WISP 2021 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

12-12-2021

The role of organizational competence on information security job performance

Joti Kaur
University of North Carolina Greensboro, j_kaur2@uncg.edu

Gurpreet Dhillon
University of North Texas

Winnie Ng Picoto
Universidade de Lisboa

The Role of Competence on Information Security Job Performance

Joti Kaur[1]
Information Systems and Supply Chain Management, University of North Carolina Greensboro,
Greensboro, North Carolina, United Sates

Gurpreet Dhillon
Information Technology and Decision Sciences, University of North Texas,
Denton, Texas, United States

Winnie Ng Picoto
ISEG, Universidade de Lisboa,
Lisbon, Portugal

ABSTRACT

Organizations invest manpower and resources to ensure that sensitive corporate data is secure in the hands of its employees. Information security policies of these organizations explicitly state responsibilities for employees. But there is a massive gap between employee security performance and understanding of their information security requirements. In this study, we explore the factors that can enhance information security job performance of employees within organizations. We argue that employee information security performance can be enhanced by developing organizational security competencies. We conduct the argument through a case study of a public sector bank in India. The in-depth case study allows us to develop a theoretical understanding of how different aspects of organizational competence allow organizations to come together to enhance information security performance.

Keywords: Competence, information security performance, tacit knowledge, explicit knowledge.

[1] Corresponding author. j_kaur2@uncg.edu +1 336 405 0892

INTRODUCTION

In recent times, there seems to be a general consensus that competencies within organizations play a vital role in the process of growth and achievement of competitive advantage for the organizations. These organizational competencies could include unique skills, technology or processes that help the organization utilize its resources to the maximum for growth and development. For instance, the organizational competencies of Walt Disney Corporation lie in organization's ability to tell a story using animation and design that has been perfected by the organization over the years. Hence, based on these competencies, Walt Disney has been able to compete and achieve sustainable competitive advantage. With the evolving trend towards information and data being one of the core assets possessed by organizations today, the demand for information security competence is on the rise. According to a recent report, information security skills and competencies are among the most in-demand skills for recruitment. The National Institute of Cybersecurity Education (NICE) also elaborates that information security competency of employees is crucial when it comes to organizational development. However, there is still a limited understanding of how organizations can enhance the security competencies of their employees. This is crucial as lack of these competencies can pose major security threats for the organization. This is evident for the fact that although organizations educate and train their employees on security best practices and have elaborate information security policies in place, organizations lost close to 6.3 billion USD due to security issues (2016 ACFE Report to the Nations).

Although many researchers have investigated the concepts of competence and resources, the conceptualization has not been deeply explored in the context of information security. McGrath et al. (1995), have explained the notion of competence emerging from an understanding of processes and skills relevant to the business. These competencies that include the skills and the know-how are acquired by employees and managerial groups through heedful interactions. Similarly, Weick and Roberts (1993) also illustrate that *know-how* and *know-that* result in a collective mindset through 'purposeful heedful interaction.' Following this body of literature, this study investigates the factors that enhance the overall information security performance of the organization by developing information security competencies of the employees.

While significant research has been done on information security policies (Crossler et al. 2019; Dhillon and Torkzadeh 2006; Posey et al. 2013), yet there is a gap in understanding how the information security performance of the employees can be improved. In this study, we explore the factors that could enhance information security job performance of employees through building better information security competence. In particular, we address the following research question:

RQ: *How information security job performance can be enhanced by nurturing information security competence?*

CONCEPTUAL BACKGROUND

Although prior studies have focused on the competencies at the organizational level, we explore the competencies of the individuals that are an integral component of the organization (Andreu and Ciborra 2009; Caldeira and Dhillon 2010).

Competence and Information Security Performance

The concept of competence has been well-researched in the literature (Appuhami 2019; Wade and Hulland 2004; Wißotzki 2018). Andreu and Ciborra (2009) postulate that capabilities and resources form an integral part of organizational routines. When employees and manager groups learn how to use these resources, they are able to develop efficient work practices that in turn helps the organization grow and develop. The concept of skills emerges when these routines and work practices are integrated into the routine of employees. These skills and knowledge result in the competence of the individuals and groups and involve not just *what* they do and *how* they do but also *for what* they do it. Researchers in the field of information security have extensively studied the importance of information security policies (Puhakainen and Siponen 2010) but *what* really makes the employees more competent and *how* their competence can be enhanced is still unclear. Extant literature recognizes that most employees are authorized to use or have access to some sensitive organizational information and data, and they may subsequently pose a threat to the organization if they are not competent to understand the security policies (Pahnila et al. 2007). Prior research has also focused on the evolving influence of employees' behaviors on an organizations' information security (Crossler et al. 2019; D'Arcy and Hovav 2007; Posey et al. 2014). However, not many studies have focused on understanding how information security competencies can enhance the performance of employees towards their information security responsibilities.

