior studies indicate that the application of organisational knowledge in computer security has potential benefits. Despite this, it appears that many organisations engage external consultants to develop their computer security policies. It appears that prior studies while supporting the concept of external security consultants to some extent in organisations, also question the effectiveness of such external expertise in terms of performance in computer security. This study examined the role of organisational knowledge in the management of computer security in organisations. A conceptual model based on Rivard et al (1997) was developed with seven constructs. An instrument with 30 questions was prepared and 19 organisations with security procedures were surveyed. The results indicate that there is a negative correlation between external knowledge and the use of policies and procedures, indicating that these policies are not well integrated with the requirements of organisations. Further, the outcome of the study also indicates that organisations are satisfied with the use explicit knowledge available in organisations for the development of computer security policies. In essence, this study concluded that currently the organisational knowledge has a limited role in computer security.

Key Words

Computer security, knowledge management and standards.

INTRODUCTION

In the past decade organisations have become significantly more reliant on computer supported information and communication systems. Higgins (1999) asserts that the role of computer security has a significant effect on organisational performance. Power (2002) claimed that computer security breaches in 2002 cost organisations in excess of US$100 billion in either lost revenue or direct costs. Studies indicate that eight out of ten organisations suffered financial loss as a result of their security breaches (Power, 2002). Higgins (1999) and Kee (2002) mention that due to technical advancement, the security breaches are becoming sophisticated, resulting in increased computer security procedures. A key factor identified by Brooks et al. (2002) as a reason why many organisations did not have effective computer security measures was that organisations often attempt to achieve a balance between cost and compliance. Organisations often find it difficult to justify the cost of a computer security expert and as a result Higgins (1999) argues that many organisations place a greater reliance on external standards and expertise when managing their computer security.

Brooks et al. (2002) state that the majority of organisations develop their computer security primarily based on external industry standards such as the Standard for Information Security Management[1]. While the implementation of AS/NZS ISO/IEC 17799 may require an organisation's internal knowledge and their security infrastructure, according to Kee (2002) and Brooks et al. (2002), an organisation's computer security may become weak if proper integration of security policies and the knowledge found in organisations fail to exist. Kee (2002) further argues that the lack of continuity between security policies and organisational knowledge has a negative effect on the quality of their computer security. Von Solms (1999) has similar sentiments while establishing a direct positive relationship between an organisation's explicit knowledge and the quality of the development of computer security recommendations, policies and mechanisms.

Although prior studies indicate that the application of knowledge management to computer security has the ability to realise considerable benefits to organisations in developing and managing their security, there is a lack of understanding of the various factors influencing their relationship (Goh, 2002; Higgins, 1999; Kee, 2002; Kwok & Longley, 1999; Von Solms, 1999). Therefore it can be argued that the ability of an organisation to improve their computer security by a more effective integration of organisation's knowledge might yield better understanding of

[1] The Standard for Information Security Management was originally AS/NZS 4444 but has been replaced by ISO 17799 which incorporates the international standard developed from BS 7799.

procedures needed to develop, implement and maintain computer security policies to combat security breaches. This has provided the impetus to this study.

LITERATURE REVIEW

The code of practice for information security management AS/NZS ISO/IEC 17799 [2] is an international codified standard applicable to Australia and New Zealand and is used by many organisations as a guide to develop best practices to develop information and computer security. While the standard has been validated through a process of industry review and approval, it appears that the standard is weak because it places a strong reliance on external computer security expertise rather than internal knowledge that can facilitate the same functions (Kee, 2002; Von Solms, 1999). Bhatt (2002) claims that organisations are currently facing extreme challenges because of the ill-defined flow of an individual's knowledge within an organisational context and hence has very little contribution to the development of the organisational objectives. Therefore, it can be argued that for effective management of security policies, organisations should consider their internal sources as well. Therefore, one would expect that, if organisations could streamline the knowledge flow, integrate existing knowledge in computer security procedures, then some of these security breaches could have been minimised.

Prior knowledge in the context of organisational procedures and controls is considered by Von Solms (1999) to support computer security. In order to realise an organisation's computer security related information flow, there should be an integrated approach to inter-organisational reporting systems. This can happen only when the knowledge in an organisation is properly understood and captured. Von Solms (1999) argues that such a process will support the organisation in integrating security compliance and decision making with their controls. Von Solms (1999) draws relationships between the computer security processes, policies and mechanisms and the organisational environment to establish a direct relationship between organisational knowledge and development of computer security related recommendations, policies and mechanisms. Smith (2001) states that organisations must recognise the value of knowledge that exists with employees and that this knowledge be converted to explicit knowledge. It is only from the existence of explicit knowledge that an organisation as a whole can benefit from the knowledge's ability to support improved decision making and problem solving. The approach taken by Smith (2001) was to consider the role of tacit and explicit knowledge within an organisational decision making and problems solving context. This can be applied to Computer Security as well.

