AN EMPIRICAL STUDY OF STAFF COMPLIANCE TO INFORMATION SECURITY POLICY IN A SOUTH AFRICAN MUNICIPALITY

Nehemiah Mavetera, Ntebogang Dinah Moroke, Abbey Sebetlele

Abstract

Despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategies still remains one of the top challenges facing global organizations. This study investigated Information Security Policy compliance of staff members of a municipality in South Africa. Factors such as information security policy, security policy strategic planning, policy implementation and compliance were considered. A questionnaire was distributed to 80 staff members from different sections in this municipality and a response rate of 100% was achieved. The study findings showed that the majority of employees are largely in support of the municipality's efforts to develop and implement a security policy framework. They also concur that compliance to security policy safeguards and prevents intrusion information, theft and "denial of service". Among other issues, it is recommended that more training and awareness campaigns should be done to all employees in order to improve security of information in this municipality. The study results can be limited by the small number of the population as indicated that the sample was equal to the population (N=n).

Keywords: Information Security Policy; South Africa

**North West University, P. Bag X2046, Mmabatho, 2735, South Africa*

1 Introduction

This study is premised on the observation that there remain some teething challenges in the implementation of information security strategies in organizations. Despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations. It is within this context that this study then seeks to establish the compliance of staff at a South African provincial government municipality. To be specific, this study investigates the compliance of staff of North West Provincial Municipal District Office to the Information Security Policy within the municipality. It should be noted that the development of the security policy involves employer's policies, planning and selection of security technology. The organization should have procedures, policies and practices in place before implementing latest software technology, such as firewall. This will help in securing gadgets like laptops and corporate networks against malware interruption to business and ensure reliance on unsecured public networks. Laudon and Laudon (2007) emphasize that observing these specifications would ultimately result in positive business solutions and would also ensure high performance and thus reducing costs.

The focus of this study is more on factors such as information security policy, software analysis, strategic planning, implementation, compliance and the use of intranet, extranet and internet services as a means to minimize and manage information security threats. The security of information systems in any organization is very important. As such, plans to ensure the success of the right implementation strategy must be in place. This will help avoid problems emanating from lack of compliance. A general problem with the department is the fact that only few people know about aspects covered by the department's information security policy. As a result, due to this widespread ignorance, the employees seem not to care about the protection of information assets and processing systems of the company. This extends to ignorance on information processing systems used to process, store and communicate information assets. It is within this context that this study investigates the extent of compliance of staff at this South African government municipality. The rest of the paper is structured as follows: Study objectives are discussed next followed by a brief on extant literature on information security policies, the study methodology and results are then presented and the research findings and discussions will be on the last section.

2 Study objectives

Among other issues that may need to be addressed with regard to information security policy, this study will address only three objectives which are to:

- Determine factors associated with compliance in the Ngaka Modiri Molema local municipality (NMMLM).
- Determine the advantages of compliance and disadvantages of a lack of information security policy.
- Provide recommendations on staff compliance to the government information security policy.

3 Brief literature review

A number of studies looked at compliance of information technology policy at different organizations. This study reviews literature with special attention given to security elements as discussed below.

3.1 Data Security Breaches

Security breach is the most common mistake employees commit by being careless when handling or storing classified documents and operating equipment. Incidents involving security breaches not only decrease employee productivity, but also damage customer confidence and the organization's reputation. This therefore, adversely affects the future economic performance of the affected firms (Campbell *et al.*, 2003). From Wen and Tarn (1998), an example of security breach by unauthorized use of a corporate network is discussed and is ranked as the most common form of security breach when using social networks. The danger of attack by unauthorized access can be minimized by performing user authentication and data encryption via a firewall. Sometimes an intruder may attempt to bypass the firewall by pretending to be an authorized user. Furthermore, in examples given by Berezina *et al.* (2012), breaches of hotel guests' personal information can result in identity theft. Identity theft is the misuse of personal information for criminal activities by a third-party in order to obtain a personal gain or to commit a crime (Spendonlife.com, 2009; Federal Trade Commission, 2010). According to the Federal Trade Commission (2010), in 2009 identity theft complaints accounted for 21 percent of all consumer complaints in the US. In the category of identity theft, credit card fraud was the most frequently reported (17 percent). Based on this, credit card information security breaches were studied as the primary focus, to better understand the potential impact of information security breaches on hotel guest's behavior.

