VOL. 3, NO.11 Nov, 2012 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences
©2009-2012 CIS Journal. All rights reserved.

http://www.cisjournal.org

Towards Implementation of the Information Security Strategies in South Africa

[1] Moyahabo Rossett Mohlabeng, [2] Sello Nicholas Mokwena, [3] Isaac O. Osunmakinde
[1, 2] Department of Computer Science, Tshwane University of Technology, South Africa
[3] Semantic Computing Groups, School of Computing, College of Science, Engineering and Technology
University of South Africa, P.O. Box 392, UNISA, 0003, Pretoria, South Africa
[1] mohlabengmr@tut.ac.za, [2] mokwenasn@tut.ac.za, [3] 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 in higher education institutions (HEIs). Research was undertaken to investigate the implementation of information security strategies in HEI in South Africa. A survey questionnaire was administered to the personnel of Further Education and Training FET) in the Limpopo Province of South Africa. The study found that HEIs lacked information security strategies and information security awareness education programmes. In the paper, we discuss in detail comprehensive survey of different security attacks on information systems and categorize them as general organizational and HEI-related attacks. We investigate and explain the status of information security implementation strategies used in Capricorn FET College, as well as international practice, and compare the two in terms of security policy coverage and security awareness coverage. A new technical information security framework is proposed and developed, based on ISO 27002, which helps to address HEI information security needs in South Africa. We conducted a deployment survey in Capricorn FET College and Science direct databases on the sub-subsystems of access control, infrastructure and policy awareness ratings of the proposed strategy, based on acceptance of security measures. This paper presents deployment analysis on how the proposed strategy could be used or implemented through real-life scenarios categorised as user-allowed access and user-denied access. We surveyed the information security implementation strategies currently in use and compared them on the basis of track awareness, intrusion prevention control systems and intrusion detection control systems. Further research issues and challenges that still have to be addressed, as well as the design of information security implementation strategies, are presented. The results of this study can be used as a reference guide to understand security management, as well as efficient and reliable implementation strategies of information systems and security strategies for organizations of all sizes.

Keywords: *Information security, strategy,HEI,data loss,policy, awareness, Infrastructure.*

1. INTRODUCTION

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function in organizations. Information security means protecting or securing information from unauthorized access, use, disclosure, interference, alteration, or damage [1].The implementation of information security may require more resources, such as controls and maintenance, to ensure effectiveness. McIlwraith [2] highlighted that safety measures in information security strategies have often been ineffective in most higher education institutions (HEIs). Thus, insufficient safety measures in institutions have introduced vulnerabilities into their networks, such as data losses and theft of data.

HEIs have experienced major data losses in which nearly 200 000 electronic data were illegally accessed, including student details and staff-related data, leading to the loss of students' financial and medical records [3]. In this environment, knowledge of information technology (IT) security threats and vulnerabilities facing HEIs is crucial to avoid potential loss of an institution's information [4].These attacks also caused illegal deletion of electronic data, which led to low academic performance among HEI students and a reduction in the morale of library staff who have to provide electronic services to the students and staff [5].

In these circumstances, security measures facing HEIs make it necessary to guard against potential loss of an institution's information [6].HEIs have an ethical responsibility to protect themselves against loss of information [7]. It is therefore necessary to investigate the implementation of information security strategies in HEIs.

The current implementation of information security strategies includes intrusion detection control systems (IDCS), firewalls, etc. According to [8] the current use of IDCS plays an important part in the institution's IT security strategy to prevent unauthorized access, while the use of a firewall filters illegal access of data that enter or leave the institution. The advantage of information security strategies is that they minimize harm and data losses suffered during unauthorized access [9]. Despite these benefits, there are challenges related to the current information security strategies in that they lack resources needed to implement security effectively, especially on the technical security level [10].Information security literature has described prevention and detection strategies linked to the incidence of information security [11].

HEIs still lack information communication and technology (ICT) infrastructure to validate, encrypt, implement and be proactive in preventing unauthorized access. Therefore, HEIs should invest in technology that encrypts all educational data, making it difficult for unauthorized users to hack into the system. This paper aims at developing a technical security model for HEIs to improve security using information security concepts. The main contributions of this paper are the following:

- Knowledge generation as a reference guide to understand information security implementation strategies in general and an information security model for South Afrikaners in particular.
- Development of a newly proposed proactive information security framework for South African HEIs based on a modified ISO/IEC 27002 by [12].
- A systematic survey and representation of research challenges and open problems in the design of an information security implementation strategy.

The rest of the study is organized as follows: Section 2 outlines the information security paradigm, Section 3presents safety fears and information security implementation, Section 4 details the proposed information security implementation strategies, Section 5 presents deployment analysis, Section 6 outlines open research issues in an information security implementation structure and section 7 concludes the paper.

2. INFORMATION SECURITY PARADIGM

2.1 Nature Of Safety In Information Security Strategy

Before we proceed to the findings, it is important to mention that the legal, IT and higher education disciplines have different perceptions of safety. However, these definitions of the term safety broadly underpin its dictionary meaning (see Figure 1). From the point of view of information security frameworks, the safety definition appears to be closer to those used in the IT and higher education spheres.

