An Activity Theory Analysis of Factors Influencing Information Security Practices in Software Organisations

Gloria E. Iyawa[1]*, Tulimeveva K. Mufeti[1]

[1]Department of Information Systems, School of Computing, University of Namibia

Received: 11th June, 2015. Accepted: 18th March, 2016. Published: 15th August, 2016.

Abstract

Information is an asset to any organisation. As a result, different organisations strive to ensure that information is well protected. This has led to organisations creating information security policies. Despite this approach, employees play a vital role to ensure that these policies are implemented. Information security has been studied in different contexts. However, in the existing literature, there is limited research which investigates the factors that influence information security practices in the context of software organisations. Similar to other business contexts, information is an important tool within software organisations. The purpose of this study was to investigate the factors that influence information security practices in software organisations using a Namibian software organisation as a case study. The use of Activity Theory as a lens helped to investigate the factors that influence information security practices in software organisations which are often overlooked. From the analysis of the findings, it is evident that factors such as employee structure, work context, information sensitivity, reputation, responsibility, accountability and policies influence information security practices in software organisations. The findings revealed that information security policies have to be enforced at different levels and units in software organisations. The findings from this study may assist software organisations when implementing information security policies.

Keywords: Information security; software organisations and Activity Theory

ISTJN 2016; 8:61-72.

*Corresponding author: E-mail: gloria.iyawa@gmail.com (G. E. Iyawa)

1 Introduction

With rising threats to organisations and their information systems, the need for information security has increased. Information security is a topic that has gained popularity in organisations (Payne, 2003; Kruger, 2006; Show, 2007; Herath and Rao, 2009; Khan et al., 2011; Aloul, 2012). Theoharidou et al. (2005) posit that information security encompasses three major areas: confidentiality, integrity and availability. This means that information within any organisation has to be accessed only by authorised persons, while ensuring that information content has not been manipulated, and at the same time, accessible when needed, without which information security is incomplete.

Software development is the process of developing software applications which capture the business processes of an organisation. In this process, sensitive customer information regarding customers' business processes is left in the possession of the software organisations. In most cases, software organisations are required to provide application support services after software applications have been deployed, and hence, software organisations are committed to take charge of important customer information. Buse and Zimmermann (2012) also explain that information is an important tool in the software development process. For this reason, information kept in the possession of software organisations should be protected.

Information security has been discussed in different contexts (Bonnette, 2003; United States General Accounting Office, 1999; Hong et al., 2003). Although there is an increasing number of studies focusing on software security (Mouratidis et al., 2005; Halkidis et al., 2006; Yang et al., 2012; El-Hadary and El-Kassas, 2014), there is little research which establishes the factors that influence information security practices in software organisations. Furthermore, the problem with previous studies is that they do not emphasise activities carried out by employees which influence information security practices in software organisations.

The main purpose of this study was to investigate the factors that influence information security practices in software organisations using a Namibian software organisation as a case study through the lens of Activity Theory. This study therefore contributes in two folds, theoretically and practically. Theoretically, this paper contributes to the body of literature which investigates the factors that influence information security practices in software organisations. Practically, the factors identified in the study can be used as a guide to improve information security practices in software organisations.

The paper is structured as follows, the research approach is presented in section 2. Data analysis is done through the lens of Activity Theory in section 3. The findings from the data analysis are presented in section 4. Section 5 concludes the study.

2 Research approach

In order to achieve the main purpose of the study, the qualitative research method was adopted. Nicholls (2011) explains that the findings of a study can be analysed in-depth when qualitative methods are employed. The qualitative research method is appropriate when a study seeks to answer the ”what, how, why” of an event (Patton and Cochran, 2002). In a bid to understand ”what factors influence information security practices in Namibian software organisations”, the qualitative method was adopted.

Yin (1989: 23) defines a case study as ”an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used”. The case study approach is appropriate for this study as it aims to understand the activities which take place within the real-life context of software organisations. Wu and Chen (2005) explain that ”...interpretive research establishes the meaning of texts and arrives at an understanding of the phenomenon to which it implicitly refers”. The study also adopts the interpretive approach as it seeks to investigate the factors that influence information security practices in Namibian software organisations.

The interview technique is an appropriate data collection method in qualitative studies (Al-Busaidi, 2008). From Wu and Chen’s (2005) argument, interviews allow the researcher capture ”rich descriptions” for the study in which they undertake. For this study, the data collection technique used was the semi-structured interview. The organisation used as a case study is a Namibian software organisation, Solitaire Software Company (pseudonym). Solitaire specialises in the development of software applications. Permission was granted by the organisation before any information was gathered.