3.2 Security Awareness

As stated by Palmer (2001), Security Awareness (SecA) is an organization's objective strategy for establishing a formal security awareness program. Security policy has to ensure that the policy framework elements are properly communicated and accessible at all levels from new hires, employees, and third parties such as contractors, partners, and up until the consultants. Moreover, the policy has to ensure that appropriate education and training are provided to all organization employees for them to be fully equipped with information security. SecA is another way of sensitizing employees of the importance of the security aspects within the company. Tsohou *et al.* (2008) alludes that Information Security (IS) awareness is a means of improving information security by enhancing the adoption of security policies, rules, regulations and counter measures. This measure is also useful in improving IS users' security behavior and altering work routines so that good security habits are applied. Despite the recent increased attention afforded to security incursions, Schmidt (2008) contends that there is a lack of user awareness and understanding of information security. Thus, greater computer security awareness, education, and training is needed (Wade, 2004; Aytes and Connolly, 2004; Kruck and Teer, 2008). Additionally, as suggested by Rotvold (2008); Vroom and von Solms (2002), all users should be aware not only of what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat.

3.3 Security Compliance

Security compliance (SC) has been a major concern for many organizations in that employees seldom comply with information security procedures. Siponen *et al.* (2007) view policies, especially those involving information security, as mere guidelines or general directions to follow rather than 'hard and fast rules' that are specified as standards. Due to this relative discretionary nature of adherence to these policies, organizations find enforcement of security to be a critical challenge. Thus more recently, research in behavioral information security has started focusing attention to employee intentions to follow security policies (Chan *et al,* 2005). On the contrary, Vroom and Solms (2004) state that General Information Security Compliance measurement and enforcement include more than what is provided by managed information security services. Activities must be managed as far as compliance is concerned.

3.4 Security Behavior

More attention needs to be given to the social and behavioral aspects of information security among AMCs as highlighted by (Hazari, 2005; Huebner and Britt, 2006; Pattinson and Anderson, 2007; Guzman *et al.*, 2008). According to Ma *et al.* (2008), because information security is more of a human problem than a pure technical problem, practitioners should pay more attention to the cultural aspects of information security. The author identified numerous user acceptance models in the literature, including the Technology Acceptance Model (TAM) (Davis, 1989; Venkatesh and Davis, 2000). Willison (2006) further argues that organizations should focus on the actual behaviors of offenders at various stages of their misuse in order to implement controls (safeguards) that would reduce the employees' ability to misuse the IS at each stage. Ball and Levy (2008), Dinev and Hu (2007), Hazari *et al.* (2008) and Novakovic *et al.*, (2009) suggested that further research on the generalizability of factors associated with technology acceptance (TA) and user behavioral studies is needed, particularly in the domain of information security. According to Chan *et al.* (2005), many information security breaches in the workplace have been attributed to the failure of employees to comply with organizational security policies. The author suggested that attention needs to be paid to learning why non-compliant behaviour takes place so that appropriate measures for curbing the occurrence of such behaviour can be found. Logan and Noles (2008) recommend that the assessment of operations and services enabled by internal security controls should be tightened because employees are responsible for numerous security breaches.

3.5 Organizational Culture

Schein (1999) defines organizational culture as the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration. Organizational culture includes the ideas shared by the people of the company and communicated between each other; basically a system of learned behaviour (Szilagyi and Wallace, 1990). This culture is the single most important factor accounting for success or failure in an organization (Deal and Kennedy, 1982). Organizations need to ensure that the interaction among people, as well as between people and information technology (IT) systems, contributes to the protection of information assets. Organizations therefore need to assess their employees' behaviour and attitudes toward the protection of information assets in order to establish whether employee behaviour is an asset or a threat to the protection of information (Da Veiga, *et al.*, 2007).