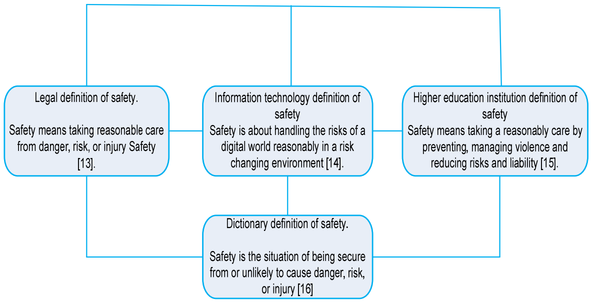

Legal definition of safety.
Safety means taking reasonable care from danger, risk, or injury Safety [13].
Information technology definition of safety
Safety is about handling the risks of a digital world reasonably in a risk changing environment [14].
Higher education institution definition of safety
Safety means taking a reasonably care by preventing, managing violence and reducing risks and liability [15].
Dictionary definition of safety.
Safety is the situation of being secure from or unlikely to cause danger, risk, or injury [16]

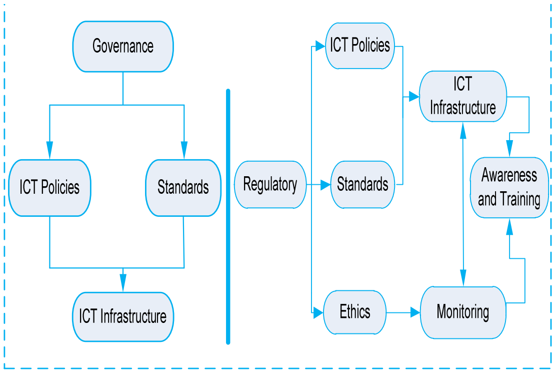
Fig 1: Definition of safety.

The use of various definitions of safety in the information security strategy contributes to a good basis of implementation of security frameworks. The definitions of safety will lead to better understanding of the information security paradigm.

2.2 Information Security Implementation Frameworks

Information security frameworks were introduced into the organization to address the implementation of security. The frameworks include holistic and partial information security frameworks [17].

Figure 2a shows a partial information security framework, while figure 2b illustrates a holistic information security framework.



(a)Partial framework (b) The holistic security adopted from [18].framework adopted from [19].

Fig 2: Partial and holistic security frameworks.

The partial information security framework appears adequate for establishing information security across institutions, as shown in figure 2a. The institution’s increased use of information security brought about extensive side effects and new issues for which there was no clarification in the integration of the partial framework [17]. Hence, figure 2a shows the elements of a partial information security framework, which includes governance, ICT policies, standards and ICT infrastructure. According to figure 2a, ICT policies and standards are influenced by the governance in the institutions, while an effective ICT infrastructure relies on good and implementable ICT policies and standards.

Although a partial security framework has its own strengths and weaknesses, its impact is rather on information security aimed at focusing on critical elements of security and consequently the promotion of partial security in institutions in the most understandable manner [20]. However, some challenges have been encountered when assessing and evaluating the risks to the entire institution’s information security [21]. Because of some weaknesses that are found in a partial framework, a holistic framework may be preferred.

Figure 2b shows a holistic framework entailing complete information security framework, which addresses all angles of information security implementation. A holistic information security framework consists of major components such as regulatory measures, ICT policies, standards, ethics, monitoring, ICT infrastructure and awareness and training. ICT policies and standards have more influence on the type of infrastructure that must be put in place. In order for ICT infrastructure tube utilized fully, monitoring has to be done in conjunction with awareness and training.

Similar to a partial security framework, a holistic information security framework has its own benefits and challenges. Some of the benefits come in the form of structural and architectural implementation. Gartner [22] has defined enterprise architecture frameworks with three levels of constructs, such as conceptual, logical and physical levels based on business, information and technical aspects, which offer more benefits in securing the entire institution's environment. Thus, the major challenge of the holistic framework is more resources to implement the framework, especially if the entire information security framework is implemented at once [23].

The differences between the partial information security framework and holistic information security framework is that the partial framework is easier to implement, as it concentrates on the specific portion of security on a high level, while the holistic information security framework focuses on all security perspectives, including the business level, information level and technical level[23]. We believe that a holistic security framework is the better information security framework, as it covers all angles of security. The information security framework may function better in any institution of any size.

2.3 Information security Strategy Applications

This section indicatesthe environments where information security has been applied and whether the outcome was successful or not. The authentication system on internet banking was improved in the second largest bank in Austria. This was undertaken to address threats through cryptography, which included usability and cost-effectiveness. The security framework was applied successfully and lessons learnt through management and employees were properly documented [19].

[24] Analyzed and implemented a security framework on e World Live Space security to improve the quality of the security. This was done mainly to examine the infrastructure that will cater for future environments. The security framework was a challenge in terms of its application, as it was too complex; fortunately it became slightly more acceptable. Indeed, information security is a vital aspect of the internal network of an institution to protect unauthorized access through the use of a firewall [25].According to[26], colleges and universities employ few security controls to address access and disruption of information. More needs to be done to improved security, even though the success factors might not be clearly visible.

3. SAFETY FEARS AND INFORMATION SECURITY IMPLEMENTATION STRATEGIES

3.1 General Organization-Related Attacks

Security attacks come in different forms for various reasons, such as malicious damage, theft of information, deletion of data action 11 September 2001 an attack on America shocked the entire world and left many people with unanswered questions, especially on the safety of information. These events cautioned security specialists to be pro-active rather than reactive in preventing threats. Critical data were lost and some were to recover [27]. Figure 3a shows summary of data breaches in general organizations over six years, while figure 3b illustrates the classification of data breaches.