Twelve employees from different departments (software engineering, network engineering and business department) were purposively selected and were interviewed individually. The interviews were recorded and subsequently transcribed. Data was analysed from individual interviews. For referencing, the structured approach is as follows:
numberOfinterview_genderOfinterviewee_departmentOfinterviewee_lineNumber. For example, the first interview in which the interviewee is a female employee from the department of network engineering, texts form line 1 to 6 will be referenced as follows: 1_F_NE_1-6.

The study was underpinned by Activity Theory. Activity Theory was used as a lens to investigate the factors that influence information security practices in the organisation. This approach was adopted by Shaanika and Iyamu (2015) in examining how enterprise architecture can be deployed in the Namibian government. Odejide and Iyamu (2012) also used this approach in examining the factors influencing deployment of risk management systems in organisations. Moloi and Iyamu (2013) adopted this approach in examining the deployment of competitive intelligence.

3 Data analysis: The Activity Theory view

Activity Theory, according to Engeström (2001), comprises of six constructs which are subjects, objects, tools, rules, community and division of labour. Activity Theory is an analytical framework which uses activity as a unit of analysis (Morf and Weber, 2000). Activity Theory posits that activity is "primary" (Morf and Weber, 2000:81). The key application of Activity Theory in this study is the emphasis on human activities and how these activities influence information security practices in software organisations. The next section describes how these constructs are linked to the activities of Solitaire Software Company, which include the roles and responsibilities of subjects, objects, tools, rules, communities and divisions of labour in the organisation.

3.1 Subjects

Subjects in Activity Theory are participants in the study who engage in different activities (Engeström, 2001). In the organisation, subjects are employees who take the role of software engineers, application consultants and network engineers. These subjects engage in one activity or the other. The organisation is comprised of employees at different levels which include employees from junior to senior levels. For example, the software engineer position comprises of intern software engineers, trainee software engineers, junior software engineers, intermediate software engineers and senior software engineers. According to one of the interviewees "... our levels are different, the position of a software engineer can come in many forms, for example, intern software engineer, junior software engineer and senior software engineer. Interns are the lowest in rank, this group of employees have to move up the ladder from intern, trainee, junior, intermediate and then to senior staff depending on the level of experience they have acquired" (1_M_NE_5-9).

Employees (subjects) perform activities within the organisation. For example, it is the duty of application consultants to communicate with customers regarding business processes which are to be incorporated in software applications. It is the duty of software engineers to translate these processes into software programs. One of the interviewees stated "It is our duty to interact with the customers and gather information regarding their business processes and afterwards we inform the software engineers" (3_M_B_6-7). It is the duty of network engineers to resolve technical issues regarding cabling and network connections within the organisation and during the deployment of software applications at customer sites. One interviewee stated: "Employees from the networking department are responsible for deploying applications at the client site..." (11_M_NE_8-9). Subjects work towards achieving something, which is the goal. The goal in Activity Theory is represented by objects. Objects are discussed in the next section.

3.2 Objects

Objects in Activity Theory represent the goals which subjects are supposed to achieve when carrying out activities (Engeström, 2001). The organisation is divided into several departments. The organisation comprises of three core departments which includes the business department, the software engineering department and the network engineering department. Subjects (employees) are assigned to each department depending on their specialisation as one interviewee indicated: "We have three core departments, software engineering, networking and business" (1_M_NE_4).

For each project, employees (subjects) have a role to play in its implementation (object). Each employee has an individual goal to achieve. Employees in a department (subjects) also have a collective goal to achieve. For example, the early phases of software projects are initiated by application consultants in the organisation. The purpose is to ensure that customers' ideas are well communicated to software engineers. The implementation phase is initiated by the software engineering department to ensure that customers' ideas are translated into software applications, while the deployment phase is initiated by the network engineering department, with the purpose of properly deploying software applications at customers' site. One of the interviewees stated: "Each department has a unique role to play in the project life cycle. The three different departments that we have here all perform different functions and these functions contribute to the progress of the project" (12_M_NE_25-27). Another interviewee stated: "As a software engineer, my colleagues and I are responsible for developing software applications, and the first step in initiating this process is to liaise with the business department, they ensure that the requirements are in line with what is to be developed, the networking guys make sure everything is properly done at the customer's site" (8_M_SE_54-57). The overall objective of each department is to ensure that they provide satisfactory services to their customers.

