An Investigation of the Information Security Strategies Implementation in Further Education and Training Colleges in Limpopo: A Case Study

Mohlabeng M.R[1], Mokwena S.N[1], Osunmakinde I.O[2]
[1] Faculty of ICT: Computer Science
Tshwane University of Technology
South Africa
[2] Faculty of College of Science
Engineering and Technology
University of South Africa
{MohlabengMR, MokwenaSN}@tut.ac.za, osunmio@unisa.ac.za

ABSTRACT: *The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function within Higher Education Institutions. The aim of the research was to investigate the implementation of information security strategies in Further Education and Training (FET) colleges in Limpopo South Africa. The study has shown that there was lack of information security strategies matter which may be addressed by awareness and education for all staff of FETs. A survey questionnaire was administered to the personnel of Further Education and Training in Limpopo Province of South Africa. The researchers have proposed a technical model that might be used at FETs to address security breaches and awareness among employees.*

Keywords: Information security, Further Education and Training, Data Loss, Policy, Awareness

Received: 13 August 2012, Revised 4 October 2012, Accepted 16 October 2012

1. Introduction

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function within higher education institutions [14].

According to [12], Higher Education Institutions (HEI) may be attacked by different information security threats emanating internally or externally. These information security threats may be in the form of software attacks, technical software errors, human error or failure, and intentional act of information extortion.

HEIs have experienced data loss in the form of examination papers theft in 2006 [7]. This loss may have been caused by user's accidentally opening files with a virus on their computers. These attacks may have been caused by hackers targeting higher education institution [5].

Figure 1 shows data loss over time and various incidents that have occurred over a period of time that have resulted in data loss.

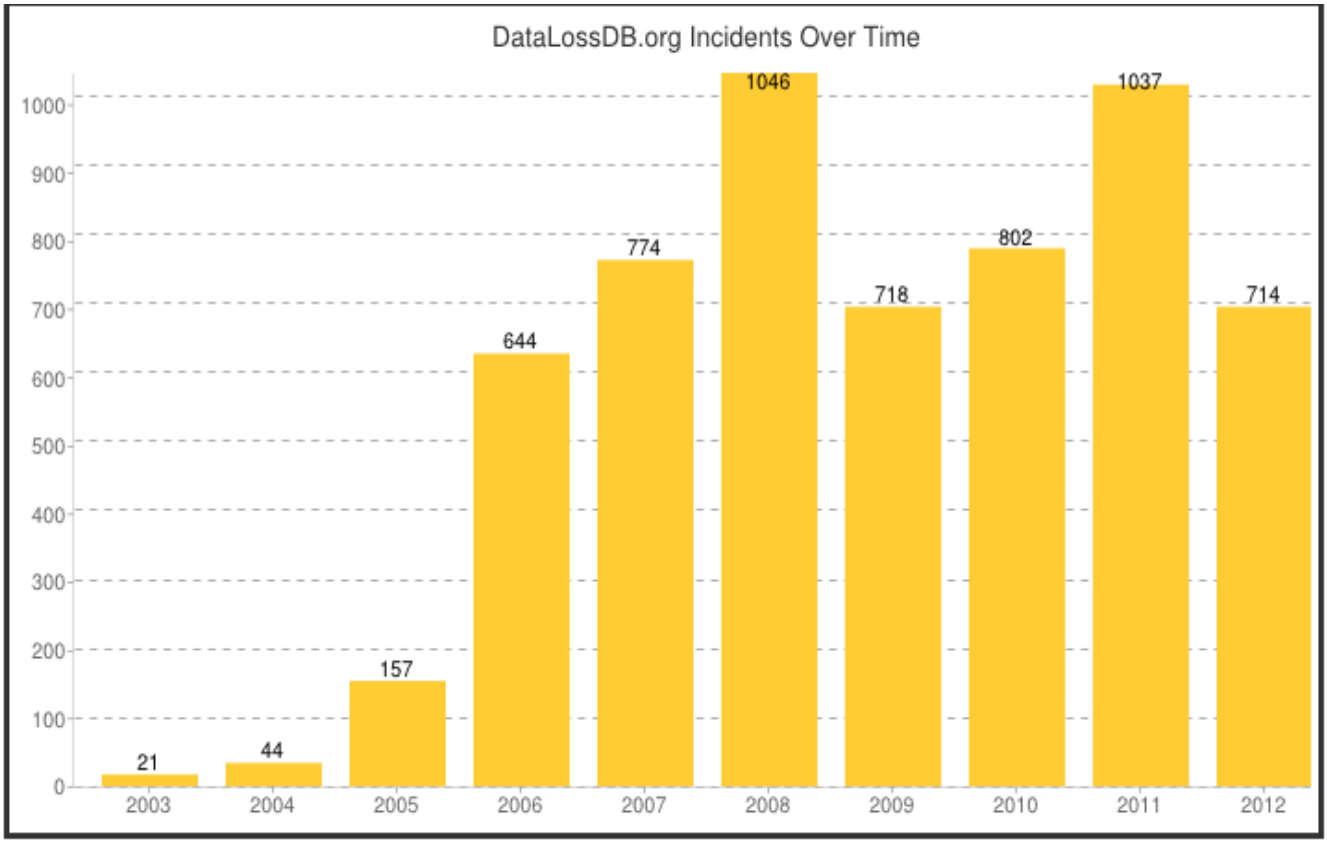

Figure 1. Data losses over time (Open Security Foundation, 2012)

Figure 1 depicts growth in data losses that have proportionally increased from 21 security incidents to 1046 security incidents between 2005 and 2008. The data losses started to decrease in 2009 from 1056 to 718 security incidents. Then in the years 2010 and 2011 there was a slight rise of security incidents from 802 to 1037. In July 2012 , the number was still at 718 security incidents. These have impacted negatively on the higher education institutions. The security incidents are categorized in figure 2.