Kee (2002), while claiming that a critical component in the development of computer security polices in an organisation depends upon external standards, also suggests that security weakness in organisations often occurs as a result of the inability to transform external standards into a viable organisational framework. The development of such a framework is dependent upon organisational knowledge and Kee (2002) suggests that there is a lack of conversion of existing organisational knowledge into security policies. Within this context Kee (2002) argues that computer security management framework in an organisation should facilitate the development, monitoring and control of the security policies in order for the organisation to achieve availability, integrity and confidentiality of information. Recognition of the roles of both tacit and explicit knowledge is essential to create organisational knowledge and improve their ability to utilise knowledge in support of decision-making. The conversion of tacit knowledge related to computer security procedures into explicit knowledge in organisations can provide better controls to combat security related problems.

The survey of computer security focused literature has provided a holistic view of how computer security functions within an organisation. From the review of prior research significant organisational computer security characteristics have been able to be identified. From prior studies, it can be argued that although organisations can be guided by external standards and expertise in the management of their computer security, these policies and procedures must be aligned with organisations infrastructure and knowledge (Goh, 2002; Higgins, 1999; Kee, 2002; Kwok & Longley, 1999; Schultze & Leidner, 2002). Significant processes within computer security rely on the ability of organisations to transfer knowledge in order to support effective decisions. Further, that this knowledge transfer process must be continuous and not only include traditional organisational knowledge but explicit expert knowledge. This knowledge management process in support of computer security can occur in the context of organisational management models (Kee, 2002; Kwok & Longley, 1999; Von Solms, 1999).

Despite the fact that external computer security standards and expertise provide a guide for organisations to manage their computer security, it appears they fail to provide a mechanism that links the security process to the

[2] ISO 17799 is considered complementary to AS/NZS 444.2:2000 Information Security Management, Part 2 Specifications for information security management systems (AS/NZS 7799.2:2000 revised).

organisational knowledge. The result is that often security policies, procedures and controls are implemented that are not strong and consistent. From a review of prior studies it appears that the application of knowledge management to computer security may provide considerable benefits to organisations in developing and managing their security. Therefore, this study raises the following question:

What is the extent of the role of organisational knowledge in computer security?

RESEARCH OBJECTIVES

The objective of this study is to develop a greater understanding of characteristics of the relationship of organisational knowledge and computer security in organisations. Although prior studies indicate that the application of organisational knowledge to computer security has potential benefits, it appears that management of this knowledge appears to be limited in organisations (Goh, 2002; Gore & Gore, 1999; Griseri, 2002; Holsapple & Joshi, 2000; Kee, 2002; Kwok & Longley, 1999; Schultze & Leidner, 2002). Although prior studies have considered the management perspective of computer security they have done so solely from a technical perspective and failed to recognise the broader organisational issues (Brooks, 2002; Kwok & Longley, 1999; Von Solms, 1999). In contrast, it appears that, prior research in knowledge management has traditionally focused on the management of knowledge within the organisational framework rather than towards organisational processes (Kreiner, 2002; Bhatt, 2002; Laszlo & Laszlo, 2002; Schultze & Leidner, 2002). Accordingly it appears that many managers have not valued organisational knowledge in organisational computer security as they have failed to recognise a clear integration between these two entities. Therefore, in can be inferred that there is lack of sufficient empirical studies to support a positivist[3] approach in examining the factors influencing the role of knowledge management in computer security.

From the review of prior studies it can be argued that organisations can be guided by external standards and benefit from computer security external expertise. However computer security procedures, the organisations infrastructure and organisational knowledge should be synchronised in order for the computer security to be effective (Goh, 2002; Higgins, 1999; Kee, 2002; Kwok & Longley, 1999; Schultze & Leidner, 2002). There is sufficient evidence to infer that computer security related processes rely on an organisation's ability to transfer local knowledge available in organisation among employees. Further this knowledge transfer process must be continuous and not only include traditional organisational knowledge but also explicit expert knowledge. Accordingly the research question raised in this study is warranted (Kee, 2002; Kwok & Longley, 1999; Von Solms, 1999). Prior studies indicate that the role of knowledge management in computer security is not yet well understood. Therefore the following hypothesis was developed to test the extent of the role of organisational knowledge in computer security:

H1: Organisation knowledge has a limited role in computer security.