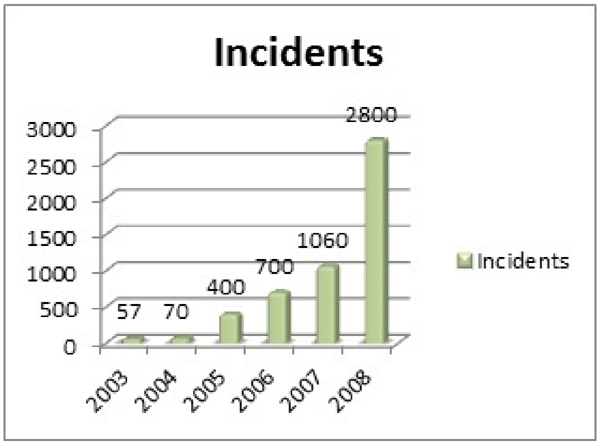


Figure 3(a).Summary of data breaches over six years [28].

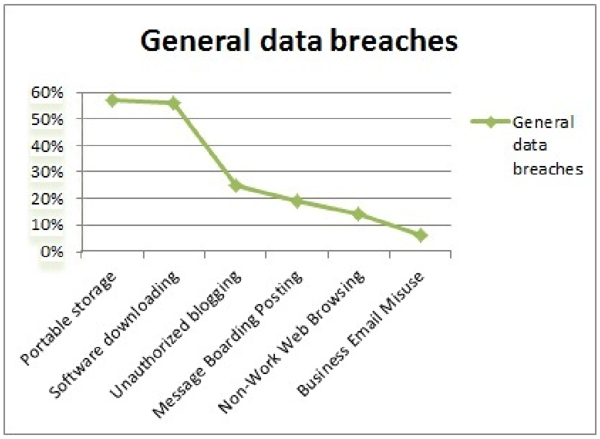


Fig 3(b): Classification of data breaches [23].

Figure 3a shows an increase in data breaches from 57 security incidents to 2800 security incidents between 2003 and 2008, while figure 3b shows an increase in unauthorized blogging by 25%, message boarding posting by 19% and portable storage use by 57% etc. These data breaches over years occurred in various ways.

Data breaches have always come in the form of internal and external attacks. The use of modern technologies makes these attacks impossible to control. Many organizations struggle with security controls that will assists in strengthening the network. According to [29], data breaches cause disruptions, which affect various organizations. Security countermeasures will assist in preventing or minimizing any data breaches that may be encountered in any organization [30].

3.2 Information Security Strategy In Higher Education Institution-Related Attacks

HEIs have noted that since 2003 approximately 8 million individuals have been affected by employee data breaches. The record of HEI data breaches that occurred from 2003 to 2012 is reflected in figure 4a [31]. While interest in securing employees' records is commonly high in both developed and developing countries, security remains crucial to protect employees' data.

Figure 4a depicts the rise in data losses from 21 security incidents to a high of 1046 security incidents between 2003 and 2012. The number of data losses started to decline in 2009 from 1046 to 718 security incidents. These incidents have had a negative impact on the HEI environment. The security incidents are categorized in figure 4b. Figure 4b shows that data were lost in different ways, such as data losses through hackers attempting to gain access unlawfully (62%), data loss through theft (64%), loss of data attributable to viruses (71%), the part web sites play in data losses (57%) and of disposal of documents (46%).

Figure 4a outlines a summary of education data breaches and the estimated education data breaches over 10 years are shown in figure 4b [31].

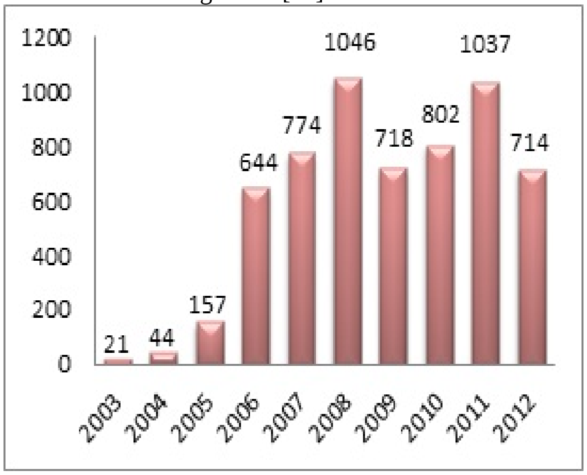


Fig 4(a): Summary of educationdata breaches [31].

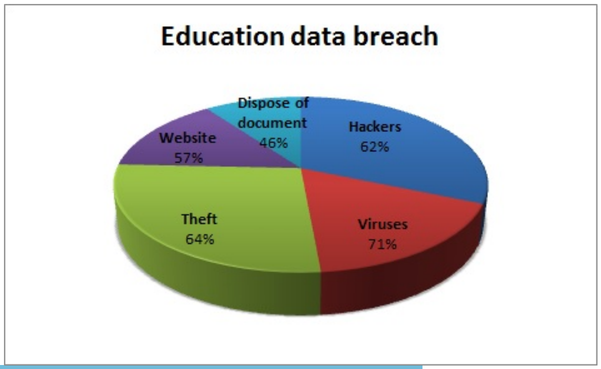


Fig 4(b): Estimated education databreaches over 10 years [31].

According to [4], HEIs have faced different information security threats emanating internally or externally. These information security threats consist of viruses, technical software errors, human error or failure. HEIs have experienced major data breaches, which led to financial losses and examination marks being lost [5].

In a survey conducted on 30 journals sampled from the Science direct database [32], 75% of articles indicated that the existing information security strategy requires improvement of safety, while 20% disagreed and 5% were undecided. Figure 5 outlines the findings of the survey.

