

DETERMINANTS OF INFORMATION CONFIDENTIALITY IN TECHNICAL AND VOCATIONAL EDUCATION AND TRAINING INSTITUTIONS IN KIAMBU COUNTY, KENYA

Kathenya M. Dorcas

Jomo Kenyatta University of Agriculture and
Technology
KENYA
carssyd@yahoo.com

Dr Agnes Njeru

Jomo Kenyatta University of Agriculture and
Technology
KENYA
agneswnjeru@yahoo.co.uk

CITATION: Dorcas, M., K., & Njeru, A. (2016). Determinants of Information Confidentiality In Technical And Vocational Education And Training Institutions In Kiambu County, Kenya. *International Journal of Strategic Management*. Vol. 5(5). PP.73-88.

ABSTRACT

TVET institutions in Kiambu County are increasingly reliant on automated and interconnected systems to perform functions essential to their lecturers welfare, and hence the increase in the Information confidentiality due to the high dependence on technology. In relation to this, this study sought to establish the effect IT literacy, IT policies, top management commitment and organizational resources as determinants of Information confidentiality in TVET institutions in Kiambu County. To achieve these objectives, this study employed descriptive survey. The population of interest of this study was lecturers, IT technicians and IT students in TVET Institutions in Kiambu County. This study used stratified random sampling to get a study sample of 62 respondents. This study collected data using a semi-structured questionnaire. The study used drop and pick later method to collect data. Prior to the data collection, a pilot study was conducted to allow for pre-testing of the research instrument to increase validity and reliability. The study used both qualitative and quantitative methods of data collection. Further, the study employed a multivariate regression model to study the relationship between independent variables and the dependent variable. The study found a significant positive relationship between information confidentiality and IT literacy, IT policies, top management commitment and organizational resources. The study therefore recommends information confidentiality awareness and training program to boost IT literacy. It further recommends that the organizations should align

their IT policies with organizational goals to make it everyone's responsibility to achieve information confidentiality. The top management should provide resources to ensure that information confidentiality managers attends industry-specific education and executive-level continuing training. Abstract should be given here in the same font and format as given here. Please do not change the format. Abstract should be between 200-300 words followed by 3-5 keywords.

Keywords: Information confidentiality, IT literacy, IT policies, Top management, Organizational resources

INTRODUCTION

According to Besnard and Arief (2005), employees may ignorantly or negligently contribute to Information confidentiality risks – for example, by unwittingly retrieving spam electronic mail, opening virus e-mail attachments, or dismissing Information confidentiality threats as unimportant in comparison with other needs such as usability. Recent survey by McAfee (2005) in an article, “threat within” indicated that; twenty-one per cent of workers allowed family and friends to use company laptops and personal computers for internet access; fifty-one per cent of workers connect their own devices or gadgets to their company personal computer; sixty per cent of workers stored personal content on their company personal computer; ten per cent of workers downloaded prohibited content at work; while sixty per cent of workers stored personal content on their company personal computer. This indicates high company information exposure to risk.

In another study by Tarimo et al. (2006) conducted in Tanzania, it is found that there is lack of personnel and resources to support information confidentiality education at colleges and universities that is one reason for lack of information confidentiality culture. Hence the study revealed that cultivating security culture is neither simple nor easy and information confidentiality is not an issue that could be addressed entirely by organizations alone; rather, many factors outside the scope of an organization have to be considered. Alnateer & Nelson (2009) have also highlighted the importance of information confidentiality management factors and cultural factors in Saudi Arabia and the study disclosed a gap in terms of addressing the influences of both Information confidentiality factors and cultural factors on the adoption of confidentiality culture in Saudi Arabia context.

In response to the heightened information confidentiality risk that companies are exposed to, many companies have developed an interest in cultivating intuitive — rather than enforced — employee adherence to information confidentiality policy, processes and procedures (Dhillon 2001). Such companies are interested in the institutionalization of information confidentiality practices as information confidentiality culture. The potential value of adopting a socio-cultural approach to information confidentiality management was recently highlighted by Galletta and Polak (2003). Their study revealed that peer and supervisory culture may be highly influential in the management of internal internet misuse and abuse. However, while progress has been made globally in the enculturation of information confidentiality, more is needed (Ernst & Young 2006).