This study has focused on the extent of the role of organisational knowledge in computer security and collected data through a quantitative approach.

INSTRUMENT DESIGN

The study of knowledge management and computer security as a combined discipline is a relatively new area and there are limited prior models or research frameworks available on which to base the design of this study. Therefore a new data model is required to develop the conceptual framework. The approach adopted to develop the new model was a *construct matrix* based on the prior study of Rivard et al. (1997). Rivard et al. (1997) developed a construct matrix based on key elements identified from prior studies. This process involved the integration of research criteria (questions) within dimensions of the study that were considered as appropriate constructs. In this study, a *computer security construct matrix* was developed based on the model of Rivard et al (1997). Similarly, a knowledge management *construct* matrix was developed to encompass key characteristics of knowledge management identified from prior literature. A total of seven constructs were designed. They are external computer security standards, computer security policy and procedures, computer security performance, organisational use of internal knowledge in computer security, organisational use of tacit knowledge in computer security, organisational use of explicit knowledge in computer security and organisational performance in the management of computer security through the

[3] Ashram (2002) states that a positivist approach is where a researcher accepts the orthodox scientific view and proceeds to analyse the issue from that standpoint. The positivist approach assumes that there is an objective truth existing "out there", which can be uncovered through the scientific method which measures relationships between variables using logic and statistics.

application of knowledge management. These seven constructs consist of a total of 30 questions. The seven constructs are developed as follows:

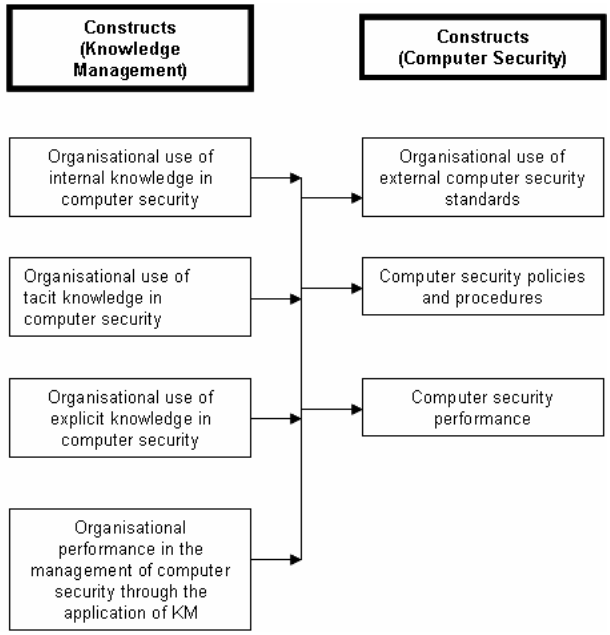
- **Construct 1** - External computer security standards (AS/NZS ISO/IEC 17799, 2001; AusCERT, 2003; Von Solms, 1999)
    - Organisational use of external IT security-related standards (Q1); The organisational development of computer security policies from external standards and guides (Q4); Organisational use of external computer security expertise for development (Q5); Organisational reliance on external standards to develop and manage computer security (Q20); Organisational reliance extensively on computer security expertise to develop and manage computer security (Q21).
- **Construct 2** - Computer security polices and procedures (Kee, 2002; Kwok & Longley, 1999; Shim et al. 2000; Von Solms, 1999)
    - Organisational use of computer security policies and procedures (Q2); Organisational documentation of computer security policies and procedures (Q3); **Construct 3** - Computer security performance (Kee, 2002; Kwok & Longley, 1999; Von Solms, 1999); Organisational computer security overall satisfaction (Q15); Organisational computer security policy development satisfaction ((Q16); Organisational computer security procedure and management satisfaction (Q17); Organisational computer security mechanisms development and management satisfaction (Q18); Organisational computer security measures development and management (Q19); and Organisational computer security is cost effective (Q14).