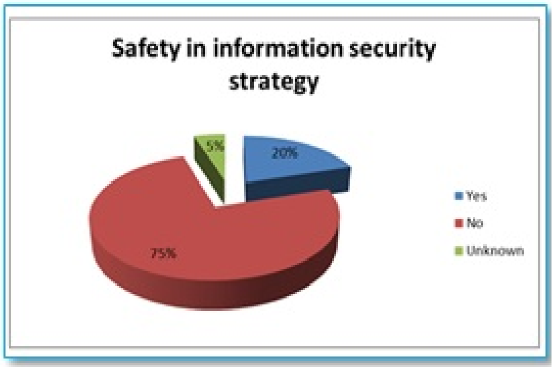


Fig 5: Does the existing information security strategy require improvement?

According to [33], the use of safety is more effective within the information security strategy because it tightens the level of security in the HEI environment. HEIs have outlined the importance of successfully developing safety features in information security strategy and have been able to apply these in their institutions [34].

3.3 Underpinning Framework

This section examines current internationally accepted information systems (IS) and an IT-related approach in order to establish the theoretical foundations for this study. This study is based on a modified ISO/IEC 27002 information security framework [12].The theoretical perspectives are used in an investigation of the implementation of information security strategies in FET colleges in South Africa. This framework consists of the main components: security policy, training and awareness and reporting has shown in figure 6[12].

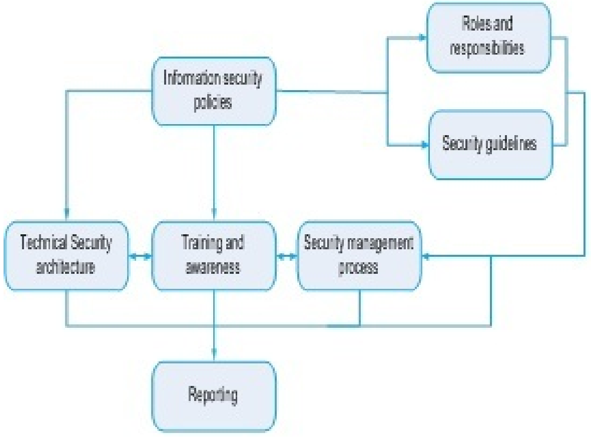

Roles and responsibilities
Information security policies
Security guidelines
Technical Security architecture
Training and awareness
Security management process
Reporting

Fig 6: Information security framework.

Figure 6 shows the significance of information security policies in roles and responsibilities and security guidelines. They contribute to the development of technical architecture, training and awareness and security management. The modified ISO/IEC 27002 information security framework [12] comprises the following components:

- **Roles and Responsibilities:**The roles and responsibilities of information security throughout the organization may need to be defined clearly and well understood. These serve as guidance for those who are responsible for directing and managing information security resources to oversee an information security function.

- **Security Guidelines and Standards:**Security guidelines and standards assist in planning for information security management in an organization. The guidelines should always be effective security practices and internationally accepted standards related to information security.

- **Security Management Processes:** Security management processes cover the creation, management and oversight of policies to ensure the prevention, detection and correction of security violations. These entail risk analysis and risk management, which may also include the establishment of accountability, management controls, physical security and penalties for the abuse and mishandling of assets in cooperation with physical and electronic formats.

- **Technical Security Architecture:** Technical security architecture focuses on the mapping between the control architecture and the safeguarding processes. These mainly describe standards for protection settings that may be implemented by technical methods and identify what is usually called technical security policy.

- **Training and Awareness:**Information security awareness assists organizations in changing their employees into the main effective security control by:

a) Increasing awareness of the need for information security on all staff levels.
b) Increasing awareness of the benefits of using the security architecture.

The major advantage of using the modified ISO/IEC 27002 information security framework is that it allows security to be controlled easily by ensuring compliance. It is also easy to implementing any type of institution without requiring extensive resources [35].

3.4 Rating Network Security Based On Information security Strategy

The mathematical model dealing with the level of information security strategy is based on Page Rank modeling in [36] as a network security rating (NSR). Our NSR model is shown in equation (1).

$$NSR(A) = (1 - d) + d\,(\frac{NSR(t1)}{c(t1)}) + \cdots + (\frac{NSR(tn)}{c(tn)})(1)$$

Wheret1, . . . , tn are networks linking to network A, C is the number of outgoing links from a network (out-degree) and d is a damping factor, usually set to 0.85.Since Page Rank assigns a high score to a node if it is pointed by highly ranked nodes, it is highly applicable in advancing information security strategy based on networks' security level.

4. PROPOSED INFORMATION SECURITY IMPLEMENTATION STRATEGY

4.1 Research Design

The research design consists of research questions, which lead to the hypotheses (see H1, H2 and H3). The questionnaire was designed based on the hypotheses that were formulated. The result obtained from the analysis of the responses from the questionnaire has been used to develop the proposed technical security framework. This led to the analysis of the proposed technical security framework that will be based on the FET data and publicly available data.

Figure 7 shows the research questions and how they are related or interact with one another. For each question, hypotheses were formulated. These assisted in the development of the technical security framework. The technical security framework was analysed using local data from FET and data that are publicly available on the internet, which was accessed via Sciencedirect database.

Figure 7 shows the research design of the study.