McGrath et al. (1995) explore the concept of competence and illustrate that individual know-how which corresponds to the skills that individuals and group members develop along with the understanding of the processes, can develop competence. This developing competence can be linked to a desired outcome that can be evaluated. In the context of knowledge-based IT competence, Bassellier et al. (2003) note that competence has two dimensions, namely *tacit* and *explicit knowledge*. Tacit knowledge involves an individual's experience and insights, whereas explicit knowledge includes access to codified knowledge and resources. Furthermore, Weick and Roberts (1993) state that 'purposeful heedful interactions' link the elements of individual know-how and know-that that are crucial for achieving organizational competence. This conceptualization of ‘purposeful heedful interaction’ is prevalent more so in the group dynamics where individuals interact with other group members to gain better knowledge, develop skills and understand the process better. This suggests the ‘collective mind’ of the members and links it to the desired outcome to be achieved through competencies. However, most of the researchers have overlooked these aspects in the field of information security performance.

Therefore, based on the conceptualization of competence and purposeful heedful interactions, we address the gap in the literature and argue that information security outcomes in terms of better security job responsibilities can be developed by enhancing competencies. Based on prior understanding on competence and performance, we argue that information security competencies can be assessed through the effective information security performance of the employees. The competencies in turn can be developed through the individual’s knowledge and heedful interactions.

RESEARCH METHODOLOGY

In this study, we use an interpretive case study approach to capture the factors that enhance the security job performance of the employees (Benbasat et al. 1987). We conduct in-depth interviews with employees of a public-sector bank in India, including branch managers, front-end staff, and IT executives.

The Case of a Public Sector Bank in India

Alpha (pseudonym) is one of the leading public sector banks of India. The bank has a network of 9300+ domestic branches, 11800+ ATMs serving over 120 million customers with 77000+ employees. The financial assets of the bank are worth USD 160 billion. The bank offers numerous digital banking services to its customers such as ‘Anytime and Anywhere’ banking and Telebanking. As a large organization with access to sensitive customer data, the bank has an elaborate Information Security Policy in place, which is reviewed yearly to keep pace with the technological developments. The Chief Information Security Officer (CISO) heads the Information Security Committee and reviews the Information Security Management Systems' performance. With regard to information security of the sensitive data that the bank has access to, the bank has detailed responsibility for every person within the bank that is part of the performance of the internal employees.

Analyzing Security performance in Alpha Bank

Our case study was carried out in a public sector bank where employees handle sensitive and financial information of its customers as well as of the organization. As an organization, the bank has outlined performance responsibilities for 'information owners' and 'information custodians' that includes maintaining the accuracy, completeness, and integrity of the information. The bank evaluates the outcome of employees' information security responsibilities regularly to avoid potential information security breaches and incidents. The in-depth case study of Alpha Bank presents some interesting aspects that contribute to and are critical for enhancing information security outcome of the employees. In Table 1, we present a few sample responses from the qualitative interviews.

Table 1. Sample interviews

Emergent Concepts	Definition	Interviewee	Sample interview quotes
Tacit knowledge	The knowledge is embedded through experience and insights - (Knowing-how)	Branch Manager	*"…employees who come with first-hand experience in information security somehow are able to deal with customer information and queries more effectively…"*
		Retail banker	*"…I generally reach out to my colleague who have experience in dealing with the issues that I face regarding customer information and data…"*
Explicit knowledge	The knowledge is codified and recorded so it	Bank Operations Manager	*"…We ensure that at a branch level, all the employees have access to the security policies and responsibilities so that each individual is*

	can be shared - (Knowing-that)		*sure of what and how to comply with…”*
		Information Security Officer	*“…Regardless of the job and designation, employees are more clear about their responsibilities through the security policy statements that are also updated regularly…”*
Purposeful heedful interactions	When facts and knowledge are communicated and incorporated into the group's collective mind	Regional Manager	*“…I have found that branches with best performance work as effective groups where the managers interact with their subordinates on a regular basis and have daily huddle sessions…”*
		Loan Officer	*“…I have personally learned the most about the details of my organization's security policies by interacting with other colleagues and my manager…”*

Given our goal to better understand the components that enhance the information security performance of the employees, we observed that employees who had past knowledge and skills of handling sensitive information were more confident of their competence to perform their information security responsibilities designated by the organization. Furthermore, the more access the employees had to the codified security policies of the organization, the more competent they felt. Interestingly, the answers of the interviewees also indicated that when the security policies and guidelines and discussed and communicated among the group members, there is higher sense of competence among the members. These interactions among the different level of group members enriches the knowledge and skills of the employees. The managers also pointed out that competent employees are more responsible towards their responsibility of keeping the data and information secure and following the security norms.

Consistent with the interview responses, employees feel more confident and assertive when the security responsibilities are communicated to them through formal or informal ways (Williams and Anderson 1991). These interactions also result in improving not just the know-how and skills - tacit knowledge - of the employees but also helps them better conceptualize the process of keeping the information secure through explicit knowledge (Puhakainen and Siponen 2010). This leads to employees feeling more competent about their information security responsibilities.