Knowledge Management Construct Matrix

The Knowledge Management Construct Matrix (KMCM) was developed from prior studies such as Arora (2002), Bhatt (2002), Goh (2002), Kreiner (2002), and Laszlo and Laszlo (2002). As there was no prior study in knowledge management with a direct reference or relationship to computer security the dimensions of the matrix were developed reliant on a theoretical framework and validation from the pilot study. The KMCM was designed based on four constructs of knowledge management and in turn included fourteen criteria (seventeen questions), namely:

- **Construct 4** - Organisational use of internal knowledge in computer security (Arora, 2002; Bhatt, 2002; Goh, 2002; Liebowitz & Wilcox, 1997; Von Solms, 1999)
    - Use of organisational knowledge in developing and managing computer security polices (Q7); Use of organisational knowledge in developing and managing computer security procedures (Q8); Use of organisational knowledge in developing and managing computer security mechanisms (Q9); Use of organisational knowledge in developing and managing computer security measures (Q10).
- **Construct 5** - Organisational use of tacit knowledge in computer security (Bhatt, 2002; Kreiner, 2002; Smith, 2001; Von Solms, 1999)
    - Organisational reliance on internal computer security expertise (Q6 & Q22); **Construct 6** - Organisational use of explicit knowledge in computer security (Allen, 2001; Goh, 2002; Griseri, 2002); Organisational use of knowledge management systems to facilitate their computer security (Q11); Organisational use of explicit knowledge to develop and manage computer security (Q23); Organisational use of explicit knowledge to develop and manage computer security policies (Q24); Organisational use of explicit knowledge to develop and manage computer security procedures (Q25); Organisational use of explicit knowledge to develop and manage computer security mechanisms (Q26); Organisational use of explicit knowledge to develop and manage computer security measures (Q27).
- **Construct 7** - Organisational performance in the management of computer security through the application of knowledge management (Bhatt, 2002; Griseri, 2002; Von Solms, 1999)
    - Organisations will improve their management of computer security through linkage of organisational knowledge and computer security (Q12 & Q28); Knowledge management systems will improve an organisations management of their computer security (Q13 & Q 29); and Knowledge management systems when applied to computer security will reduce costs for organisations (Q30).

The conceptual schema of this study was developed principally from the literature review. As limited prior study has occurred in the combined disciplines of knowledge management and computer security it is recognised that this study will be, to a degree, abstract in nature and therefore the conceptual framework of the study should be clearly articulated.



Conceptual Study Framework – Constructs

INSTRUMENT PREPARATION

The opinion survey has been developed to be subjective based on quantitative values. The survey has been designed to utilise a multiple scale technique, consisting of yes/no, frequency and Likert type scales. The frequency questions were based on a numerical scale structure that provides the respondents with the ability to select a value with a grouping criteria. The Likert Scale based questions were designed to support the respondent's to provide an opinion based response by selecting from a structured scale which includes: strongly disagree (SA), disagree (D), neither agree nor disagree (N), agree (A), strongly agree (SA) and not applicable (NA). The "not applicable" component of the Likert scale was included because it has been recognised that not all criteria within the survey instrument would apply to all organisations. To facilitate the data analysis a weighting was placed on all questions. Questions relating to the respondents organisation profile (QP1 to QP7) were allocated a sliding scale from 1 and higher relating to the number of responses assigned to the criteria. Questions eight to fourteen (Q8 to Q14) which yes/no styled questions were allocated values of one (1) for yes and two (2) for no. The remaining questions from fifteen to thirty (Q15 to Q30) utilised a Likert scales ranging in value from one to five respectively. All questions which were considered not applicable by the respondent were assigned a value of zero (0).

In excess of 100 survey instruments were distributed to select respondents of which 19 participated. The survey was conducted by both electronic and manual distribution and the responses from the organisations were performed anonymously. The approach taken for the administration of the study was duplicated from the pilot study. The distribution of the survey instrument was supported with the assistance of computer security focused associations and networks so as to assist developing not only sufficient response but such organisations and representatives that fall within the sampling technique criteria. The facilitating organisations were the Western Australian Information Security Special Interest Group (WAISSIG) and the IEEE Computer Society, WA Chapter.

Prior to administering, the survey questions were validated for appropriateness, relevance and reliability. The approach that has been taken for the validation of the survey instrument was to utilise both a peer review and pilot study techniques. The data samples have been collected through utilising a stratified random purposeful sampling technique (SRPST). During the survey instrument development and respondent sample selection, the possibility of error was considered and mitigated. The SRPST was selected as the most appropriate method for respondent

sampling as it was recognised to be suitable because respondent organisations considered in this study must have an acceptable level of existing computer security and their representative completing the instrument must also have an understanding of broader issues relating to the management of that security.