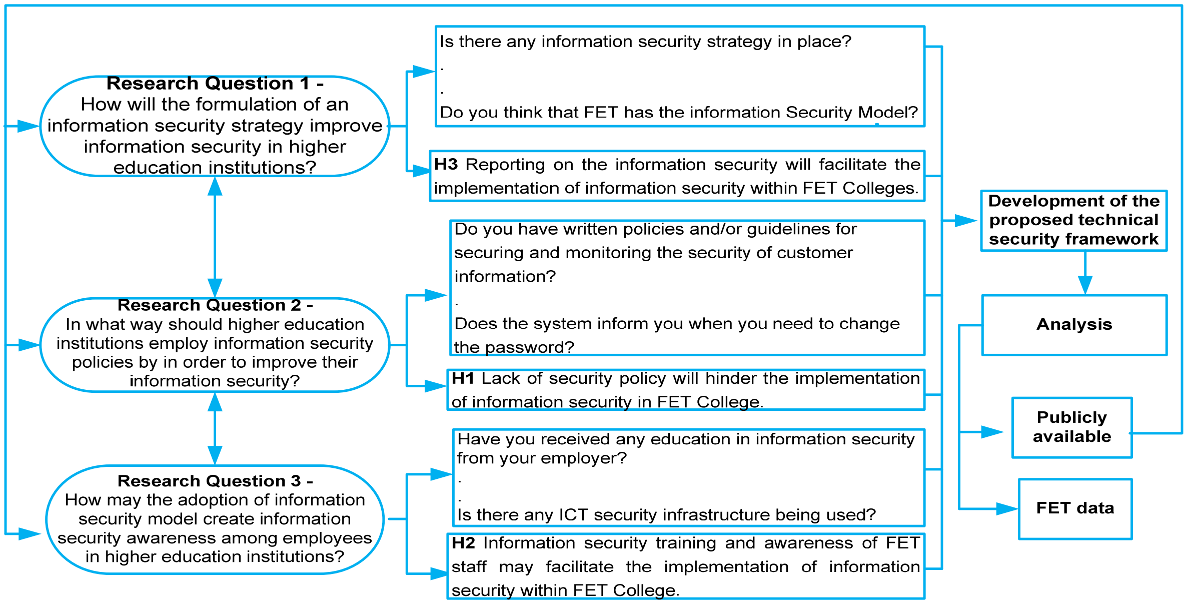

Research Question 1 - How will the formulation of an information security strategy improve information security in higher education institutions?
Research Question 2 - In what way should higher education institutions employ information security policies by in order to improve their information security?
Research Question 3 - How may the adoption of information security model create information security awareness among employees in higher education institutions?
Is there any information security strategy in place?
.
.
Do you think that FET has the information Security Model?
H3 Reporting on the information security will facilitate the implementation of information security within FET Colleges.
Do you have written policies and/or guidelines for securing and monitoring the security of customer information?
.
Does the system inform you when you need to change the password?
H1 Lack of security policy will hinder the implementation of information security in FET College.
Have you received any education in information security from your employer?
.
.
Is there any ICT security infrastructure being used?
H2 Information security training and awareness of FET staff may facilitate the implementation of information security within FET College.
Development of the proposed technical security framework
Analysis
Publicly available
FET data

Fig 7: Research design.

The next subsections outline the proposed information security implementation strategy.

4.2 User Interface As A Security Measure

The system uses user interface as a security measure to access its data by using usernames and passwords for authentication purposes. This requires valid credentials before the system is accessed. If credentials are correct, the system will allow access, otherwise it will display a message: “Invalid username or password”. In the front of the user interface, there is security radar that determines the level of security at the time of access. This security radar indicates “green “to show that the system is secure enough to be accessed, while “yellow “indicates that the level of security is medium, implying that there is little security control, and “red “indicates that the system is not safe at all owing to viruses, threats or breaches on the system.

Generally the number of people who access the system will be categorized by the internet protocol (IP) addresses, which uniquely identify computers and/or organizations where individuals work. If large organizations such as Microsoft, Cisco, etc. access a system on a regular basis, this might mean that the system is secure enough to work. If large organizations access a system only once, there could be suspicion that the system might not be secure enough. More information on this is presented in subsection 4.9.

4.3 Advanced Encryption As A Security Measure

Advanced encryption is used as a security measure, which includes advanced encryption standard (AES). AES is used in encrypting all types of data on the system, preventing unauthorized access. This applies to encryption of usernames and passwords and also data that are saved on the system. With the use of AES, the data are well-encrypted and well-defined to create better optimized performance on the network.AES is difficult to break because it uses up to 128 characters. The worldwide Microsoft Company uses AES to encrypt some of its systems. Hence, the proposed system has adopted AES.

4.4 Access Control As A Security Measure

Access control is used as a security measure to control any access to the system. The credentials are validated to ensure that only authorized individuals access the system. If valid credentials are provided, allowance or permission to use the system will be provided. In cases where credentials may be incorrect, the error message will respond appropriately. Every action that may occur will be logged in the audit log for reference in future. The access control includes read, write and modify.

Thirty-two journals were sampled from Science direct databases for a survey of access control; 85% of users indicated that they were experiencing challenges with access in organizations, while 11% had no problems and only 4% were undecided. Such a huge number implies that there is a need for a strong access control. Figure 8 shows the survey result on the enforcement of access.