Figure 2 shows how data was lost in different ways as indicated in below:

- Data may be lost through the hacker trying to gain access unlawfully also shown by 22%.
- Data may also be lost through fraud indicated by 12%.
- Viruses and stolen laptops (14%) may also contribute to the loss of data.
- Web site takes part in data losses with 10% and 7% of dispose of documents.

The researcher has made some contributions towards minimizing the data losses.The major contributions in this paper are the following:

1. Development of new technical security model based on modified ISO/IEC 27002 by [3].

2. Application and evaluation of the proposed model using real life network security data publicly available on [6] and network data captured from the FET College.

2. Background

This section examines current internationally accepted information system (IS) and information technology (IT) related approach in order to establish the theoretical foundations for this study. The theoretical perspectives are used in the investigation of

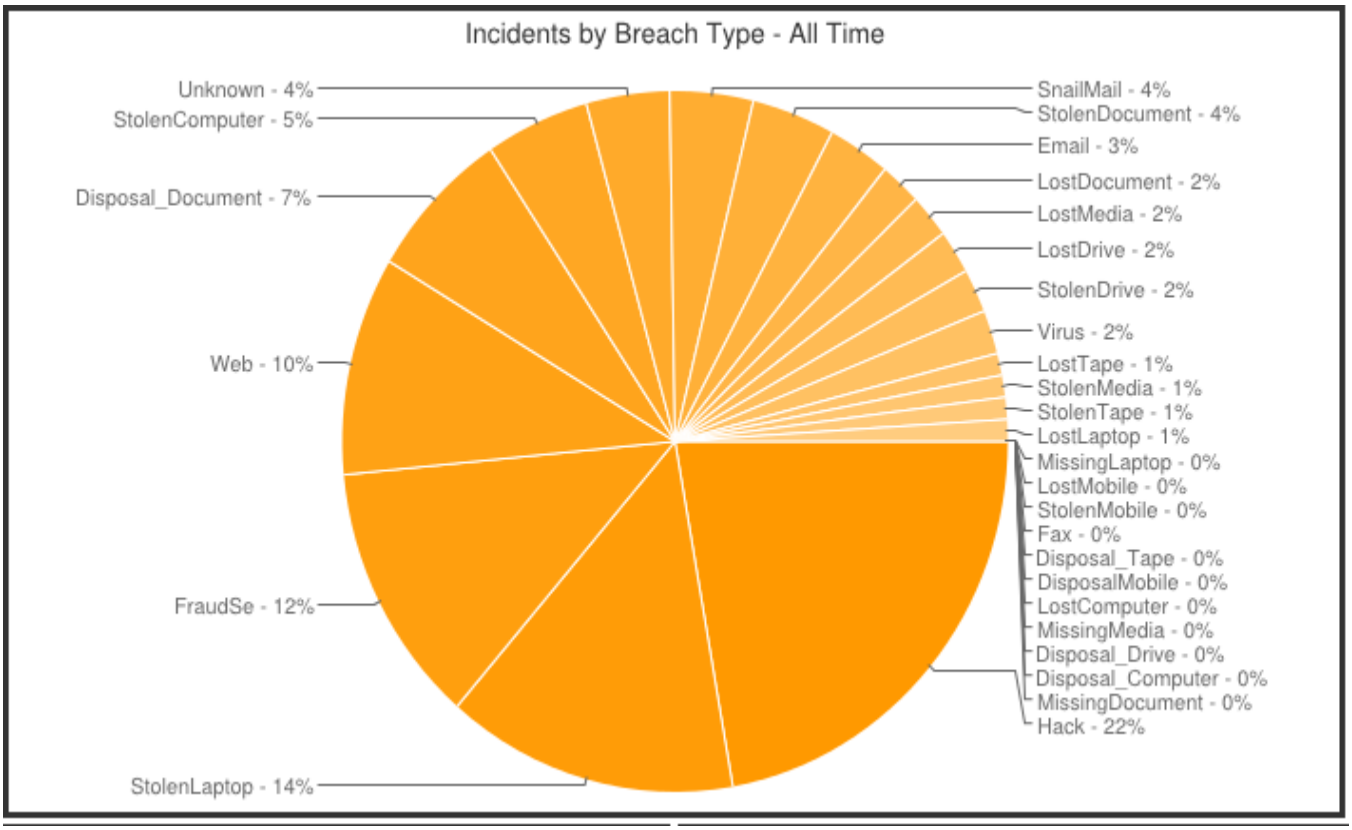

Figure 2. Incidents security breach (Open Security Foundation, 2012)

implementation of information security strategies in FET colleges.

This study is based on [3] modified international organization for standardization and the international electro-technical commission (ISO/IEC) 27002 information security framework. This framework consist of main components which are security policy, training and awareness and reporting.

2.1 Related Work

According to Farlex (2011), Information Security is the safeguard of information and information systems against illegal access or alteration of information. This study deals with College as Higher Education Institution. Information security is critical within HEI in order to protect the institution's information. Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction [9].