The survey instrument was based on thirty questions (items) designed from a combination of prior studies. The approach to determine reliability was to apply Cronbach's Coefficient Alpha test. This was applied to the questions of the overall instrument, constructs collectively and by constructs individually. The instrument for the thirty items returned an alpha of **0.7372**. Saunders (2003) and Zikmund (1994) state that this level although not high is an acceptable level for verifying repeatability for the instrument. Dooley (2001) argues that Cronbach's alpha will generally only return strong result for those items (questions) which are based on a scale response such as Likert type scales. Accordingly questions fifteen to thirty of the instrument were evaluated and returned an alpha of **0.8170**. Saunders (2003) and Zikmund (1994) state that this level demonstrates acceptable reliability. Therefore from the perspective of the reliability of the instrument items (questions) and construct design it can be argued that they are suitable for this study.

An issue recognised in the testing of the constructs is that they were developed from a limited set of prior literature and accordingly the data may be multidimensional. The internal consistency of each of the constructs individually was considered and an evaluation of the constructs returned values over 0.7740 to most constructs. The application of Cronbach's alpha to the individual constructs has demonstrated the reliability of constructs two, three, four, six and seven. Dooley (2001) argues that this reliability evaluation approach can often result in skewed results when the size of the data pool is limited. Due to the exploratory nature of this study, the results obtained were considered acceptable. Therefore it is assumed that the instrument used is free from error and is expected to yield consistent results[4]. The content validity was achieved through peer review. The peer review involved the solicitation of the evaluation of the survey instrument by colleagues to verify it for relevance, appropriateness, applicability and the use of scales of questions. The peer review was conducted to further refine the survey instrument prior to the second validation step, the pilot study. The peer review process involved the circulation of a draft survey instrument and covering peer review request to colleagues for instrument evaluation. A total of six peer review requests were completed and comments used to refine the instrument further. The survey instrument was considered to have strong content validity as the development of the survey was based on instruments already in existence such as the Australian Computer Crime and Security Survey and the Code of Practice for Information Security Management. The instrument question validity was strong with an alpha of 0.7372[5] and hence for the purposes of this study the content validity was considered appropriate.

DATA ANALYSIS

The descriptive analysis of the constructs was performed based on frequency distribution which considered the standard deviation, error of skewness and error of Kurtosis. Many studies choose to ignore such responses, usually called 'outliers', during the analysis of data because they may distort the analysis (Zikmund, 1994). For the purposes of this study the Empirical Rule was applied to ensure that the collected data was suitably allocated within the bell-shaped curve[6]. The data distribution for constructs one to seven had an acceptable level with the mean and hence for the purposes of this study constitutes a reliable distribution.

An analysis of the correlation of constructs was conducted in order to consider the role of organisational knowledge in organisational computer security. Although significant correlations occurred with Constructs 1 and 5 with other constructs they have been withdrawn from the study due to an inability to demonstrate reliability. Construct 2 which measured the use of computer security policies and procedures by organisations had a <u>significant negative correlation</u> with construct 6 **(-0.536**) which measured the use of explicit knowledge by organisations in managing their computer security. Construct 3 which measured computer security performance related to development, management and cost, demonstrated a <u>significant positive correlation</u> with construct 6 **(0.735**) which measured organisational use of explicit knowledge in the development and management of their computer security. Construct 4 which measured the use of internal knowledge by organisations in the development and management of their computer security showed no major correlation. Construct 6, apart from the identified correlations with constructs 2 and 3, showed no other major correlations.

[4] Constructs 1 and 5 did not yield high levels of reliability and therefore will be reviewed or removed from the formal study – Refer Appendix E for Pilot Study Construct Data Structure

[5] Note that questions 15 to 30 returned an alpha of 0.8170 – Refer Appendix D – Pilot Study Questions Reliability

[6] Traditionally referred to as the Normal Distribution Curve and refer Table 3.0 Main Study Construct Descriptive Statistics

The correlations of constructs 1 and 5 were not significant and hence they were not considered in detail in this study. Construct 1 that measured the use of computer security external standards and expertise by organisations in the development and management of their computer security, had a significant positive correlation (0.550) with construct 2, which measured the use of policies and procedures by organisations in managing their computer security. Further construct 5, which measured organisational use of tacit knowledge, had a significant positive correlation (0.486) with construct 7, which measured an organisation's performance in the development and management of their computer security. The implications of these findings are that it would appear that for those organisations who utilise external standards and expertise have a stronger application of computer security polices and procedures. Further, those organisations that have a stronger reliance on tacit knowledge tend to have a stronger organisational performance in the management of their computer security.