3.3 Tools

In the organisation, the tools which enable the subjects (employees) achieve their goals (objects) include computers, internet facilities, programming tools, telephones, documents, customer files and customer information. Telephones are situated in each departmental unit. Telephones facilitate communication between customers and employees in the organisation.

Computers also facilitate employees in carrying out work activities, for example, checking e-mails and writing software programs. The internet is used to access employee e-mail and sending messages to customers. The internet is also used to access some client applications.

Another vital tool used by employees is customer information. Customer information help employees perform their duties. One interviewee from the software engineering department explained ”Customer information is very important to us, we need it to verify our output during software development. We also need customer information when providing helpdesk support services to our clients” (7_M_SE_10-13).

3.4 Rules

Departments within the organisation are guided by policies in order for employees to meet their goals. These policies were created by the management. There are different policies which guide the different departments as well as policies which guide each employee. The organisation’s policy does not permit employees to share passwords even if they work within the same domain. One interviewee stated ”We are not allowed to share passwords with anyone, even when we work within the same department, because we all have to be responsible for our actions on the system” (5_F_B_82-83). In the business department, application consultants are not allowed to view customer information outside their domain. Customer information is meant to be kept private within the context of its application. The department is also guided by rules in which application consultants are specifically assigned to discuss with customers.

Password policies are kept stronger within the software engineering department and the networking department. The software engineering and networking department are guided by the departmental password policies, as well as the individual password policies because they have direct access to modify, add and delete customer information. Employees on the lower hierarchy have limited access to customer information. One interviewee stated: ”Due to the nature of our jobs and the access to information which is provided by our customers, we have to be careful in the way customer data is accessed. Junior employees within our department are given restricted access or no access at all” (10_M_SE_93-95).

Senior employees within these departments ensure that these policies are strictly adhered to, in order not to make mistakes that could be damaging to the organisation’s reputation. Senior employees within these departments strictly enforce these policies to ensure that staff members do not lose their reputation as a result of unintended mistakes made due to inexperience. One interviewee stated ”...at the same time we do not want our junior employees to make unnecessary mistakes which can be attributed to lack of experience and that is one the reasons why we restrict access to customer information on those levels”

(4_F_B_121-123).

The organisation also uses activity logs as a means of recording activities of applications which employees work on. This is part of their policy to keep track of the activities carried out by each employee.

3.5 Community

Employees (subjects) from different departments form the community. These employees have a common goal (objects). The community also work together regularly to ensure that the goals of each employee is aligned with the central goal of the project. Meetings are usually held to ensure that each subject's activity is in line with the objectives of the project. One interviewee stated "We usually have meetings which involves key employees who are participating in a project. The meeting brings together selected employees from the three main departments in the organisation" (10_M_SE_140-142). The success of a project is a collective effort of the various departments who take part in the project.

3.6 Division of labour

Each employee (subject) in the organisation is assigned work, which forms part of a project. Work activities are divided among the employees in the organisation. Each employee has a role to play despite their level in the organisation. One of the interviewees stated: "It doesn't matter if you are a network engineer or software engineer, you have to be assigned work, even if you are an intern, trainee, or even a senior staff, you have to contribute something" (2_F_B_145-147).

4 Findings

This section discusses the findings from the analysis of the data as presented above. As shown in Figure 1. The factors influencing information security practices in software organisations include employee structure, work context, information sensitivity, reputation, responsibility, accountability and policies.