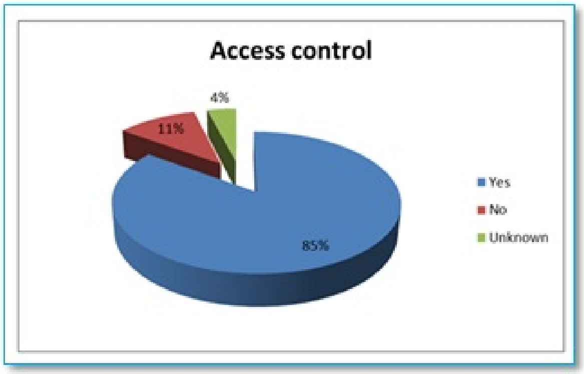


Fig 8: Is there a challenge in access enforcement in a System?

According to [37], access control is a main security requirement to protect institutions' information and can easily be implemented in any organization. Appropriate access control provides effective control to handle complex security systems in a flexible and dynamic way. Access control elements such as intrusion detection systems have been implemented and evaluated and have resulted in a positive method for preventing unauthorized access [38].

4.5 ICT Infrastructure As A Security Measure

ICT infrastructure has been used as a security measure to ensure that information is secured on the network. ICT infrastructure includes intrusion prevention control systems (IPCS), IDCS and firewalls. An IPCS proactively detects any unusual or unauthorized access that occurs on the network to tighten security, while an IDCS reactively detects unwanted or unauthorized access. The firewall blocks unauthorized access and allows only authorized individuals to the system. This process filters the traffic in and out of the system.

Twenty-seven journals were sampled from the Science direct database for a survey on ICT infrastructure; 80% of users indicated that there are proactive security measures against attacks in organizations, while 15% disagreed and only 5% were undecided. Figure 9 shows that employing proactive security measures protect the environment against all kinds of attacks.

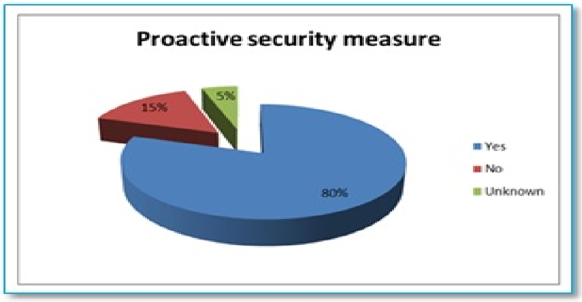


Fig 9: Does a proactive security measure protect environment against internal or external attacks?

ICT security infrastructures better able to provide protection to existing and newly developed ICT systems that are implemented globally. This ensures good security measures to the technical environment of institutions [39]. The critical ICT infrastructure contributes to the level of security among the communication media and also serves as good control for systems [40].

4.6 Policy As A Security Measure

Security policy provides management with direction and a way of maintaining information security in line with business requirements and applicable laws and regulations. Management develops a security policy in line with business objectives in order to serve as a security control in the institution. The information security policy document should be approved by management and communicated to all employees and appropriate external parties. ICT policy includes information security policy, interception and surveillance policy, data backup policy and ICT service continuity policy.

The information security policy document states management's commitment and sets out the organization's approach to overseeing information security. This information security policy should be communicated throughout the organization to users in a form that is applicable, clear, available at all times and comprehensible to the intended reader. Information security policy helps to enforce security in an organization to ensure that unauthorized access is prevented at all times.

4.7 Training And Awareness As A Security Measure

Training and awareness used as security measure promote pro activeness in preventing unnecessary human error. This will also inform and educate users on the importance of information security.

Thirty-eight journals were sampled from Science direct databases for a survey on information security training and awareness;85% of the journals indicated that training and awareness contribute to improving security, 11% did not see any value and also 4% were undecided. This implies that there is a huge need of awareness and training. Figure 10shows the survey results on information security training and awareness.

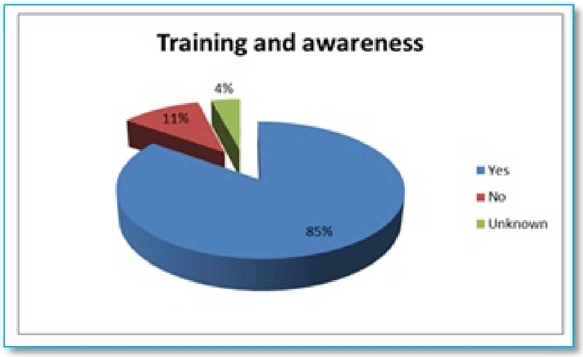


Fig 10: Do training and awareness contribute to security?

4.8 The Proposed Technical Security Framework

This section explores the proposed technical security framework, which comprises four main components: the user interface, encryption, access control and infrastructure, which were briefly discussed in sections 4.1 – 4.7.

The user logs in on the user interface, using a username and password, which are controlled by security radar to check the level of security, and then the credentials are encrypted and validated. After encryption and validation, if valid credentials have been completed successfully, the user will be allowed to access system data. Then audit logs are created on the server containing the details of who logged in, which files were accessed and which infrastructure was affected. The infrastructure includes the firewall, switches, IPCS, IDCS and servers.

These might have some benefits for the system to reduce data losses. The benefits of this system framework are:

- It ensures that many users have restricted and controlled access to employees' records.
- It gives employees confidence in securing the data.
- It provides proactive IPCS in protecting the network against attacks.
- It provides security radar on the dashboard to check the level of security.
- It tracks information security awareness through IP addresses.

Figure 11 shows the proposed technical security framework.