An analysis of the correlation of construct 2 and construct 6 (Refer Figure 1) clearly demonstrates a significant negative correlation. The data indicate that for those organisations that have a greater reliance on computer security policies and procedures do not utilise explicit (or documented) organisational knowledge to manage their computer security.

An analysis of the correlation of construct 3 and construct 6 (Refer Figure 2) clearly demonstrates a significant positive correlation. The data indicate that those organisations that have a greater reliance on explicit or documented knowledge have a stronger performance of their computer security.

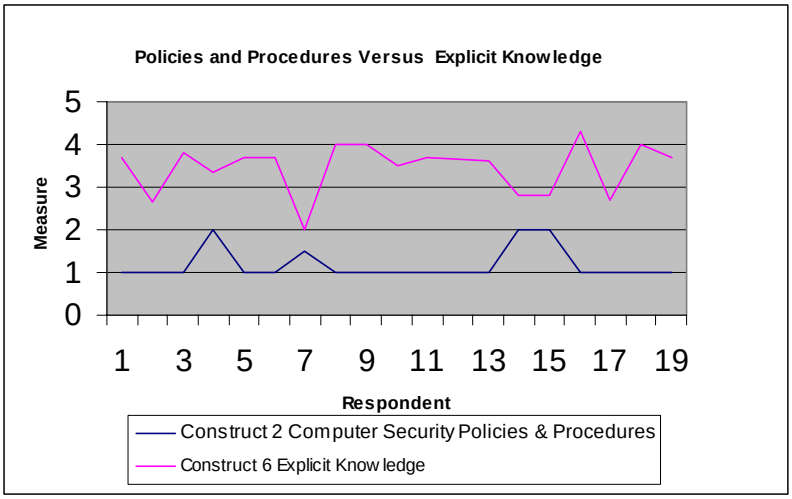


Figure 1 Correlation of Organisational Use of Polices and Procedures & Organisational Use of Explicit Knowledge in the Development and Management of Their Computer Security

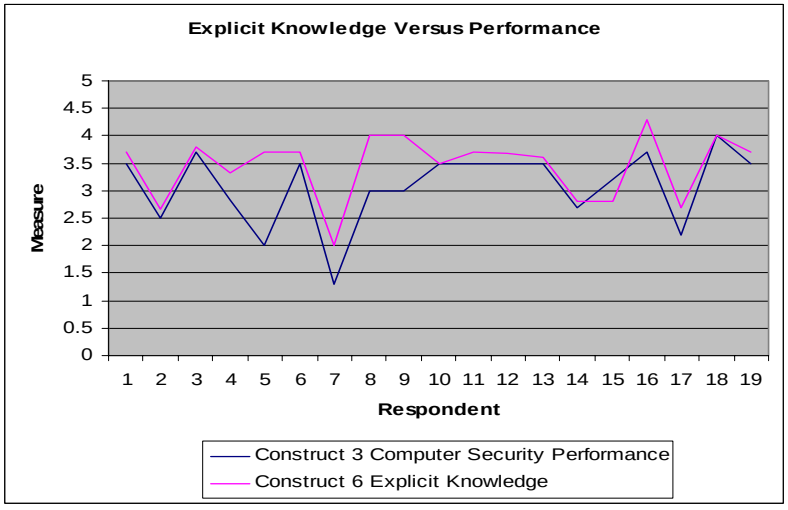


Figure 2 Correlation of Those Organisations Who Utilise Explicit Knowledge in the Development and management of Their Computer Security & Their Satisfaction with Their Performance of Their Computer Security

DISCUSSION

The analysis of the correlations of the constructs and supporting items (questions) has identified several significant factors and trends. The study found that those organisations using external expertise have a strong positive relationship with those organisations that utilise computer security policies and procedures. This is consistent with prior studies of Higgins (1999), Kee (2002) and Von Solms (1999) who argue that computer security standards are necessary to provide organisations with a structured framework of computer security polices and procedures. From the Australian Computer Crime and Security Survey it is argued that 43% of Australian organisations utilise external computer security standards. This is also consistent with the respondent demographics of this study which demonstrated that 50% of respondents utilised external computer security standards. A significant factor emerged in the study was that the organisations that utilised computer security polices and procedures had a significant negative relationship with those organisations that utilised explicit organisational knowledge. In other words, people in organisations felt that external expertise is necessarily productive in establishing security procedures. Therefore it could be asserted that those organisations which have a reliance on computer security policies and procedures which are derived from external computer security standards do not utilise organisational knowledge found in various documentations within the organisation in the computer security development and management process. This appears to indicate that external consultants, perhaps, 'sell' their solutions to organisations without actually studying the organisation. Further as no major correlation was realised between those organisations who utilised computer security polices and procedures with the use of organisational knowledge, it can be argued that no significant evidence exists to show that organisations utilise their local knowledge in the development and management of their computer security. This finding is new and needs detailed examination.