According to Schlienger and Teufel (2003), there is no unique tool set and method for studying information security culture with regards to what to assess and how to assess it. However, Tipton and Krause (2007) stress that security does not lie only in firewalls, passwords and awareness training, but also in a culture that views and thinks correctly about information security issues. A culture of information security needs to be embedded into the organizational culture, to allow them to view and think correctly about information security problems. Schein (1999) describes culture as existing in three levels which are artifacts espoused values and shared tacit assumptions. This definition however is not specific to information security despite being widely accepted as a general organizational culture definition, hence its enhancement by Van Niekerk and Von Solms (2010).

3.6 Security Policy

The objective of any organizational policy is to influence and determine employees' course of action (Tejaswini and Rao, 2009). On the other hand, Mishra and Dhillon (2006) differ by saying policies may be crystal clear and detailed, but the result may not turn out to be as desired, especially with regard to information security. Security policy consist of statements of ranking information risks, identifying acceptable security goals and the mechanisms for achieving these goals (Laudon and Laudon, 2007). Within this context, the security policy drives policies determining acceptable use of the firms' information resources and identifying which members of the company have access to its information. Hong *et al.* (2006) argue that an Information Security Policy consists of the rules set-up for the use of information assets, and the statement set-up for the security priorities to achieve organizational objectives. It also includes the guidelines for the scope of information security; the principle for information management and resource use; and the principle for supporting security techniques.

According to Wen and Tarn (1998), the first step that an organization must take in an effort to defend itself against an attack from the hackers is to ensure that it has a well-defined, documented and enforceable security policy in place. In addition, this security policy should include published security guidelines to inform users of their responsibilities. Since availability, integrity and secrecy of data must be maintained, security policy defines network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, and virus protection measures, and employee training (Sanderson and Forcht, 1996). Guel (2007) regards security policy a formal, brief and high-level statement or plan that embraces an organization's general beliefs, goal, objective and acceptable procedures for a specified subject area.

3.7 Security Technology Control Measures

It is widely believed that organizational efforts to manage Information System security are typically focused on vulnerabilities in technological assets such as hardware, software, networking, at the expense of managing other sources of vulnerabilities, such as people, policies, processes, and culture (Halliday *et al.*, 1996). A computer system's security can be compromised in many ways. The ways may be a denial-of-service attack that can make a server inoperable, a worm can destroy a user's private data, or an eavesdrop per can reap financial rewards by inserting himself in the communication link between a customer and her bank through a man-in-the-middle (MITM) attack. As security is always a major concern in most of the networked computer systems, embedded systems should provide security features to defend the attack and protect the confidential and sensitive data. Many Trojan Horses and viruses use the security holes of exception to trigger attack, such as buffer overflow attack (Yau *et al.,* 2008).

4 Study methods and data

The quantitative exploratory and descriptive design was used to identify, analyze and describe factors contributing to staff compliance to the information security policy in government departments. Struwig and Stead (2004) have a different way of defining quantitative method. The authors define these methods as a form of conclusive research involving a big representative samples and fairly structured data collection procedure. The study is a blue print in such a way that maximum control is exercised over factors that could interfere with the validity of the research results (Polit and Hungler, 1999).

The target population was employees from the local municipality in South Africa. The population consists of 80 (Eighty) employees from different sections in that municipality. The data collection was done using questionnaires. Municipal staff members who qualified as respondents were asked to complete the questionnaire. All items in a questionnaire are measured using a standard four-point Likert scale (strongly disagree to strongly agree). The researchers prepared and distributed 80 questionnaires to the employees and a response rate of 100% was obtained. This means that the sample size (n) was equal to the population (N). The questionnaire had two sections, the first on gathering data on respondents' demographics and the second section consist of six constructs. SPSS version 22 was used to execute the analysis.

Table 1 provides information on the demographic profile of respondents.