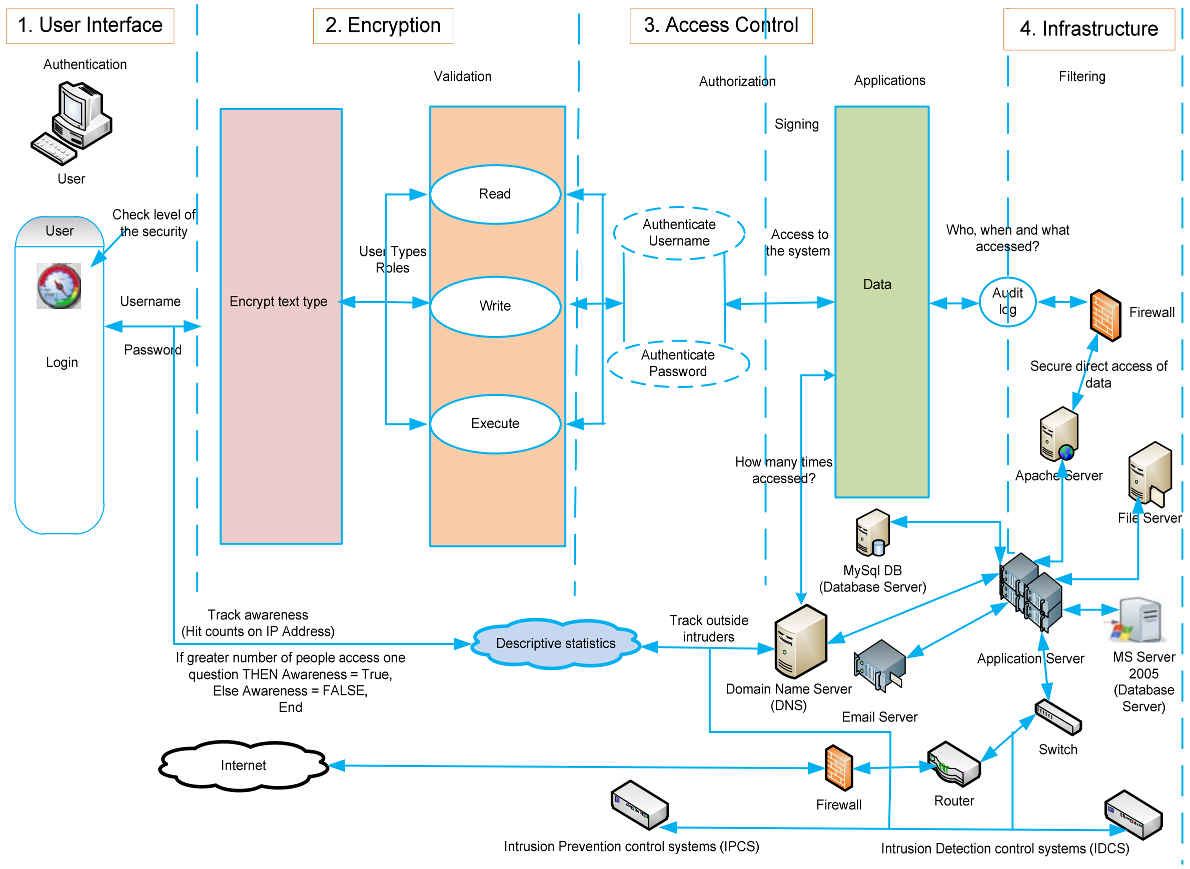


Fig 11: Proposed technical security framework.

4.9 Rating Information Security Implementation Strategy Using Ranking Model

Figure 12 illustrates the interconnection between different security networks (A to F) of various organizations.

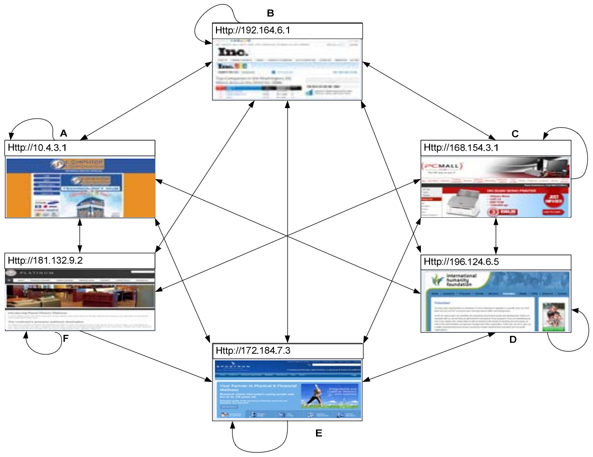


Fig 12: Interconnection of security networks

The different security networks of various organizations can communicate with one another by using IP addresses. Each security network has the capability of creating internal communication.

As described in section 3.4, equation (2) can be used for rating the information security implementation strategy associated with figure 12.

$$NSRx = (1 - d) + d \sum_{\forall y \in \mathrm{I}x} \frac{NSRy}{|Oy|} \qquad (2)$$

Table 1 describes the notations in equation (2)

Table 1: Notations

Ix The set of networks that communicates with x
|Ix|The number of networks that communicates with x
Ox The set of networks that are communicated to by x
|Ox| The number of networks communicated to by x
d Damping factor (set to 0.85 for Page Rank)

The security ratings will be done to include individuals who use their networked computers with identified by IP addresses. If more IP addresses access the target network, it might mean that the network is popular and could also imply that it is not safe. If IP addresses of well-known companies such as Microsoft or Oracle access the network, it might mean that the network may be safe enough.

5. DEPLOYMENT ANALYSIS

5.1 Status Of Information Security Implementation Strategies In Capricorn Fet College

This section shows analysis carried out using the two data sets. These include observations based on information security policy and awareness using local data from Capricorn FET College and data that are publicly available on the internet [32].