The study has demonstrated strong evidence to support that those organisations that utilise explicit organisational knowledge in the management and development of their computer security believed that they have a more satisfactory level of computer security performance. It should be noted that performance was not empirically measured in this study. Further, those organisations that utilise tacit organisational knowledge believed that their overall organisational performance in the development and management of their computer security is superior. This indicates that organisational knowledge plays a key role in computer security. In particular the evidence from these organisations supports that a direct linkage between organisational knowledge and their computer security through a knowledge management system would improve efficiency and reduces costs. Therefore it can be concluded that the application of knowledge management to an organisation's development and management of computer security can have a positive relationship and directly improve efficiency and reduce costs. For the purposes of this study the issue is, then, to what extent is knowledge management currently utilised by organisations.

From this study there was only indicative evidence that 20% of respondent organisations currently utilised knowledge management in the development and management of their computer security. It can therefore be asserted that, despite the positive influence of the application of knowledge management to the development and management of computer security, there was no significant evidence to support the major use of tacit or explicit knowledge by organisations in the development and management of their computer security. Therefore, the hypothesis for this study is considered accepted. Accordingly it can be affirmed that organisational knowledge has a limited role in organisational computer security.

STUDY IMPLICATIONS

The theoretical implications are that prior studies have more focus towards the technical aspects of computer security standards, policies and procedures and have failed to recognise the importance of both tacit and explicit knowledge within organisations. From a practical implication organisations would appear to have an opportunity to reduce their computer security costs and improve performance through an integration of computer security practices and organisational knowledge.

LIMITATIONS

This study is a preliminary study into the role of organisational knowledge in computer security and has been limited as only a few prior studies have been conducted within this discipline and therefore only limited prior information

was available for the purposes of developing this study. Although the study has in fact yielded strong results they are themselves limited by the minimal number of respondents. However the study is still considered acceptable both in design and outcomes as this is a preliminary study and has effectively achieved its objectives. Consideration should be given towards future research so that lessons learnt from this study can contribute to stronger data collection and applicability.

FUTURE RESEARCH

This study has identified a number of dimensions of the role of organisational knowledge in computer security that warrants further research. In particular it would appear that existing organisational practices which support the use of external computer security standards, associated policies and procedures are restrictive in nature to effectively engage the use of organisational knowledge. Given that this preliminary study has demonstrated that there is a strong argument for the application of knowledge management in order to improve an organisations development and management of their computer security, future research should focus on how existing standards and practices can be improved to allow for a stronger integration of computer security procedures with organisational knowledge through the application of knowledge management systems.

CONCLUSION

Although prior studies indicate that the application of knowledge management to computer security has potential benefits, there was limited prior study that directly dealt with this problem (Goh, 2002; Gore & Gore, 1999; Griseri, 2002; Holsapple & Joshi, 2000; Kee, 2002; Kwok & Longley, 1999; Schultze & Leidner, 2002). Although these prior studies supported external computer security standards and guides as foundations for effective organisational computer security, they only made recommendations as to how an organisation should develop and implement the security and failed to provide a mechanism that links the security process to the organisational knowledge. The result is that often security policies, procedures and controls are implemented that are neither strong nor consistent with the organisation's objectives. This study examined the role of organisational knowledge in computer security and concluded that currently organisational knowledge has a limited role in computer security. Although the role of organisational knowledge in computer security is currently limited, it appears that the application of knowledge management systems to organisational computer security development and management processes would enhance the performance and reduce costs of such practices.

REFERENCES

Allen, J. H. (2001). *The Cert Guide to System and Network Security Practices*. New York: Addison-Wesley.

Arora, R. (2002). Implementing KM - a balanced score card approach. *Journal of Knowledge Management, 6*(3), 240 - 249.

Arsham, H. (2002). *Topics in Statistical Data Analysis: Inferring from data*, from http://ubmail.ubalt.edu/~harsham/stat-data/opre330.htm, accessed on the 17th May 2003

AS/NZS ISO/IEC 17799. (2001). *Information technology - Code of practice for information security management* (International Standard No. AS/NZS ISO/IEC 17799). Sydney: Australian Standards International Ltd.