Table 1. Demographic profile of respondents

Variable	Category	Responses	
		n	%
Gender	Female	45	56.3
	Male	35	43.7
Age group	15 - 20 years	0	0
	20 - 25 years	5	6.3
	25 – 30 years	15	18.8
	30- 35 years	18	22.5
	35 years and above	42	52.5
Qualification	Grade 10	7	8.8
	Matric	17	21.3
	National Certificate	5	6.3
	National Diploma	18	22.5
	Degree	15	18.8
	Post Graduate	18	22.5
Job level	Senior Management	7	8.8
	Middle management	18	22.5
	Supervisory	19	23.8
	Lower Rank	36	45.0
Work experience	1 – 3 years	27	33.8
	3 – 6 years	15	18.8
	6 – 10 years	15	18.8
	10years and above	23	28.7
Race group	Black	65	81.3
	White	9	11.3
	Colored	5	6.3
	Indian	1	1.3
Marital status	Single	38	47.5
	Married	33	41.3
	Divorced	5	6.3
	Widowed	1	1.3
	Cohabitant	3	3.8

It is evident that females are more (56.3%) represented than males (43.7%) in this survey. This is proven by the responses gathered as shown in Table 1 above. Also shown is that the municipality comprise of elderly people who are aged 35 years and above (52.5%). The youngest employees (6.3%) are of the age group 20 to 25 years. The majority of respondents at this department have varying qualifications with 22.5% in possession of national diploma and about 40% with university degrees. About 55.1% of respondents in this study are in different levels of management with 23.8% representing those on the supervisory positions, 22.5% in middle management and the least at top management level. The rest of the respondents are employees at lower positions. All of the employees at the municipality have been with this organization for a period of more than a year, with almost 30% having a working experience of more than 10 years. It is also not surprising to realize that most of the employees are Blacks (81.3%) with Indians in minority (1.3%).

4.1 Data analysis and empirical results

This section provides analysis of the results presented in tables. Firstly, the study provides evidence about the quality of data used and then addresses the objectives as outlined in Section

4.1.1 Reliability and validity:

Firstly, the instrument used for data collection was tested for reliability prior to addressing the objectives set for the study. For the researcher to establish the validity and reliability of the research instrument, it is necessary to clarify these concepts and to relate it to this research. According to Jaeger (1990), reliability is considered as a measure concept that represents the consistency with which an instrument measures a given performance or behaviour. The questions are structured in a way to ensure that all are fully and clearly written. Each question must have a consistent meaning to all respondents and is constructed to ask one and only one question. The items used in this study have been tried and tested by numerous previous studies. Boudreau (2001) recommend application of validated and tested data so as to obtain improved reliability of constructs and results.

The reliability of the instrument in this study is assessed with Cronbach's alpha. Byrne, *et al.* (1989) suggested that items for each question have to represent a single concept (cited by Montshiwa and Moroke, 2014). Several authors such as Blaha *et al.* (2001) and Diamantopoulos and Siguaw (2006) supported this suggestion. The value of Cronbach's alpha coefficient ranges between 0 and 1, with the values closer to 0 implying that the items do not measure the same construct and values closer to 1 providing opposite implication. A rule of thumb 0.6 is set as a yardstick due to the sample size used. To ensure convergent validity, the study used factor loadings and the variance for each constructs are calculated as suggested by Siponen *et al.* (2007). The reliability and validity measures as calculated are shown in Table 2 which gives a summary of results from the factor analysis method.

Table 2. Convergent validity and internal consistency and reliability

Construct	Items	Factor loading	Variance extracted	Cronbach's alpha
Security awareness	ISP1	.802	31.054	0.785
	ISP1	.779		
	ISP2	.739		
	ISP3	.718		
	ISP4	.655		
	ISP5	.644		
	ISP6	.568		
	ISP7	dropped		
Organisational Culture	OC1	.761	4.130	0.826
	OC2	.717		
	OC3	.668		
	OC4	.647		
	OC5	.638		
Information Security Policy	ISP1	.832	14.522	0.821
	ISP2	.761		
	ISP3	.722		
	ISP4	.675		
	ISP5	.514		
Data Security Breach	DSB 1	.746	6.522	0.762
	DSB 2	.721		
	DSB 3	.651		
	DSB 4	.566		
Security Compliance	DSB 5	.782	4.133	0.708
	DSB 6	.612		
	DSB 7	.601		
Security Technology Control Measures	STCM 1	.779	3.150	0.685
	STCM 2	.521		
Chi-square test χ^2 300.287 df 200 $Sig.$ 0.000				

As shown above, all the constructs are acceptable. This provides an assurance that the data and constructs used are reliable and consistent. The variances associated with each construct are different implying the divergence of constructs with the first one having more weight than others. This is in accordance with Hair *et al.* (2006). All factor loadings are in excess of 0.5 except for ISP 7 which was dropped from the analysis. Maximum likelihood method was used to obtain the loadings and the overall fit of factor model was assessed with a chi-square test which proved to be statistically significant.