Statement of the problem

TVET Institutions in Kenya are increasingly reliant on automated and interconnected systems to perform functions essential to their lecturers' and students welfare and services. However, the factors that benefit TVET Institutions operations, speed of processing and access to information, increase the risks of computer intrusion, fraud, and disruption. TVET Institution systems in Kenya are increasingly becoming more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. However, despite these risks, TVET Institutions have not put in place adequate measures to counter the risks. Knapp et al. Many empirical researches have been done in the area of information confidentiality. Dojkovski, Sneza, Sharman and John, (2010) did an interpretive study in Australia on fostering information confidentiality culture in small and medium size enterprises and found out that future of information security is complex and threats more sophisticated and data breaches more damaging. They also found that most secure organizations spend time and money on staff and until there is staff training awareness, then the organization is not secure. Also, in Ethiopia, Gebrasilase and Lessa (2011) did a study to ascertain the nature of information confidentiality culture in public hospitals in Hewassa. They found that information confidentiality is a vital tool within hospital environment playing a leading role in the protection of patients' information and privacy. The hospitals also manage huge amount of information and databases and all this has to be duly protected to guarantee the quality and make sure information is used only for rightful purpose.

Further, TVET institutions fail to allocate adequate resources and IT policies to counter the risks. This indicates that there are still a lot to be done to curb information insecurity in TVET Institutions in Kiambu County in Kenya.

However, despite the massive inquiry into Information confidentiality, none of these studies has been done to establish the role of IT literacy, IT policies and regulations, top management commitment and organization's resources as determinants of Information confidentiality in TVET Institutions in Kiambu County in Kenya.

Objectives of the Study

General objective

The overall objective of the study was to establish the determinants of Information confidentiality in TVET Institutions in Kiambu County.

Specific Objectives

1. To establish the influence of IT literacy on Information confidentiality in TVET Institutions in Kiambu County, Kenya.
2. To determine effect of IT policies on Information confidentiality in TVET Institutions in Kiambu County, Kenya.
3. To explore the influence of top management commitment on Information confidentiality in TVET Institutions in Kiambu County, Kenya.

4. To establish the influence of organizational resources on Information confidentiality in TVET Institutions in Kiambu County, Kenya.

Significance of the study

Ensuring that there is an effective organizational Information confidentiality culture where lecturers intuitively protect institutions information assets, TVET Institutions could improve information confidentiality. Therefore, this study would help TVET Institutions in Kiambu County and other institutions alike, as it highlights key challenges of promoting a behavioral and learning approach to Information confidentiality to complement traditional technological and managerial approaches for TVET Institutions. The study would therefore make recommendations to counter the challenges for a successful development of Information confidentiality culture in the Institutions.

Further, the management of the institutions, would benefit from this study from adopting a risk-based approach to Information confidentiality and was educated about the potential strategic role of information technology and Information confidentiality

This study also would be of value to scholars. This is because, it adds to the existing pool of reference material in the field of Information confidentiality. Further, the study would form basis for further research on the gaps that were identified and recommended for further research.

Limitations of the study

The geographical scope of the study was Kiambu County from which TVET institutions were sampled. The researcher however expected some hindrances while conducting the study. The researcher anticipated low generalizability of finding, where the findings could not be used to present a general picture of state of TVET institutions in Kenya. However, to mitigate this, the study selected adequate sample that is scientific, conforms to law of large numbers and central limit theorem whereby a sample of 30 cases is considered normally distributed. Therefore a sample of 62 respondents was adequate. With these, generalizations were made assuming that the sample was large enough and scientifically selected.

The researcher further anticipated uncooperative respondents. To counter this challenge, the study assured the respondents of confidentiality of information that they gave and that the information they gave would be used for academic purposes and where applicable may influence policies that would have positive implications on information security in their organizations.

The researcher anticipated that the respondents may be biased in giving out information or giving guarded responses which would compromise the study's objectivity and reliability. This limitation was overcome by explaining to the sampled population the essence of the study. Further, the researcher assured the respondents that no one would be victimized on the information that they gave.

LITERATURE REVIEW

The study reviewed relevant literature in line with the objectives of the study to analyse the determinants of information confidentiality in Technical vocational and Educational Training Institutions in Kiambu County in Kenya. The review also identifies the research gaps and areas for further research.