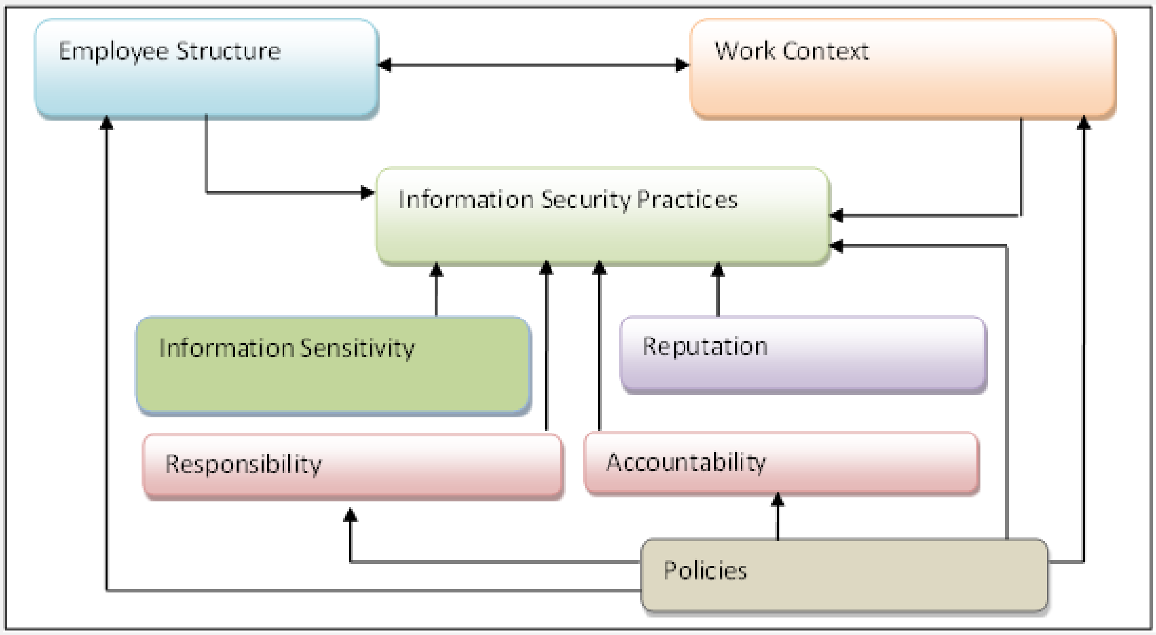

Figure 1: Factors influencing information security practices in Namibian software organisations

4.1 Employee structure

Based on the analysis, it is evident that the way employees are structured within the organisation plays a significant role in determining how customer information is accessed by employees in the organisation. The purpose of this enforcement is to ensure that employees do not abuse customer information. The organisational policies ensure that employees are well grounded in the working environment before they are given access to customer information. The organisation uses this policy as one of the measures to enforce information security within the organisation.

4.2 Work context

The organisation maintains a strict emphasis on policies. Despite employee structures being put in place, the organisation also strives to eliminate redundant use of customer of information, and as a result, employees only have access to information required to perform their duties. The organisation employs this technique to ensure that employees do not have unnecessary privileges to information that they do not need.

4.3 Information sensitivity

The organisation has a policy which restricts inexperienced employees from gaining access to sensitive customer information. This policy improves information security practices within the organisation, thereby decreasing the amount of information security threats internally. In-depth understanding and use of customer information comes through experience and continuous interaction with the work environment which has to be built before employees are given access to such information. Activity Theory assisted in establishing the role of employees in the organisation.

4.4 Reputation

The organisation tries to maintain a good reputation with customers, and as a result, enforce strict information security policies. The organisation values its external reputation, and hence, would not want to damage it as a result of information security threats to customer information. This is one of the reasons information security is narrowed down to the lowest level. The organisation also tries to ensure that employees do not make mistakes as a result of their inexperience; as a result, junior employees are given access to customer information only when they completely understand the work context.

4.5 Responsibility

The organisation strives to ensure that employees (subjects) are responsible for activities carried out, and as a result, passwords are not shared among employees (subjects). When employees are aware that their actions cannot be hidden on the system, they will try to reduce activities that compromise existing information security practices.

4.6 Accountability

Activity logs are kept within the organisation to ensure that employees are accountable for their actions with regards to customer information. With Activity Theory, it was possible to understand the measures put in place by the organisation to enforce accountability for user actions on the system. The analysis also reveals that employees can be easily tracked by their actions, and hence, will try to reduce activities that compromise existing information security practices.

4.7 Policies

Policies guide the way activities are carried out in organisations. Having effective policies in place ensures that activities are carried out in a structured and orderly manner. Based on the analysis, it is evident that the organisation employs different policies that enforce information security practices. These practices are enforced at different levels and work contexts in the organisation.

5 Conclusion

The purpose of this study was to identify the factors that influence information security practices in software organisations. The study also examined the activities carried out in the organisation using Activity Theory as a lens. The use of Activity Theory as a lens also helped to examine how activities carried out by subjects (employees) in a community facilitate information security practices at Solitaire Software Company.

With this study, it was possible to establish that Solitaire Software Company places information security in high esteem, and hence, it is embedded in their practices. The findings also reveal that these practices are embedded through policies which are applied at both departmental and individual levels. The use of Activity Theory in the analysis of factors that influence information security practices in software organisations brings a different perspective both theoretically and practically as it contributes to the body of literature which uses Activity Theory to analyse the activities which take place in software in software organisations as well as establishing the factors that influence information security practices in software organisations. From a practical perspective, software organisations can adopt the findings in their existing policies to enhance information security practices.