Next the paper present the results of the responses gathered from respondents regarding security policies. Table 3 portrays constructs that pertain to employee views on information security policy.

To determine employees' views concerning Information security policy

Table 3. Views about information security policy

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
The department has information security policy in place.	3.8	13.8	15.0	30.0	37.5
I know where to get IT security policy copy	5.0	11.3	23.8	37.5	22.5
Information security policy drives policies determining acceptable use of the firm's information resources.	3.8	12.5	22.5	50.0	11.3
Information security policy provides instruction for the development and implementation of a security posture, as well as provides guidelines for the acceptable uses of the systems.	2.5	10.0	21.3	52.5	13.8
Carelessness and behaviour of employees who fail to comply with organizations information security policies and procedures put the organization at information risk.	3.8	7.5	18.8	41.3	28.8
Monitoring policies and procedures have to ensure that users throughout an organization are following established procedures.	2.5	8.8	18.8	42.5	27.5

It is evident according to responses in Table 3 that the majority of employees (67.56%) at the municipality are well-informed of information security policies at their workplace. This is not surprising given their age distribution and the duration they have been with this department. The responses reveal that a reasonable number of these employees concur that the management has made sure that they are kept abreast of the security policies in the organization and have knowledge that their ignorance will put the department in jeopardy. It is also very impressive to realize that these employees are aware of what their department's responsibility is in terms of information security policy. This is in support of suggestions by Vroom and Solms (2004). It is also clear the municipality has considered Wen and Tarn (1998), who recommended that organizations should defend themselves from hackers firstly by ensuring that a well-defined, documented and enforceable security policy is in place as confirmed by 67.5% of respondents.

To determine employees' views concerning Security Awareness

Table 4. View concerning security awareness

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
It is mostly regarded as aiming at improving information security by enhancing the adoption of security policies	3.8	3.8	13.8	53.8	25.0
There is need to increase security awareness by offering additional security awareness training.	3.8	2.5	13.8	45.0	35.0

The majority of respondents as shown in Table 4 seem to be agreeing on the issue of security awareness as responses reveal. A total of 80% (45%+35%) of these employees concur with Fritsche and Rodgers (2007) recommendation that though they are well-informed of the importance of security in their organization, additional training should be provided to everyone.

To determine employees' views concerning Objective Security Compliance

Table 5. Security compliance

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
The employees seldom comply with information security procedures	3.8	6.3	43.8	36.3	10.0
Due to the relatively discretionary nature of adherence to these policies, organizations find enforcement of security a critical challenge	2.5	5.0	27.5	51.3	13.8

It is expected of the employees who are in possession of the information security policy documents and also are aware and understand what the contents of these documents are to comply with security as instructed. However, it is evident that even though the majority of the municipality employees have knowledge of the policy on information securities, they do not fully comply with these policies. This is confirmed in Table 5 by 46.3% who concur that employees seldom comply with information security procedures. About 65% of them are in agreement that this discretionary nature of adherence to these policies, the NMDLM finds it more challenging to enforce security. This supports Siponen *et al*. (2007)'s views about security compliance.

To determine employees' views concerning security Technology Control Measures

Table 6. Views concerning security technology control measures

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
All access requests and rights should be formally documented and approved by whoever has the authority to grant such access rights	3.8	1.3	8.8	61.3	25.0
Firewalls are placed between the company network and the Internet, to provide on-going protection by denying suspicious traffic	1.3	2.5	22.5	48.8	25.0
By introducing log audit which is monitoring/ logging mechanism is to ensure compliance with regulations in order to strengthen the information security	1.3	6.3	25.0	48.8	18.8

As Halliday, Badenhorst and von Solm (1996) indicated, the management of information systems securities by organization should be more focused on vulnerabilities in technological assets. Reponses provided confirm that the municipality management and employees are not ignorant when it comes to these control measures. These findings coincide with the notion by Halliday *et al*. (1996).