Theoretical Review

Theory of planned behavior

This is a theory about the link between beliefs and behavior. The concept was proposed by Ajzen (1991) to improve on the predictive power of the theory of reasoned action by including perceived behavioural control (Ajzen, 1991). It is one of the most predictive persuasion theories. It has been applied to studies of the relations among beliefs, attitudes, behavioral intentions and behaviors in various fields such as advertising, public relations, advertising campaigns and healthcare. The theory states that attitude toward behavior, subjective norms, and perceived behavioral control, together shape an individual's behavioral intentions and behaviors. In relation to the study, this theory can be used to explain lecturers' intention to abide by IT policies to ensure Information confidentiality in their institutions. This is because the policies put in place would predict how the lecturers handle IT resources in an institution.

Resource-Based Theory

This theory suggests that organizational resources that are costly or hard to imitate help organizations retrieve competitive advantage. In the case of this study, competitive advantage is looked at in terms of information confidentiality culture. One resource-based research stream has considered the functional capabilities of IC as the source of competitive advantage (e.g., Bharadwaj, 2000). Another perspective has focused on how resources are channeled and utilized to bring competitive advantage (e.g., Ravichandran & Lertwongsatien, 2005). However, both streams agree that resource availability determines information confidentiality capabilities and further affects organizational performance (Ray, Muhanna & Barney, 2005).

From a resource-based view, Information confidentiality culture is enacted through the resources of organizations. Powell and Dent-Micallef (1997) categorized organizational resources as human, business, and technology. Human resource relates to people and ambiance of organizations, including culture, communication, consensus, CEO commitment, and strategy integration. Business resource relates to process and policy, including supplier relationship, training, process, and performance benchmarks. Technology resource includes computer hardware and software. Adequate resources ensure that organizations can adequately foster Information confidentiality culture. Without sufficient monetary, employee support and management support (resources) it will be hard to achieve information confidentiality culture.

Cognitive Learning Theory

This theory states that humans generate knowledge and meaning through sequential development of an individual's cognitive abilities, such as the mental processes of recognize,

recall, analyze, reflect, apply, create, understand, and evaluate. The Cognitivists' (Piaget 1976; Bruner 1960; Bruner 1966) learning process is adoptive learning of techniques, procedures, organization, and structure to develop internal cognitive structure that strengthens synapses in the brain. The learner requires assistance to develop prior knowledge and integrate new knowledge. The purpose in education is to develop conceptual knowledge, techniques, procedures, and algorithmic problem solving using Verbal/Linguistic and Logical/Mathematical intelligences. The learner requires scaffolding to develop schema and adopt knowledge from both people and the environment. The educators' role is pedagogical in that the instructor must develop conceptual knowledge by managing the content of learning activities. The theory insists that the learner is expected to use skill and knowledge obtained during learning to solve problems in real life situations (Wood, 2003). Similarly, to develop information confidentiality culture in an organization, employees in the organization needs to be well equipped with skill and knowledge to know do and don'ts to safeguard the organizational information. Therefore, IT literacy is of essence in fostering information confidentiality culture in an organization and therefore TVET Institutions should endeavor to employ qualified lecturers in areas of IT and also ensure that all the lecturers have at least basic knowledge in use of a computer.

Three-Component Model of Commitment

This model proposes that organizational commitment is experienced by the employee as three simultaneous mindsets encompassing affective, normative, and continuance organizational commitment. Affective Commitment reflects commitment based on emotional ties the employee develops with the organization primarily via positive work experiences. Normative Commitment reflects commitment based on perceived obligation towards the organization, for example rooted in the norms of reciprocity. Continuance Commitment reflects commitment based on the perceived costs, both economic and social, of leaving the organization. This model of commitment has been used by researchers to predict important employee outcomes, including turnover and citizenship behaviors, job performance, absenteeism, and tardiness (Meyer et al., 2002). Meyer and Allen (1997) provide a comprehensive overview of the theoretical lineage of this model. However, in this study, the model is used to predict lecturers' behaviors towards information confidentiality in an institution based on the level of top management commitment.