The study indicates that employees play an important role to ensure that information security policies are strictly enforced. The study also revealed that factors such as employee structure, work context, information sensitivity, reputation, responsibility, accountability and policies influence information security practices in Namibian software organisations which are often overlooked.

The limitation of this study is the use of one Namibian software organisation as a case study, and hence, may be difficult to generalise the findings. However, for future research, different software organisations can be used as case studies.

References

[1] Al-Busaidi ZQ. Qualitative research and its uses in health care. Sultan Qaboos University Medical Journal, 8, 1, 11-19 (2008).

[2] Aloul FA. The need for effective information security awareness. Journal of Advances in Information Technology, 3, 3, 176-183 (2012).

[3] Buse RPL, Zimmermann T. Information needs for software development analytics. Proceedings of the 34th International Conference on Software Engineering, Zurich, Northern Switzerland, 987-996 (2012).

[4] Bonnette CA. Assessing threats to information security in financial institutions. http://www.sans.org/reading-room/ (2003). Accessed 10 May, 2015.

[5] El-Hadary H, El-Kassas S. Capturing security requirements for software systems. Journal of Advanced Research, 5, 4, 463-472 (2014).

[6] Engeström Y. Expansive learning at work: Toward an activity theoretical reconceptualization. Journal of Education and Work, 14, 1, 133-156 (2001).

[7] Halkidis ST, Chatzigeorgiou A, Stephanides G. A qualitative analysis of software security patterns. Computers & Security, 25, 5, 379-392 (2006).

[8] Herath T, Rao, HR. Encouraging information security behaviours in organisations: Role of penalties, pressure and effectiveness. Decision Support Systems, 47, 154-165 (2009).

[9] Hong K, Chi Y, Chao LR, Tang J. An integrated system theory of information security management. Information Management & Computer Security, 11, 243-248 (2003).

[10] Khan B, Alghathbar KS, Nabi SI, Khan KM. Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5, 26, 10862-10868 (2011).

[11] Moloi R, Iyamu T. Understanding the deployment of competitive intelligence through moments of translation. International Journal of Information Technology and Web Engineering, 8, 2, 33-45 (2013).

[12] Morf ME, Weber WG. Psychology and the bridging potential of A. N. Leont'ev's Activity Theory. Canadian Psychology, 41, 2, 81-93 (2000).

[13] Mouratidis H, Giorgini P, Manson G. When security meets software engineering: A case of modelling secure information systems. Information Systems, 30, 8, 609-639 (2005).

[14] Nicholls C. The advantages of using qualitative research method. http://www.alexander-technique-college.com (2011). Accessed 20 May, 2015.

[15] Odejide AA, Iyamu T. Structuration analysis of factors influencing risk management deployment. Educase Management of Innovation and Technology (ICMIT), IEEE Conference on, 405-411 (2012).

[16] Patton MQ, Cochran M. A guide to using qualitative research methodology. http://fieldresearch.msf.org (2002). Accessed 15 May, 2015.

[17] Payne S. Developing security education and awareness programs: prevention in theform of education and awareness programs can help campuses avoid security ills. Educase Quarterly, 6, 49-53 (2003).

[18] Shaanika I, Iyamu T. Deployment of enterprise architecture in the Namibian government: The use of activity theory to examine the influencing factors. Electronic Journal of Information Systems in Developing Countries, 71, 6, 1-21 (2015).

[19] Show J. Information security in practice from an Activity-Theoretic perspective. Proceedings of the 6th Annual Security Conference, Las Vegas, NV, 1-8 (2007).

[20] Theoharidou M, Kokolakis S, Karyda, M, Kiountouzis, E. The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24, 6, 472-484 (2005).

[21] United States General Accounting Office. Information security risk assessment: Practices of leading organisations. http://www.gao.gov/special.pubs/ai00033.pdf (1999). Accessed 10 May, 2015.

[22] Wu C, Chen S. Interpretive Research: An assessment and relevance in Nursing. Tzu Chi Nursing Journal, 4, 4, 8-13 (2005).

[23] Yang N, Yu H, Qian Z Sun H. Modeling and quantitatively predicting software security based on stochastic Petri nets. Mathematical and Computer Modelling, 55, 1, 102-112 (2012).

[24] Yin RK. Case Study Research - Design and Methods, Sage Publications Inc, New York, USA (1989).