To determine employees' views concerning Data Security Breach

Table 7. Views concerning data security breach

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
I know what is information security breach	1.3	8.8	11.3	48.8	30.0
There is always information security breach by members.	1.3	8.8	38.8	32.5	18.8
Security breaches decrease employee productivity	2.5	5.0	42.5	28.8	21.3

As Table 7 reveals, the majority of the employees are knowledgeable about data security breach and its impact in the future of an employee and the wellbeing of the organization. This is proven by 78% (48%+30%) representing respondents concurring on the knowledge about information security breach and about 50% confirming that this breaching could decrease the employee productivity. Despite the knowledge these employees have, it is clear that some of them (about 50%) are continually not upholding the laws concurring with Campbell *et al*. (2003) definition of data security breach.

To determine employees' views concerning Security Behavior

Table 8. Views about security behavior

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
Organizations should focus on the actual behaviors of offenders at various stages of their misuse in order to implement controls (safeguards).	1.3	10.0	23.8	47.5	17.5

Respondents are of the opinion that to avoid further security breach by employees, it is the responsibility of the organization to make a follow up on the matter. The recommended solution according to these employees is that organizations should be more focused on the actual behaviors of offenders at various stages of their misuse.

To determine employees' views concerning Organizational Culture

Table 9. Views about organizational culture

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
Security does not lie only in firewalls, passwords and awareness training but also in a culture that views and thinks correctly about information security issues.	1.3	10.0	15.0	46.3	27.5
Organizations need to ensure that there is an interaction between people and information technology (IT) systems and that should contribute to the protection of information assets.	1.3	2.5	18.8	50.0	27.5

Literature dictates that culture of information security needs to be embedded into the organizational culture which Schein (1999) describes as existing as being in existence in three levels such as artifacts espoused, values and shared tacit assumptions. This may allow culture to view and think correctly about information security problems. The findings of this study are in accordance with the description given by Schein. As shown in Table 9, about 74% (46.3%+27.5%) of respondents concur that security does not lie only in firewalls, passwords and awareness training but also in a culture that views and thinks correctly about information security issues confirming Tipton and Krause (2007) idea.

To determine employees' views concerning the advantages of security policy

Table 10. Advantages of to security policy

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
Provides instruction for the development and implementation of a security posture as well as provides guidelines for the acceptable and accepted uses of the system	1.3	2.5	13.8	68.8	13.8
It prevents vulnerabilities in technological assets such as hardware, software and networking	2.5	6.3	17.5	51.3	22.5
Provides an organization with a concise yet high level and comprehensive strategy to shape its tactical security solutions in relation to business objectives	1.3	5.0	21.3	53.8	18.8
Deals with the processes and procedures that the employee should adhere to in order to prevent confidentiality, integrity and availability of information	1.3	3.8	16.3	60.0	18.8
It safeguards and prevents intrusion, information theft, and "denial of service"	1.3	2.5	23.8	52.5	20.0

This study intends to examine the advantages of having an organization effectively implementing the information security policy. Amongst the five advantages identified as shown in Table 10, it is evident that the majority of the respondents about 82% (68.87%+13.8%) are more in support of one that emphasizes provision of instruction for the development and implementation of security postures. The least preferred advantage according to respondents is the fact that it safeguards and prevents intrusion, information theft, and "denial of service" 72.5% (52.5%+20%).