The three components may be used to describe affective attachment to information confidentiality in the organization, perceived costs of neglecting it, and a felt obligation to abide by policies to enhance Information confidentiality. The affective component is defined as employees' emotional attachment to, identification with, and involvement in ensuring Information confidentiality in the organization. This is in response to top management commitment in ensuring Information confidentiality in the organization. The continuance component in the case of Information confidentiality and management commitment may be look at as the perception of costs associated with risk of Information confidentiality absence in an organization. The normative component may describe the top management commitment leading to employees' feelings of obligation to abide by policies to ensure information confidentiality in the organization. In fact, Thong *et al.*, (2004) notes that top management participation in information confidentiality initiatives gives an impression of their support, and other employees will not see initiatives as an extra burden but a signal of how to value the initiatives.

Conceptual Framework

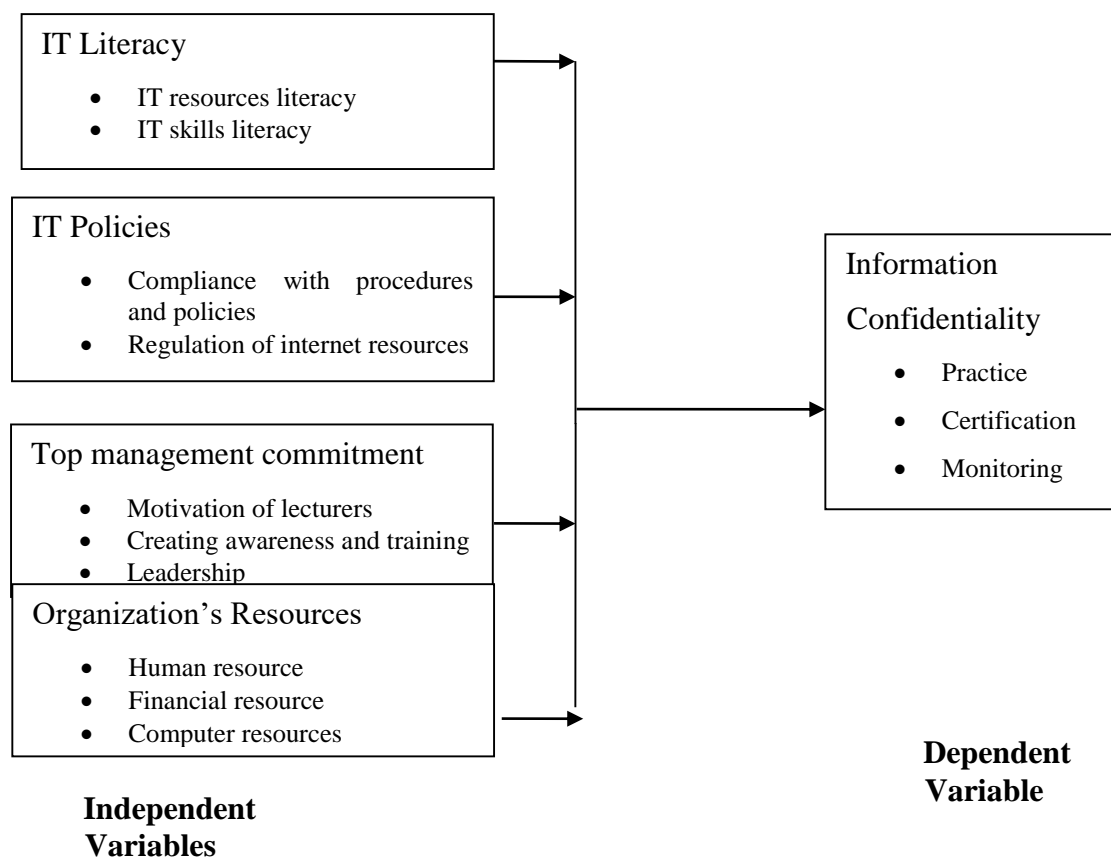


Figure 2.1: Conceptual Framework

Empirical Review

Information confidentiality face lots of challenges due to several factors such as the development of Information Technology. Henry (2006) established that it is vital that employees are adequately trained to protect the information assets in their organization. Henry notes that properly trained and diligent employees can become the strongest link in an organization's security infrastructure. Doherty and Terry (2009) in their study established that

organizations are not able to protect the confidentiality of information if they do not ensure that all employees involved understand their roles and responsibilities through adequate training.

Appari & Johnson (2010) indicated that IT policies are a key determinants of Information confidentiality. They noted that an IT policy outlines do and don'ts in an organization. Berti and Rogers, (2004) in their study indicated that the most significant vulnerability for many organization in regard to Information confidentiality is human factor. They however noted that this is often left unaddressed. Berti and Rogers notes that human factor can simply be addressed through introduction of policies and training.