According to [10], the information security policy may play significance in preventing, detecting and responding to security breaches. The information security policy may also be proactively protect the availability, confidentiality and integrity of higher education institution's information resources ([1] David, 2002).

Information security policy may be crucial in protecting the information which has been established broadly in both the research and industry fields [8] [11]. Having a proper information security policy might lead to a better information security awareness.

Information security may present itself into three main categories: awareness, training and education. Security awareness programs are intended to enable user to focus on security related issues such as risks, threats and vulnerabilities: and awareness programs may be designed to enable users to handle all security matters that do not need particular technical knowledge. Security awareness programs may require lot on the trainers to acquire information [13]. Higher education institution may improve their security by providing awareness and training for various staff members, in order to minimize security breaches.

2.2 Underpinning Framework

This study is based on [3] modified ISO/IEC 27002 framework. This framework consists of the main components security policy, training and awareness and reporting. It is further highlighted two aspects added under security policy which are roles & responsibilities and security guidelines & standards. It is also further subdivided under roles & responsibilities into security management processes and risk management and under security guidelines & standards into technical security architecture, detailed technical procedures and asset classifications as shown by figure 3 which is dealt with in details below:

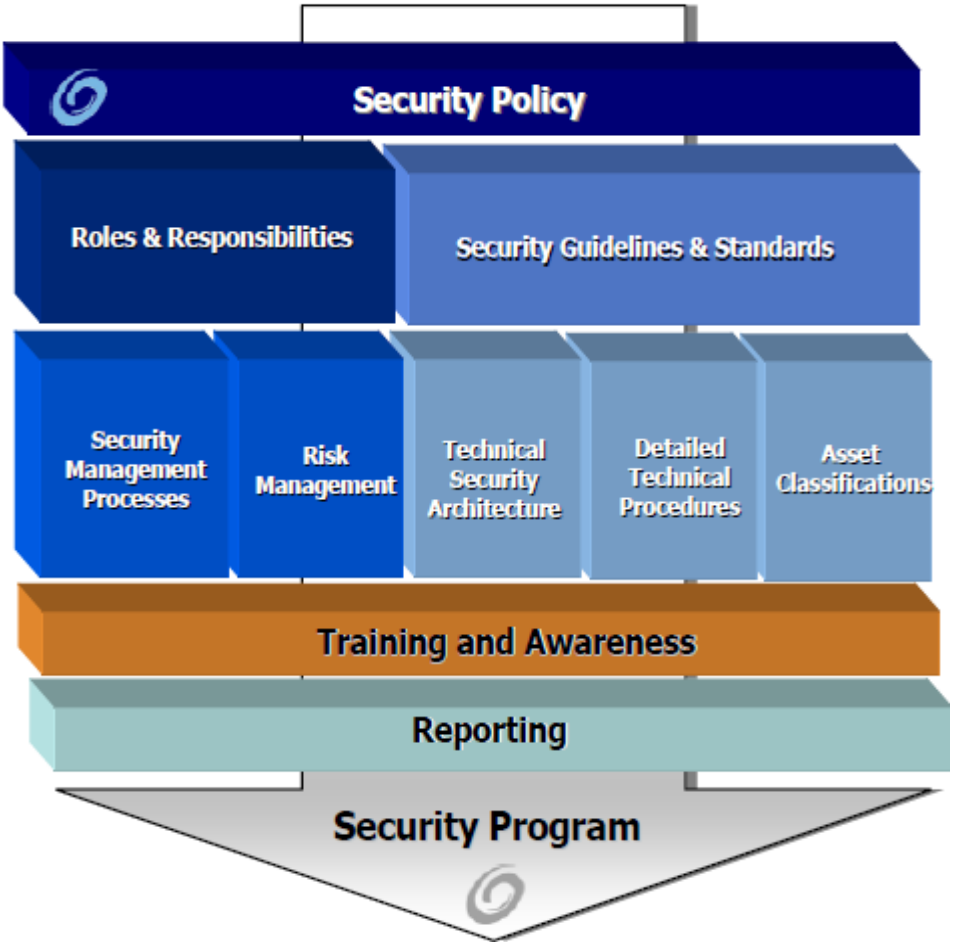

Figure 3. Information security framework

[3] modified ISO/IEC 27002 framework components are indicated below:

• Roles and responsibilities

The roles and responsibilities for information security throughout the organization may need to be defined clearly and well understood. These serves as a guidance for those with responsibility for directing and managing information security resources to oversee an information security function.

• Security guidelines and standards

Security guidelines and standards may assist in planning for information security management for organization. The guidelines may always be suggested to be effective security practices and internationally accepted standards related to information security.

• Security management processes

Security management processes may cover the creation, management and oversight of policies to ensure the prevention, detection and correction of security violation. These entails risk analysis, risk management which may also include the

establishment of accountability, management controls physical security and penalties for the abuse and mishandling of its assets in cooperation of physical and electronic formats.

• Technical security architecture

Technical security architecture may focus on the mapping among the control architecture and the safeguard processes. These mainly describe standards for protection settings that may be implemented by technical methods and identifies what may usually be called technical security policy.

• Training and awareness and security program

Information security awareness may assists organizations in changing their employees into the main effective security control by:

≡ Increasing awareness concerning the need for information security at all staff level.

≡ Increasing awareness concerning benefits of using the security architecture

This modified framework is more relevant to this study because all of components will be facilitated by training and awareness and also highlights the reporting component which will improve the implementation of information security.