To determine what the disadvantages of non-compliance to security policy are

Table 11. Disadvantages of non-compliance to security policy

Statement	Strongly disagree	Disagree	Don't know	Agree	Strongly agree
Decreases employee productivity, damages to consumer confidence and the organization's reputation and promotes theft of classified information	3.8	7.5	26.3	40.0	22.5
Policy needs to be audited to ensure that they are in line with the objectives, goals and vision of the organization	3.8	2.5	15.0	50.0	28.8
Carelessness and behaviour of employees who fail to comply with organization's information security policies and procedures put the organization at information risk	0	3.8	27.5	35.0	33.8

One of the disadvantages of the non-compliance to information security policies as identified by most of the respondents is the lack of keeping policies up to date and making sure that they are in line with the objectives, goals and vision of the organization. Another disadvantage this non-compliance could have is a decrease in employee productivity, damages to consumer confidence and the organization's reputation. This could in addition promote theft of classified information. Though carelessness and behaviour of employees who fail to comply with organization's information security policies and procedures has been identified as another disadvantage, it appears to be the least threat (35%) according to the findings of this study.

5 Study conclusions

The study sought to determine factors associated with information technology policy compliance in South African municipality. The organization comprises of 80 employees who all took part in the study. A reasonable number of these employees concur that the management has made sure that they are kept abreast of the security policies in the organization and have knowledge that their ignorance will put the department in jeopardy. It is also encouraging to realize that these employees are aware of what their department's responsibility is in terms of information security policy as also suggested by Vroom and Solms (2004). It is also noted that most of the employees take security awareness into consideration to some extent. All employees are bound to be security conscious as indicated by Humphrey (2008) and Rodgers that additional training should be provided to every employee. Security compliance remains a mammoth task to staff as they seldom comply with the policy on information security. The study revealed only 65% complying with the policy.

It has also been proven that the majority of employees are largely in support of the municipality's efforts to develop and implement security policy frameworks. They also concur that compliance to security policy safeguards and prevents intrusion, information theft, and "denial of service". This is supported by Tejaswini and Rao (2009) who highlighted that the objective of any organizational policy is to influence and determine employees' course of action. Guel (2007) emphasize that compliance to security policy embraces an organization's general beliefs, goal, objective and acceptable procedures for a specified subject area. Respondents pointed out that carelessness and unbefitting employees' behaviour results non-compliance to organization's information security policies and procedures. This is in accordance with Chan *et al.* (2005) who are of the opinion that many information security breaches in the workplace have been attributed to the failure of employees to comply with organizational security policies.

It is recommended that more training awareness campaigns should be done to all employees in order to improve security of information. This is supported by Siponen *et al*. (2007).

References

1. Berezina, K., Cobanoglu C., Miller, B. L. and Kwansa, F.A. (2012) 'The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth', International Journal of Contemporary Hospitality Management, Vol. 24, No. 7, pp.991 – 1010.
2. Blaha, J., Merydith, S.J., Wallbrown, F.H. and Dowd, E.T. (2001) 'Bringing another perspective to bear on the factor structure of the MMPI-2', Measurement and Evaluation in Counselling and Development, Vol. 33, pp.234-243.
3. Byrne, B. M., Shavelson, R. J., and Muthén, B. (1989). Testing for the equivalence of factor covariance and mean structures. The issue of partial measurement invariance. Psychological Bulletin, Vol. 105, No. 3, pp.456-466.
4. Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003) 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', Journal of Computer Security, Vol. 11, No. 3, p 431-48.
5. Chan, M., Woon, I., and Kankanhalli, A. (2005) 'Perceptions of information security in the workplace: Linking information security climate to compliant behavior', Journal of Information Privacy & Security, Vol. 1, No. 3, pp.18-41.
6. Da Veiga, A., Martins, N., and Eloff, J.H.P. (2007) 'Information security culture - validation of an assessment instrument'.
7. Diamantopoulos, A., and Siguaw, J.A. (2006) 'Formative versus Reflective Indicators in Organizational Measure Development: A Comparison and empirical illustration' British Journal of Management, Vol. 17, No. 4, pp.263-282.
8. Halliday, S., Badenhorst, K., and von Solms, R. (1996) A Business Approach to Effective Information Technology Risk Analysis and Management', Information Management & Computer Security, Vol. 4, No. :1, p19-31.
9. Hair, J.F.J., Black, W.C, Babin, B.J, Anderson, R.E., and Tatham, R.L. (2006) Multivariate data analysis. Sixth ed. 2006, Pearson Prentice Hall.
10. Hong, K., Chi, Y., Chao, L. R., and Tang, J. (2006) 'An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan' Information Management & Computer Security, Vol. 14, No. 2, pp.104-115.
11. Jha, P.C., Kapur, P.K., Bali, S., and Kumar U.D. (2010) 'International Journal of Reliability, Quality & Safety Engineering' Vol. 17, No. 3, pp.209-222.
12. Kokka, S. (1998) 'Property rights on an Internet', Journal of Technology Law & Policy, Vol. 3 No.2, pp.24-35.
13. Langelier, C., and Ingram, J. (2001) National State Auditors Association and the U.S. General Accounting Office: Management Planning Guide Information System Security Auditing: [online] http://www.gov [cited May 11, 2013]
14. Laudon, K. and Laudon, J. (2007) Management Information Systems: Managing the Digital Firm, 9th Edn., Prentice Hall, (country).
15. McCollum, T. (1997) 'Computer crime', Nation's Business, pp.18-26.