Ruighaver (2007) pointed that Information confidentiality should not only be investigated in a simplistic manner focusing on end-users and on the technical aspects but also it should have a management focus as it is a management problem.

In a study by Tarimo et al. (2006) conducted in Tanzania, it is found that there is lack of personnel and resources to support Information confidentiality education at colleges and universities which is a major set back in achieving Information confidentiality. Hence the study revealed that Information confidentiality is not an issue that could be addressed entirely by organizations alone; rather, many factors outside the scope of an organization have to be considered.

Johnson and Koch (2006) in their study established that a challenge facing information confidentiality is lack of top management commitment. Johnson and Koch indicated that management is not supportive of information confidentiality in terms of budget or time, thus impacting the level of security awareness and security technology. In line with this, Gupta & Hammond (2005) study established that while organizations often use power surge protectors, they are unlikely to deploy encryption, firewalls, access control technologies and dial-back modems, this they noted that it threatens information confidentiality in an organization. Moreover, with fewer breaches, there will be fewer reports to business owners and thus information confidentiality may appear even less important and attract less management attention and support (Gupta & Hammond 2005).

Therefore, this study investigated the role of IT literacy, top management commitment, organizational resources and compliance to IT policies in fostering Information confidentiality culture in TVET Institutions in Kiambu County in Kenya.

Critique of the existing literature relevant to the study

Though literature indicates that there is inadequate implementation of Information confidentiality, some institutions fosters this culture. What lacks is clear explanation as to the motive behind the implementation. According to Kraemer and Carayon (2005) Information confidentiality culture is critical to the success or failure of overall Information System performance. While looking at it lightly, this makes sense, however, an organization that employs a positive Information confidentiality culture is not immune to Information confidentiality risks. This is because, other external challenges plays role in determining level of Information confidentiality in organizations.

Kankanhalli *et al.* (2005) highlights that organizations foster this culture as a result of the benefits associated. Maynard & Ruighaver (2006) found evidence to suggest that there are a number of organizations forced to conform to external audit and government regulation. Therefore, the implementation of security policies may not have derived from a belief in the importance of security practices but a result of external requirements. Hence, employees tend to consider Information confidentiality as inconvenience and new policies and associated controls are often met with resistance.

Ruighaver (2007), indicated that Information confidentiality issue should not only be investigated in a simplistic manner focusing on end-users and on the technical aspects but also it should have a management focus as it is a management problem. However, what Ruighaver fails to capture is that Information confidentiality culture can only be achieved if all the stakeholders would implement it in unison. Instead of stressing focus only on the management, the stress should be emphasized even on the employees who are main culprit of Information confidentiality culture.

Therefore, a study on determinants of Information confidentiality in TVET institutions in Kenya is of essence.

Research Gaps

Available literature notes that Information confidentiality receives little or no attention from the top management. It is indicated not to be a priority. However, it is not yet clear why even after realizing the need to ensure Information confidentiality, TVET Institutions still lack information confidentiality policies in place that governs the use of computers and network resources. The literature available also fails to describe the desirable employee characteristic that needs to be employed to ensure Information confidentiality in institutions. In addition, available literature is derived from other countries, and in fact from developed economies, therefore, the results obtained lack general applicability in TVET institutions situation in Kenya.

Mishra and Dhillon (2009) found organizations are inclined to treat security spending as a cost, and often fight to gain funding for security initiatives. Dojkovski (2011) argued that there is evidence that organizations will only adopt security functions after a major loss from a security incident. Security concern will remain low if there is no major loss due to lack of security. Along the same line, Tarimo (2006) found that computer security functions continue to face difficulties to get support from management in terms of resources allocation and training.

Therefore, the current study sought to establish the determinants of information confidentiality in TVET institutions in Kenya. The study sought to establish the role-played by IT literacy, IT policies, top management commitment and organizational resources in ensuring Information confidentiality in TVET institutions in Kenya.

METHODOLOGY

This study adopted a descriptive survey design which is a method of collecting information by interviewing or administering a questionnaire to a sample of individuals (Orodho, 2005).

According to Cooper and Schindler (2008), descriptive survey attempts to describe or define a subject, often by creating a profile of a group of problems, people, or events, through the collection of data and tabulation of the frequencies on research variables or their interaction .