AusCERT. (2003). *Computer Crime & Security Survey*. Brisbane: AusCERT - Australian Computer Emergency Response Team.

Bhatt, G. D. (2002). Management strategies for individual knowledge and organizational knowledge. *Journal of Knowledge Management, 6*(1), 33 - 39.

Boisot, M. H. (1998). *Knowledge Assets: Securing Competitive Advantage in the Information Economy.* New York: Oxford University Press.

Brooks, W. J., Warren, M. J., & Hutchinson, W. (2002). A security evaluation standard. *Logistics Information Management, 15*(5/6), 377 - 384.

Dooley, D. (2001). *Social Research Methods.* New Jersey: Prentice Hall.

Goh, S. C. (2002). Managing effective knowledge transfer: an integrative framework and some practice implications. *Journal of Knowledge Management, 6*(1), 23 - 30.

Gollmann, D. (2001). *Computer Security*. England: John Wiley & Sons.

Gore, C., & Gore, E. (1999). Knowledge Management: The Way Forward. *Total Quality Management*(July).

Griseri, P. (2002). *Management Knowledge: A critical view.* New York: Palgrave.

Gunton, T. (1994). *A Dictionary of Information Technology and Computer Science*. England: Penguin Books Ltd.

Hair, J. J., Bush, P. R., & Ortinau, J. D. (2000). Exploratory Design. In *Marketing Research: A Practical Approach To The New Millennium* (pp. 214 -238). Singapore: McGraw-Hill.

Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. *Information Management & Computer Security*, *7*(5), 217 - 222.
Holsapple, C. W., & Joshi, K. D. (2000). An investigation of factors that influence the management of knowledge in organisations. *Journal of Strategic Information Systems*, *9*, 235-261.
Horwitch, M., & Armacost, R. (2002). Helping Knowledge Management Be All It Can Be. *The Journal of Business Strategy*, *23*(3), 26-31.
Kee, C. K. (2002). Security Policy Roadmap - Process for Creating Security Policies. *Sans Institute Electronic Library Available online at http://rr.sans.org/policy/roadmap.php Sourced on the 29th October 2002*.
Kizza, J. M. (2002). *Computer Network Security and Cyber Ethics*. London: McFarland & Company Inc.
Kreiner, K. (2002). Tacit management: the role of artefacts. *Journal of Knowledge Management*, *6*(2), 112 - 123.
Krutz, R. L., & Vines, R. D. (2001). *Mastering the Tem Domains of Computer Security*. New York: Wiley Computer Publishing.
Kwok, L. F., & Longley, D. (1999). Information security management and modelling. *Information Management & Computer Security*, *7*(1), 30 - 39.
Laszlo, K. C., & Laszlo, A. (2002). Evolving knowledge for development: the role of knowledge management in a changing world. *Journal of Workplace Learning*, *6*(4), 400 - 412.
Liebowitz, J., & Wilcox, L. C. (1997). *Knowledge Management and Its Integrative Elements*. New York: CRC Press.
Mugo, F. W. (2000). *Sampling In Research*. Retrieved 16/04/2003, 2003, from http://trochim.human.cornell.edu/tutorial/mugo/tutorial.htm
Power, R. (2002). CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends*, *8*(1).
Rivard, S., Poirier, G., Raymond, L., & Bergeron, F. (1997). Development of a Measure to Assess the Quality of User-Developed Applications. *The DATA BASE for Advances in Information Systems*, *28*(3), 44 - 58.
Saunders, M., Lews, P., & Thornhill, A. (2003). *Research Methods for Business Students*. Essex: Pearson Education Ltd.
Schultze, U., & Leidner, D. E. (2002). Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions. *MIS Quarterly*, *26*(3), 213 - 242.
Shim, J. K., Qureshi, A. A., & Siegel, J. G. (2000). *The International Handbook of Computer Security*. Chicago: Fitzroy Bearborn Publishers.
Simpson, J. A., & Weiner, E. S. C. (1989). *The Oxford English Dictionary*. Oxford: Clarendon Press.
Simon, S., Grover, V., Teng, J., & Whitcomb, K. (1996). The relationship of information system training methods and cognitive ability to end user satisfaction, comprehension and skill transfer: A longitudinal field study. *Information Systems Research*, *7*(4), 466-490.
Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of Knowledge Management*, *5*(4), 311 - 321.
Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50 - 57.
Zikmund, W. (1994). *Business Research Methods* (International Ed. ed.). Orlando, FL: The Dryden Press.

COPYRIGHT