3. Methodology

This section presents the research design of this study. The data was collected using survey method based on the questionnaire. Then the proposed technical security model was designed based on the research questions which are aligned with combination of both questions in the questionnaires and hypotheses. The alignment of the questions in the questionnaire and hypotheses is shown later in figure 4.

3.1 Research Design

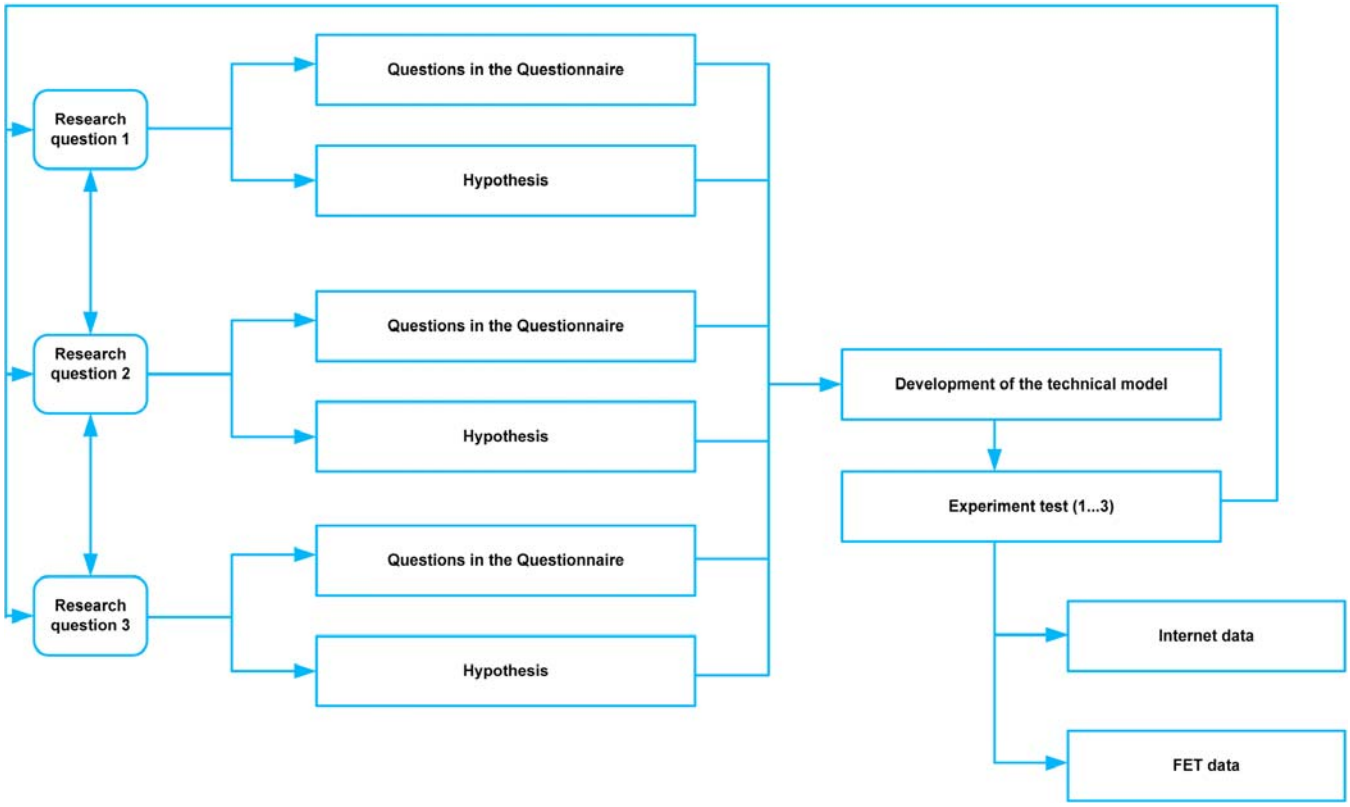

Figure 4. Summary of the research design

This research was guided by three research questions . The permission to conduct this study in the Capricorn FET College was approved by the Chief Executive Officer (CEO). The participants were made aware and participated voluntarily. The respondents to the survey questions were Capricorn FET information technology (IT) technical, lecturing and administrative staff in Limpopo Province.

The data was collected using the questionnaire designed based on the hypotheses. A total of 65 questionnaires were distributed to three campuses (Polokwane, Seshego and Senwabarwana Campuses) and the Central Office of Capricorn Further Education and Training (FET) College in Limpopo Province in South Africa.

The questionnaires were hand delivered and collected by the researcher. The staff members filled in the questionnaire and the researcher collected the questionnaire immediately. Other questionnaires were collected the following day or week after. 91% of participants responded, while 9% of participant did not respond to the questions.

The questionnaire were based on 5-point Likert scales with 1 for strongly agree and 5 for strongly disagree in order to determine the ratings. The results of the questionnaire were used in developing the proposed technical model.