The target population of this study was therefore drawn from 309 respondents which included 263 lecturers, 8 IT technicians and 38 IT students in two TVET institutions in Kiambu county (Thika Technical Training Institute and Kiambu Institute of Technology).

To collect data a semi-structured questionnaire with both close ended and open ended questions was used. Kombo and Tromp (2006) indicate that semi structured questionnaire refers to the use of already prepared questions during the study. The open-ended questions provided additional information that may not have been captured in the close-ended questions. The study was concerned with variables which cannot be directly observed such as opinion, perception and feelings of respondents. According to Oso, (2009), such information can best be described through questionnaires. Its purpose was to collect a lot of information over a short period of time.

Questionnaire was preferred in this study because respondents of the study are literate and quite able to answer questions asked adequately. Also, information required can easily be described in writing as indicated by (Oso, 2009). The questionnaire was developed in accordance with the research objectives. The questionnaire was kept short and structured with mostly multiple-choice selections in a likert scale.

The study collected quantitative data using a self-administered questionnaire which were delivered to the respondents. The filled questionnaires were then collected later through drop and pick later method.

RESULTS AND DISCUSSION

The study established that IT literacy influences information confidentiality in TVET institutions in Kiambu county to a great extent. The study also indicated that experience with IT systems, IT resources literacy and IT skills literacy influenced information confidentiality for the TVET institutions in Kiambu county to a very great extent. Further, tools literacy influenced information confidentiality in TVET institutions in Kiambu County to a great extent. The study established that the institutions conducts competency assessment that helps employees improve their learning skills and direct institutions to renovate functions, courses, and strategies and thus nature an information confidentiality culture; that knowledgeable employees are able to utilize their own knowledge and information to create value and enhance information confidentiality in an institution and that IT literacy provides the best workplace preparedness for the graduates especially the areas related to information confidentiality.

The study established that IT policies influence information confidentiality in the TVET institutions in Kiambu County to a great extent. The results also shows that majority of institutions had put in place policies to aid information confidentiality. Majority of the institutions were shown to have put enough effort to ensure that policies to aid information confidentiality are followed.

The study established that the use of internet resources in the companies is highly regulated, that IT policies in the companies are crystal clear, that employees in their company comply

with information confidentiality procedures and policies laid down and that information confidentiality policies ensure the confidentiality, integrity, availability, and better control of information assets. Further, the study indicated that the TVET institutions in Kiambu County forbid use of institution's computer and internet resources for personal use and that IT policy influence and determine employees' course of action on IT related issues in the institutions. The study also showed that the institutions are adapting training policies for all employees who handle computers and Internet resources to ensure reduced exposure to information confidentiality risks.

The study also established that top management commitment influences information confidentiality in TVET institutions in Kiambu County to a great extent. The study also illustrated that top management originates activities that allows business to achieve its objectives, vision and mission, that top management play an important role in expediting the implementation of information system security initiatives as well as bringing ISM alignment with the corporate objective and strategies and that lack of commitment of the top management to information confidentiality support leads to inadequate planning.

Further, the study indicated that top management in TVET institutions in Kiambu County in Kenya are involved in allocation of organizational resources to address information confidentiality and other risks and motivates employee towards achieving information confidentiality.

According to the study results, organization resources influence information confidentiality in TVET institutions in Kiambu County in Kenya to a great extent. Further, the study established that human resource, specialized knowledge, computer and Internet resources and financial resources are organizational resources that influences information confidentiality of TVET institutions in Kiambu County to a great extent.

The study has also shown that the TVET institutions in Kiambu County conducts constant training to develop human resource on areas of information confidentiality and that their company hires qualified human resource to ensure information confidentiality. Further, the study indicated that TVET institutions in Kiambu County possesses a portfolio of unique, technologically-oriented resources/capabilities needed to develop, implement and support information systems and that the management in the TVET institutions in Kiambu County are willing to invest in system and equipment that would support information confidentiality in the institutions. Also, it was established that TVET institutions in Kiambu County makes budgetary allocations aimed at improving level of information confidentiality and that the management motivates best employees in regard to information confidentiality through reward and promotions.