16. Montshiwa, V.T. and Moroke, N.D. (2014) ‘Assessment of the Reliability and Validity of Student-Lecturer Evaluation Questionnaire: A Case of North West University’, Mediterranean Journal of Social Sciences, Vol. 5, No. 11, pp.352-364.
17. Paliotta, A. (1999) A personal view of a world class IT auditing function http://www.isaca.org/art11.htm (1999) [cited May 15 2013].
18. Palmer, M.E. (2001)’ Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age’, Information Systems Security, Vol. 10, No. 2.
19. Reichers, A. E., and Schneider, B. (1990) Organizational climate and culture: Evolution of constructs, organizational climate and culture. B. Schneider (Ed.), Title of book. San Francisco: Jossey-Bass.
20. Rossouw, C. and von Solm, R. (2003) Towards Information Security Behavioural Compliance, Port Elizabeth Technikon, Port Elizabeth, South Africa.
21. Schein, E.H. (2009), The Corporate Culture Survival Guide. New and Revised Edition, Wiley and Sons, San Francisco.
22. Schlienger, T., and Teufel, S. (2003) ’Information security culture – from analysis to change’ Proceedings of ISSA, pp.183-195.
23. Siponen, M., Pahnila, S., and Mahmood, A. (2007) New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne,L., Eloff, J., von Solms, R., (Boston: Springer), in IFIP International Federation for Information Processing, Vol. 232, pp. 133-144.
24. Struwig, F.W., and Stead, G.W. (2010) Planning, Designing and Reporting Research. Maskew Miller Longman Ltd, Pearson Education South Africa.
25. Szilagyi, A.D., and Wallace, M.J. (1990) Organizational Behavior and Performance: (5th Ed.) Scott, Foresman and Company, Illinois.
26. Tejaswini H., and Raob H.R. (2009) ‘Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness’, Decision Support Systems, Vol. 47, No. 2, pp.154–165.
27. Tipton, H., and Krause, M. (2007) Information Security Management Handbook, Auerbach Publications.
28. Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008) ‘Process-variance models in information security awareness research’, Information Management & Computer Security, Vol. 16, No. 3,pp. 271-287.
29. Van Niekerk, J., and Von Solms R. (2010) ‘Information security culture: A management perspective’, Computers & Security, Vol. 29, Pp. 476-486.
30. Vroom, C., and von Solms, R. (2002) A Practical Approach to IS Security Awareness in the Organization, in Security in the Information Society: Visions and Perspectives. In Proceedings of IFIP TC 11 17th International Conference on IS Security, Boston: Kluwer Academic Press, p19-38.
31. Vroom, C., and von Solms, R. (2004) ‘Towards Information Security Behavioural Compliance’, Computers and Security, Vol.23, No. 3, pp.191-198.
32. Willison, R. (2006) ‘Understanding the Perpetration of Employee Computer Crime in the Organisational Context’, Information and Organization, Vol. 16 No. 4, pp.304-324.
33. Yau, C.H., Tan, Y.Y. Fong, A.S. and Mok, P.L. (2008) ‘Embedded Architectural Design Using Protection Logics to Defend Attack of Buffer Overflow and Unauthorized Access of Code’, in IEEE 8th International Conference on Computer and Information Technology Workshops, 8-11 July 2008, pp.265.