Correlations

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Information Security Strategy	1	.731**	.484**	.564**	.141	.186	.536**	.741**	.955**	.767**	.881**	.861**	.635**	.861**	.808**
Policies	.731**	1	.672**	.834**	.263*	.330*	.743**	.871**	.771**	.555**	.678**	.627**	.877**	.627**	.586**
Change Password	.484**	.672**	1	.746**	.616**	.670**	.771**	.550**	.432**	.299*	.375**	.362**	.781**	.362**	.337**
Password Safe	.564**	.834**	.746**	1	.427**	.504**	.611**	.730**	.531**	.320*	.443**	.409**	.725**	.409**	.369**
Use of someone username	.141	.263*	.616**	.427**	1	.889**	.405**	.114	.071	-.017	.036	.035	.336**	.035	.017
Allowed someone else to use your username	.186	.330*	.670**	.504**	.889**	1	.498**	.192	.123	.014	.080	.073	.413**	.073	.051
Education	.536**	.743**	.771**	.611**	.405**	.498**	1	.677**	.567**	.400**	.496**	.455**	.848**	.455**	.423**
Educational programs	.741**	.871**	.550**	.730**	.114	.192	.677**	1	.771**	.589**	.692**	.649**	.765**	.649**	.616**
Competent staff members	.955**	.771**	.432**	.531**	.071	.123	.567**	.771**	1	.747**	.890**	.831**	.672**	.831**	.783**
Infrastructure	.767**	.555**	.299*	.320*	-.017	.014	.400**	.589**	.747**	1	.838**	.896**	.477**	.896**	.952**
Tools	.881**	.678**	.375**	.443**	.036	.080	.496**	.692**	.890**	.838**	1	.932**	.589**	.932**	.879**
System Encryption	.861**	.627**	.362**	.409**	.035	.073	.455**	.649**	.831**	.896**	.932**	1	.542**	1.000**	.941**
Strong authentication technique	.635**	.877**	.781**	.725**	.336**	.413**	.848**	.765**	.672**	.477**	.589**	.542**	1	.542**	.505**
Information Security Model	.861**	.627**	.362**	.409**	.035	.073	.455**	.649**	.831**	.896**	.932**	1.000**	.542**	1	.941**
Positive aspects of information security	.808**	.586**	.337**	.369**	.017	.051	.423**	.616**	.783**	.952**	.879**	.941**	.505**	.941**	1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 1. Correlation of Data

The levels above of correlation of data indicated by 0.5 or above shows strong significant correlation, while less 0.5 level weak significant. The data indicates the correlation between all descriptions of the questions. 59 questionnaires were answered. The characters below have been assigned the descriptions as there is was no sufficient space to cater table 1 correlation table.

The Table 2 Assign table indicate the descriptions of characters for the variables shown in table 1 correlation of data.

From the data in table 1, indicate strong relationship between information security strategy and policies. Having proper information security strategy, these cause a good basis of developing policies that are well informed. Even though policies are more high level documents as compared to information security strategy there is clear tight between them. As the results this can serve as control mechanism and guidance in taking more informed information security decisions.

Character	Description	Character	Description
A	Information security strategy	**I**	Competent staff members
B	Policies	**J**	Infrastructure
C	Change password	**K**	Tools
D	Password safe	**L**	System encryption
E	Use of someone username	**M**	Strong authentication technique
F	Allowed someone else to use your username	**N**	Information security model
G	Education	**O**	Positive aspects of information security
H	Educational programs		

Table 2. Assign table

The changing of passwords and education shows a strong relationship. This is not very surprising as the change of passwords requires a good awareness and training. The skills that are obtained from training can then enable the staff members not to use other staff member's password. As such there security risks are much reduced in this regard.

Without any doubts the relationship between the infrastructure and encryption seems more outstanding. This indicated by Table 1 Correlation of Data. However, with FET views of security infrastructure as a need to have in order to implement good secure environment that will ensure capability of encryption to work well. In this regard, FETs have been reluctant to spend money on infrastructure security because it is extremely difficult to prove that security serves the bottom line. This may eventually be negative to the FETs and place their existence at risk.

Education around the staff members has always been crucial in developing and empowering staff members. These have been seen on the strong relationship between education and competent staff members stipulated by table 1 correlation of data. If the staff members are equipped with education and awareness in relation with information security, it will then be clearer that more staff members will have competence skills. Having competencies can lead to ease to implement information security.

The correlation between awareness, education and positive aspects of information security can then be questioned. This is does not show tight relationship at shown in table 1 correlation of data. It is expected that out of awareness and education positive aspects of information security should be clearly outlined.

The proposed technical model has been developed from the results of the questionnaire and hypothesis stated in above figure 4. The proposed technical model comprises of four major components including the user interface, encryption, access control and infrastructure.

The proposed technical model starts with the user interface were the authentication occurs. The user will have to login using usernames and passwords. If usernames or passwords are incorrect, the system will display the error message which will be displayed as "*invalid password or username*". If the username or password is correct, the password will be assigned to the user under the read, write and execute access rights.

The user access will be validated before the authentication happens. Then username or password will be authenticated to the system. If authenticity is not correct, the system will request another username or password, otherwise the system will give the user access to system data. Depending on the valid credentials the users will be authorized to the system with the signed certification. The system data will create audit logs on which user's access of data is depended on the infrastructure.. The firewall should be able to filter viruses that might temper into the apache server on the infrastructure.

The domain name server (DNS) was used to allocate the internet protocol (IP) address for all devices that connect to the network to utilize network resources. The infrastructure should have application server that will be connected to microsoft SQL database and microsoft server 2005 for storage of databases. The switch may interact with the router in order to route the data into the outside world to the internet. The proposed technical security model has some benefits that may impact positively on the the system.