Regression Model summary of Independent Variable on the dependent variable

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
--------------	------------------------------------	----------------------------------	----------	-------------

		B	Std. Error	Beta		
1	(Constant)	1.207	1.2235		1.615	0.367
	IT Literacy	0.752	0.1032	0.152	4.223	.0192
	IT policies	0.687	0.3425	0.054	3.724	.0239
	Top Management Commitment	0.545	0.2178	0.116	3.936	.0251
	Organizational Resources	0.439	0.1937	0.263	3.247	.0454

The study conducted a multiple regression analysis so as to determine the relationship between determinants of Information Confidentiality in TVET institutions and the four variables investigated in this study. The regression equation $Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \varepsilon$ was:

$$Y = 1.207 + 0.752X_1 + 0.687X_2 + 0.545X_3 + 0.439X_4$$

Whereby Y = Information Confidentiality

X₁ = IT literacy

X₂ = IT Policies

X₃ = Top management commitment

X₄ = Organizational resources

According to the regression equation established, taking all factors into account (IT literacy, IT policies, top management commitment and organizational resources) constant at zero, information confidentiality will be 1.207. The data findings analyzed also shows that taking all other independent variables at zero, a unit increase in IT literacy will lead to a 0.752 increase in information confidentiality; a unit increase in IT policies will lead to a 0.687 increase in information confidentiality, a unit increase in top management commitment will lead to a 0.545 increase in information confidentiality and a unit increase in organizational resources will lead to a 0.439 increase in information confidentiality. This infers that IT literacy contribute most to the information confidentiality followed by IT policies.

RECOMMENDATIONS

The study recommends that training programs should be conducted to ensure that personnel at all levels of the organization understand their information confidentiality responsibilities and that they properly use and protect the information resources entrusted to them. Creating

awareness offers a blended solution of activities that promotes security, establishes accountability, and informs the workforce of security concerns. Training strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role.

The study recommends that organizations should make IT policies that align information confidentiality with the organization's objectives and make it everyone's responsibility to achieve information confidentiality. Information confidentiality is frequently perceived as the responsibility of the information confidentiality department. This perception is generally perpetuated through information confidentiality initiatives being funded as stand-alone projects and the failure to inform employees of their role in the protection of information and intellectual property assets. Also, the study recommends that the information confidentiality status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

An information confidentiality strategy that is aligned with the company's risk management and corporate governance requirements should be developed and implemented. Further, organization policies put in place should seek to ensure that each line of business that "owns" information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information confidentiality manager to ensure that requirements are properly reflected and prioritized in the information confidentiality strategy.

Further, the study recommends that over time, information confidentiality efforts should be revised based on changes in organization's mission, operational requirements, threats, environment, or deterioration in the degree of compliance. Periodic assessments and revision can be a valuable means of identifying areas of noncompliance and addressing them. Executives should ensure a life-cycle approach to compliance by monitoring the status of their programs to ensure that ongoing information confidentiality activities are providing appropriate support to the organization; policies and procedures are current; and security controls are accomplishing their intended purpose.

The study recommends that top management should communicate consistently that every employee is accountable for information confidentiality by ensuring that expectations are clearly communicated in the company's information confidentiality policies and standards, and consistently demonstrate that violations will not be tolerated. The top management should ensure that every employee, including management, attends an information confidentiality awareness update annually and new employees should be appropriately informed of the company's information confidentiality concepts and practices.

The study also recommends that senior management in TVET institutions in Kiambu County should ensure that all requests for technology expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request. Further, the study recommends that the top management provides funds to ensure that information confidentiality managers attends industry-specific education and executive-level continuing training to increase their understanding of the business information confidentiality related risks and enhance their skills in addressing these challenges.

CONCLUSIONS

The study concludes that IT literacy influences information confidentiality in TVET institutions in Kiambu County to a great extent. The study showed that experience with IT systems, IT resources literacy and IT skills literacy were elements of IT literacy that influenced information confidentiality in TVET institutions in Kiambu County in Kenya. In acknowledgement of importance of IT literacy as a critical element of information confidentiality, it was established that the TVET institutions in Kiambu County conducts competency assessment that helps employees improve their IT skills and direct organizations to renovate functions, courses, and strategies and thus nature an information confidentiality culture. Also, TVET institutions in Kiambu County studied were indicated to employ IT literate individuals in the IT department.