Furthermore, the employees with tacit knowledge will be able to show better information security competence based on their previous insights and skills developed through skills. Explicit knowledge that is based on the codified knowledge also encouraged employees to be more competent towards their security performance (Bock et al. 2005). Finally, enhancing and improving competencies has strategic and transformational impact (Dhillon 2008; Fonseca and Picoto 2020).

Based on the initial analysis of the case study, we propose the conceptual model as presented in Figure 1.

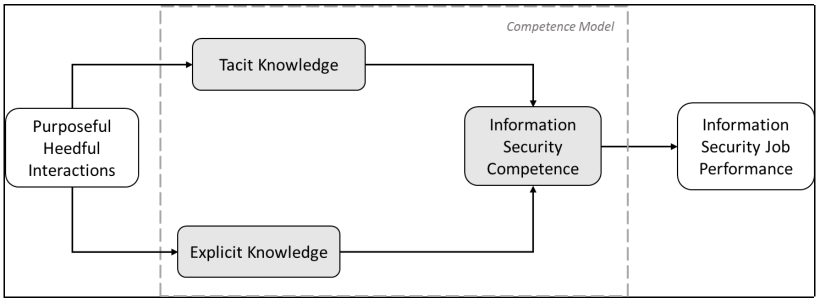
Competence Model
Tacit Knowledge
Purposeful Heedful Interactions
Information Security Competence
Information Security Job Performance
Explicit Knowledge

Figure 1. Conceptual Model

FUTURE DIRECTIONS

Based on the theoretical conceptualization of organizational competence (McGrath et al. 1995) and purposeful heedful interactions (Weick and Roberts 1993), we explore the factors that can enhance information security job performance within organizations. Through an in-depth case study and our initial analysis, we build our conceptual model depicting that purposeful heedful interaction, and tacit and explicit knowledge can improve information security competencies for an organization. These improved competencies lead to a security outcome - in the form of better information security job performance of the employees – that boosts the overall information security performance of the organization. As a future research direction, it would be useful to empirically test our conceptual model.

REFERENCES

ACFE. (2016). "Report to the Nations on Occupational Fraud and Abuse". Retrieved from: https://www.acfe.com/rttn2016/resources/downloads.aspx

Andreu, R., and Ciborra, C. U. 2009. "Organizational Learning and Core Capabilities Development: The Role of It," in *Bricolage, Care and Information*. Springer, pp. 189-205.

Appuhami, R. 2019. "Exploring the Relationship between Strategic Performance Measurement Systems and Managers' Creativity: The Mediating Role of Psychological Empowerment and Organisational Learning," *Accounting & Finance* (59:4), pp. 2201-2233.

Bassellier, G., Benbasat, I., and Reich, B. H. 2003. "The Influence of Business Managers' It Competence on Championing It," *Information Systems Research* (14:4), pp. 317-336.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, pp. 369-386.

Bock, G.-W., Zmud, R. W., Kim, Y.-G., and Lee, J.-N. 2005. "Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate," *MIS Quarterly*, pp. 87-111.

Caldeira, M., and Dhillon, G. 2010. "Are We Really Competent? Assessing Organizational Ability in Delivering It Benefits," *Business Process Management Journal*.

Crossler, R. E., Bélanger, F., and Ormond, D. 2019. "The Quest for Complete Security: An Empirical Analysis of Users' Multi-Layered Protection from Security Threats," *Information Systems Frontiers* (21:2), pp. 343-357.

D'Arcy, J., and Hovav, A. 2007. "Deterring Internal Information Systems Misuse," *Communications of the ACM* (50:10), pp. 113-117.

Dhillon, G. 2008. "Organizational Competence for Harnessing It: A Case Study," *Information & Management* (45:5), pp. 297-303.

Dhillon, G., and Torkzadeh, G. 2006. "Value-Focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16:3), pp. 293-314.

Fonseca, P., and Picoto, W. N. 2020. "The Competencies Needed for Digital Transformation," *Online Journal of Applied Knowledge Management (OJAKM)* (8:2), pp. 53-70.

McGrath, R. G., MacMillan, I. C., and Venkataraman, S. 1995. "Defining and Developing Competence: A Strategic Process Paradigm," *Strategic Management Journal* (16:4), pp. 251-275.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly*), pp. 1189-1210.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & Management* (51:5), pp. 551-567.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly*, pp. 757-778.

Wade, M., and Hulland, J. 2004. "The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research," *MIS Quarterly*, pp. 107-142.

Weick, K. E., and Roberts, K. H. 1993. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative science quarterly*), pp. 357-381.

Williams, L. J., and Anderson, S. E. 1991. "Job Satisfaction and Organizational Commitment as Predictors of Organizational Citizenship and in-Role Behaviors," *Journal of Management* (17:3), pp. 601-617.

Wißotzki, M. 2018. "The Notion of Capability in Literature," in *Capability Management in Digital Enterprises*. Springer, pp. 27-39.