The benefits of this system model are:

• To provide high level security on the system

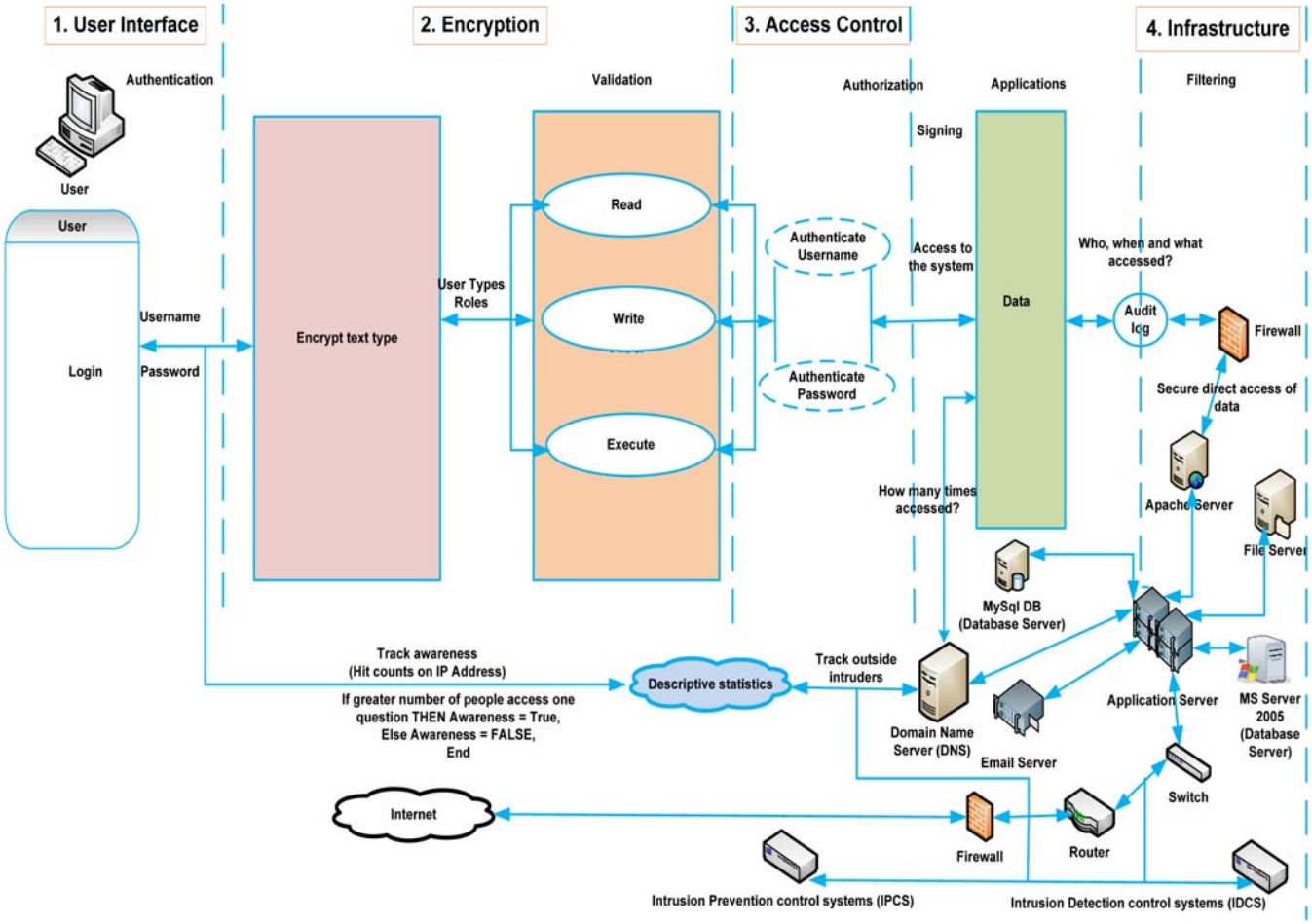

Figure 5. Proposed technical model

Description	Covers currently in information security policy	Coverage needed
Violation and breaches	42%	75%
Virus	45%	70%
Encryption	47%	60%
User access management	49%	76%
Physical security	25%	65%
Responsibilities	20%	70%
Enforcement	10%	60%

Table 3. Information Security Policy (ISP) in Capricorn FET College

• To provide cheaper and more easier to implement technical security solution in any higher education institution

• To create more flexible functionality and to create awareness on the information security.

The below Figure 6 shows the current coverage of features of information security policy at the FET with the coverage as needed.

4.2 Experiment 1: Observation of Information Security Policy on Data Set 2

The experiment 1 shows the table 4 with coverage of features of information security policy gathered from the internet.

4.3 Experiment 2: Observation of Information Security Awareness on Data set 1

The experiment 2 indicates an awareness of information security at Further Education and Training (FET) College.. The high