On the role of IT policies as a determinant of information confidentiality in TVET institutions in Kiambu County, the study concludes that IT policies are determinants of information confidentiality in institutions. To this end, the institutions studied had put in place IT policies to enhance information confidentiality. In the TVET institutions in Kiambu County studied, efforts are put in place to ensure that policies to aid information confidentiality are followed. This ensures that employees in TVET institutions in Kiambu County comply with information confidentiality procedures and policies laid down. IT policies in the institutions studied were indicated to be crystal clear, these policies ensures confidentiality, integrity, availability, and better control of information assets. Most of the institutions have in place policies that forbid use of institution's computer and Internet resources for personal use.

The study has concluded that the top management commitment influences information confidentiality in TVET institutions in Kiambu County to a great extent. Top management in TVET institutions in Kiambu County play an important role in expediting the implementation of information system security initiatives as well as bringing ISM alignment with the corporate objective and strategies. The top management's support is responsible for initiating awareness and training programs, committed to the Information confidentiality Policy. Top management facilitates education and training for employees to ensure awareness on information asset protection while ensuring consistent enforcement of information confidentiality policies and standards.

Further, the study concluded that organizational resources influences information confidentiality in TVET institutions in Kiambu County in Kenya to a great extent. The organizational resources established to influence information confidentiality in the TVET institutions in Kiambu County include human resource, specialized knowledge, computer and Internet resources and financial resources. The TVET institutions in Kiambu County conducts constant training to develop human resource on areas of information confidentiality and also hires qualified human resource to ensure information confidentiality. TVET institutions in Kiambu County also make budgetary allocations aimed at improving level of information confidentiality.

The study also concludes that there is a positive relationship between information confidentiality and IT literacy, IT policies, top management commitment and organizational resources. All factors had a significant p-value ($p < 0.05$) at 95% confidence level. The most significant factor was established to be IT literacy, followed by IT policies then top

management commitment while organizational resources was the least significant among the factors.

REFERENCES

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50 (2), 179–211.
- Alnatheer, M. & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia.
- Appari, Ajit & M. Johnson, Eric (2010) Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management*, Vol. 6, No. 4.
- Besnard, D. & Arief, B. (2005) Computer Security Impaired by Legitimate Users, *Computers & Security*, 23, 253-264.
- Cooper, D. R., and Schindler, P. S. (2008). *Business Research Methods* (8th edn). McGraw-Hill: New York.
- Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security*; Vol.20, No.2, pp.165-172.
- Ernst & Young (2006) *2006 Global Information Security Survey*, Ernst & Young.
- Gebrasilase, Temesgen and Lessa, Lemma Ferede (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital, *The African Journal of Information Systems*, 3(3:1).
- Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small businesses, *Information Management & Computer Security*, 13(4), 297-310.
- Johnson, D.W. & Koch, H. (2006). Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, IEEE Society Press.
- Knapp, K.J., Marshall, T.E., Rainer, R.K., Ford, F.N. (2006). Information security: management's effect on culture and policy, *Information Management & Computer Security*, 14(1), 24-36.
- Kraemer, S., Carayon, P. (2005) Computer and Information Security Culture: Findings from Two Studies. *Proceedings of the Human Factor and Ergonomics Society 49th Annual Meeting*.16, 293-314.
- McAfee (2005) *The Threats Within*, McAfee.

- Mishra, S. & Dhillon, G. (2009). Information systems security governance research: a behavioral perspective, *Presented at 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, New York, USA.
- Ordho, A.J. (2005) *Essentials of Educational and Social sciences Research Methods*. Nairobi: Masola Publishers
- Oso, W. Y., and Onen, D. (2005). *A Guide to writing Research Proposals and Reports*. Option Press: Kisumu.
- Ruighaver, A.B., Maynard, S.B., Chang, S. (2007) Organizational security culture: Extending the end-user perspective. *Computers & security*, 26, 56–62. Ruighaver, A.B., Maynard, S.B., Chang, S. (2007) Organizational security culture: Extending the end-user perspective. *Computers & security*, 26, 56–62.
- Tarimo, C. N., Bakari, J. K, Yngström, L., & Kowalski, S. (2006). A Social-Technical View of ICT Security Issues, Trends, and Challenges: *Towards a Culture of ICT Security - The Case of Tanzania*
- Thong, J. Y. L., Yap, C. S., & Raman, K. S. (2004). Engagement of External Expertise in Information Systems Implementation, *Journal of Management Information Systems*, 11, 2, 209-231.