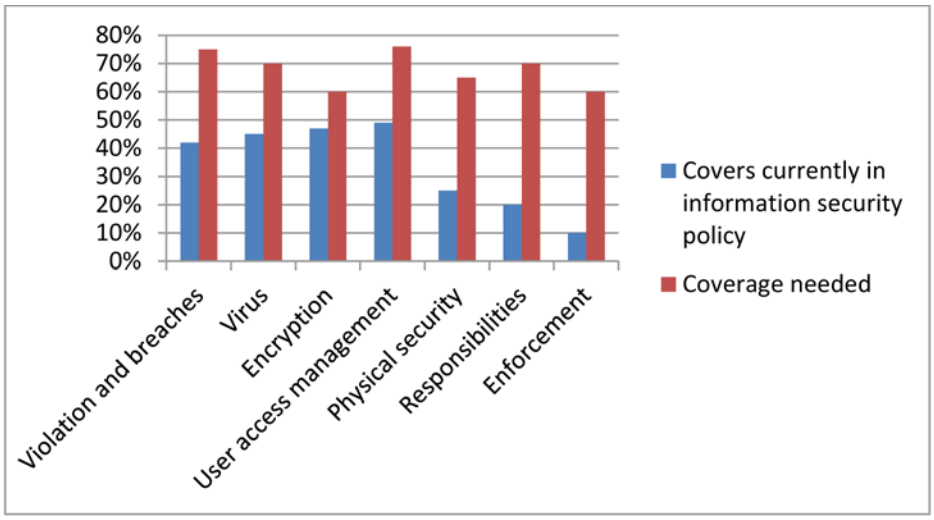

Figure 6. Information Security Policy in Capricorn FET College

	Coverage in ISPs	Coverage in ISPs [%]
Security issue		
Violations and breaches	51	84%
User access management	44	72%
Contingency planning	31	51%
Physical security	29	48%
Disclosure of information	22	36%
Viruses, worms, etc.	21	34%
Encryption	14	15%
Mobile computing	11	18%
Software development	10	16%
Personal usage of information	8	13%
Internet access	5	8%
Extra issues		
Responsibilities	41	67%
Enforcement	33	54%
Awareness and training	23	38%
Compliance with legislations	21	34%
Information classification	13	21%
BS (1)7799 reference	12	20%

Table 4. Information Security Policy (ISP), [2]

Security issues	**Security Issue % Currently in Place at Capricorn FET College**	**% Thought Was Needed**
Tough Passwords	50%	70%
Require Password modification	55%	72%
Firewalls on External link	40%	75%
Internal Firewalls	52%	74%
Encrypted Files Used	40%	71%

Table 5. Capricorn FET Security Measures

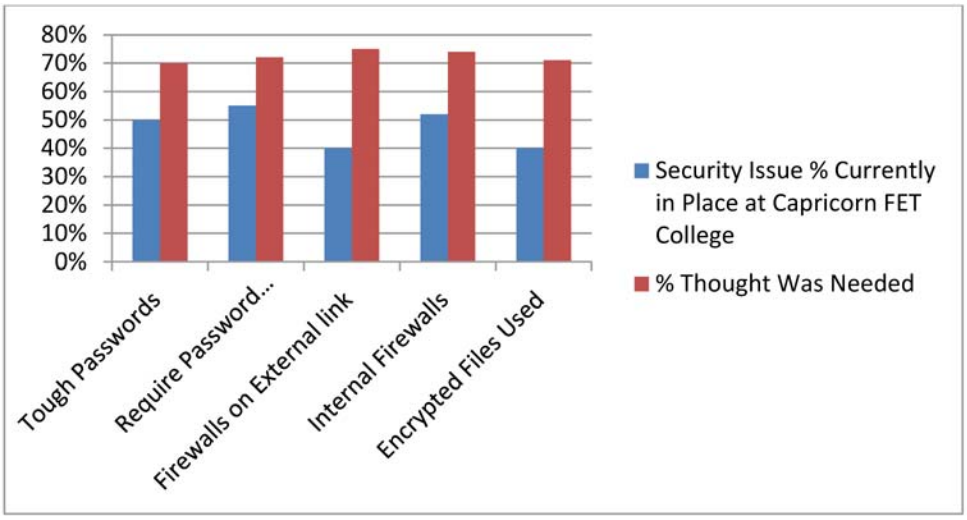

Figure 7. Capricorn FET Security Measures

Security Measures	Security Issue % Currently in Place at Arkansas state University	% Thought Was Needed
Tough Passwords	50%	93%
Require Password modification	64%	89%
many Level verification	65%	84%
standard Risk Analysis Performed	34%	86%
Firewalls on External link	94%	93%
Internal Firewalls	64%	80%
Encrypted Files Used	31%	61%

Table 6. Security Measures

number of employees seems not to be aware of the information security. These may be tracked through Domain Name Server (DNS) which assigns every machine an Internet Protocol (IP) address. The log file on the DNS may be able to track who logged in and what was changed. If many computers using different IP addresses accesses the same question it may mean that no awareness was provided. If one IP address gets a lot of hit counts from the DNS, it might mean that many employees may be aware of information security. The information gathered from the DNS log file is reflected on table 5.

4.4 Experiment 2: Observation of Security Awareness on Data Set 2

The information as shown in table 6 is gathered via the internet. According to the research done by [4] indicated in Table 1 below: The Figure 8 is a graphical representation of above table 6.

5. Comparing the Proposed Technical Security Model With Other Models

The below table 7 indicate the comparison of various technical security model with the proposed technical security model.

From table 7, it is clear that the proposed technical model has more features to prevent unauthorised accessed as compared to other models. This implies that having adopted the proposed technical security model may reduce data loss and unauthorised access.

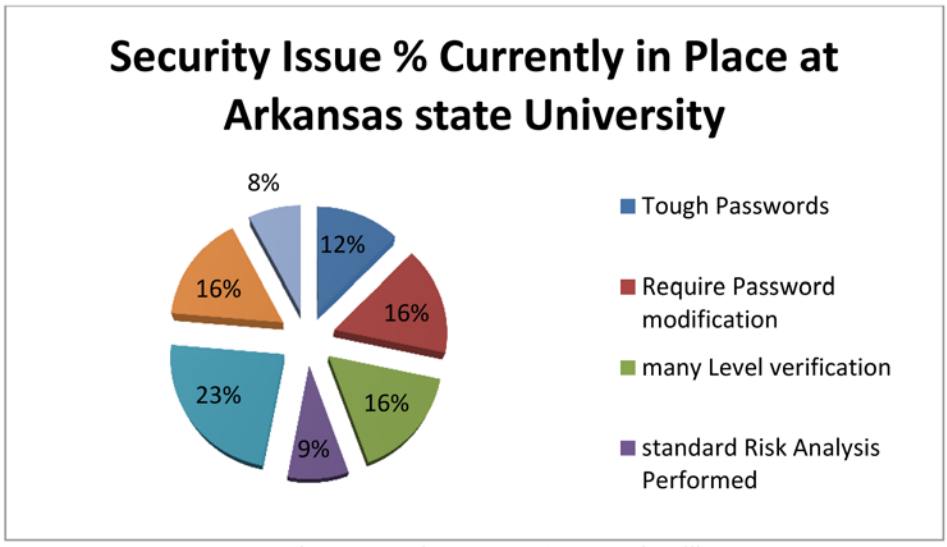

Figure 8. Security Measures [4]

	FEATURES	1ST SECURITY MODEL (NASSCOM, 2012)	2ND MODEL SECURITY (Stoneburner, 2001)	PROPOSED TECHNICAL SECURITY MODEL
1.	Authentication	✓	✓	✓
2.	Encryption	✓	✓	✓
3.	Validation	X	X	✓
4.	Authorization	✓	✓	✓
5.	Signing	✓	X	✓
6.	Log files	✓	✓	✓
7.	Application	✓	X	✓
8.	DNS server	✓	✓	✓
9.	Track awareness	X	X	✓
10.	IPCS	X	X	✓
11.	IDCS	X	✓	✓

Table 7. Comparison of security model

and Training (FET). If more awareness and education may be emphasized in relation to information security, it may make

6. Conclusion

The information security threats and the ever-growing body of regulation have made information security a significant function within HEI. The information security may fail because of various reasons including lack of information security policy, access control and awareness . The majority of respondents seem not to be aware of information security policies in Further Education information security to succeed. This study is based on modified ISO/IEC 27002 framework by [3]. The proposed technical model may be used at other HEIs to address security breaches and awareness among employees as it has more features as compared to other security model.

7. Acknowledgement

First we would like to thank almighty God for his strength, comfort, and knowledge that have helped us through our whole life. Without God none of this would have been possible. We would like to thank our families. I would also acknowledge Francinah Sewela Mohlabeng and Kgwerano Covenant Kgatla for motivation and encouragement in this study. Thank you for all your encouragement during this long drawn out process.

References

[1] Baskerville, R., Siponen, M. (2002). An information security meta-policy for emergent organisations. *Information Management and Computer Security*, 15 (5/6) 337–346

[2] Doherty N. F., Anastasakis, L., Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29, 449–457. Loughborough University, The Business School, Ashby Rd, Loughborough, Leicestershire LE11 3TU, United Kingdo FARLEX. 2011. *Information security* [Online] Available at: http://www.thefreedictionary.com/information+security

[3] Innova. (2011). *Information Security Management Framework Implementation* [Online] Available at: www.innova-sa.eu (12/04/2012)

[4] Jones, R. Stallings, T. J. (2010). *Computer and Information Technology.* Information Technology Services Dept. Arkansas State University CCSC: Mid-South Conference.

[5] Marks, A. (2007). *Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research.* PhD thesis, University of Salford.

[6] Open Security Foundation. (2012). *Data Loss Statistics* [Online] Available at: http://datalossdb.org/statistics (07 July 2012)

[7] Piazza, P. (2006). Security goes to school, *Security Management*, 50 (12) 46–51. Arlington.

[8] Schneier, B. (2000). Secrets and Lies: Digital security in a networked world. *John Wiley & Sons Inc*.

[9] The New York Times Company. (2012). Information Security [Online] Available from: http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity.htm (21/03/2012).

[10] Von Solms, R., Von Solms, S. H. (2004). From policies to culture. *Computer & Security*, 23 (4) 275-279.

[11] Whitman, M. E., Mattord, H. J. (2004). Improving Information Security through Policy Implementation. *In:* Proceedings of the 7th Annual Conference of the Southern Association for Information Systems.

[12] Whitman ME, Mattord HJ. (2005). *Principles of Information Security*. 2nd ed. Thomson.

[13] Wilson. (2003). Building an information Technology Security Awareness and Training Program. NIST, Special publication, p. 800 – 50.

[14] Winkler, I, Hayden, L. (2005). *Social engineering through human intelligence*. *The Information Systems Security Association Journal*. p. 6–8.

[15] Yasinsac, A. (2002). Information Security Curricula in Computer Science Departments: the Theory and Practice, Department Science Florida State University, *Journal of Computer security*.

[16] Nasscom. (2012). Security Services and Technical Model [Online] Available at: www.dsci.in/framework/358 (08/07/2012)

[17] Stoneburner, G. (2001). *Underlying Technical Models for Information Technology Security.* National Institute of Standards and Technology. NIST Special Publication 800-33 *Available at* http://www.cio.gov/documents_details.cfm/uid/1F432D72-2170-9AD7-F25F5B2F61667D6A/structure/Information%20Technology/category/IT%20Security-Privacy (0/07/2012).