5.1.1 Information Security Policy Coverage

The information security policy coverage encompasses the international expected information security policy coverage, current coverage of information security policy in Capricorn FET College and expected coverage of information security policy from the proposed security framework. The international expected information security policy coverage is obtained from [41],[42] and [43], while the expected coverage of the information security policyand the current coverage of the information security policy are obtained from Capricorn FET College through a questionnaire.

Figure 13 outlines the information security policy coverage.

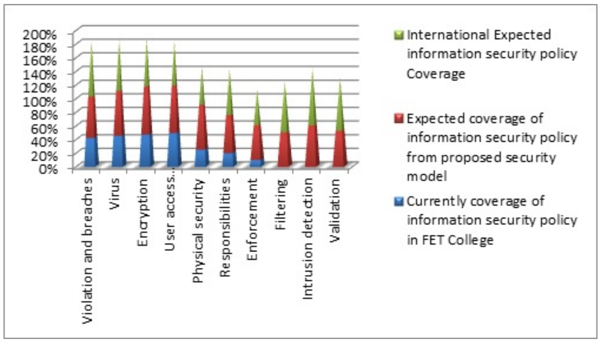


Fig 13: Information security policy coverage

Figure 13 showed a rise in violation and breaches at an average of 80% of the international expectation regarding an information security policy. The variation between the current FET coverage and international expectation indicates that the current FET coverage is insufficient in terms of filtering (0%), user access management (49%), intrusion detection (0%) and validation (0%), among others, with low ratings for other security components as well, as shown in figure 13. This situation has have been caused by the current financial constraints faced by the FET. This implies that the FET still lacks infrastructure to improve security to meet international standards.

5.1.2 Information Security Awareness Coverage

Information security awareness coverage entails the international expected information security awareness coverage, current coverage of information security awareness in Capricorn FET College and expected coverage of information security awareness by the proposed security framework. The international expected information security awareness coverage is obtained from [6],[44] and[45], while the expected coverage of information security awarenessand current coverage of information security awareness are obtained from Capricorn FET College through qauestionnaire. Figure 14 illustrates the coverage of information security awareness.

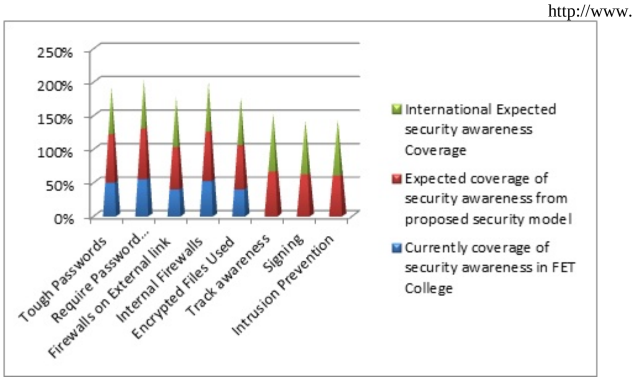


Fig 14: Information security awareness coverage

Figure 14 outline information security awareness coverage, which encompasses international expected information security awareness coverage, current coverage of information security awareness in Capricorn FET College and expected coverage of information security awareness by the proposed security framework. The variation between the current FET and international expected awareness coverage indicates current FET coverage deficiencies, indicated by 55% of the required password modification and also the low statistics of track awareness (0%), signing intrusion prevention (0%), etc. Results are shown in figure 14.

5.2 Scenario Of The Information Security Implementation Strategy

5.2.1 Scenario 1 – User-Allowed Access

Figure 15 shows the positive scenario of how a user is allowed into the system.

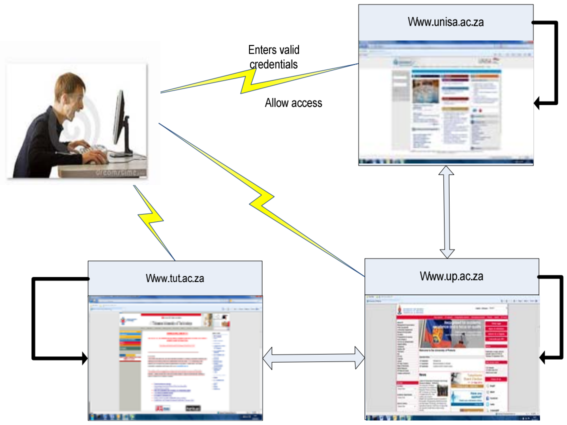


Fig 15: Access allowed on the system

Figure 15 indicates how Khomotso Maenetsha, the IT manager at Fetakgomo municipality in Limpopo Province, accesses the system. Khomotso would like to apply for admission to an engineering course on behalf of his younger sister who is staying in Tzaneen. Firstly, Khomotso is concerned about security on his laptop and the University of South Africa (UNISA) website. He accesses the website on the home page where the security radar is displayed. The security radar allows him to check the level of security of any institution.

He finds that the website is safe to browse; on the home page the radar is displayed in “green”. Then he enters his credentials, such as username and password, and passes through encryption and validation to ensure that the credentials have been secured and verified. He is then allowed even on the firewall, which filters access. Khomotso manages to obtain access, which allows him to manipulate data and register his younger sister. Now Khomotso and his younger sister are satisfied. He then decides to visit the application again. This implies that Khomotso trusts the UNISA network.

5.2.2 Scenario 2 – Unable To Access The Network Resources

Figure 16 shows the negative scenario of how a user is denied access to the system.

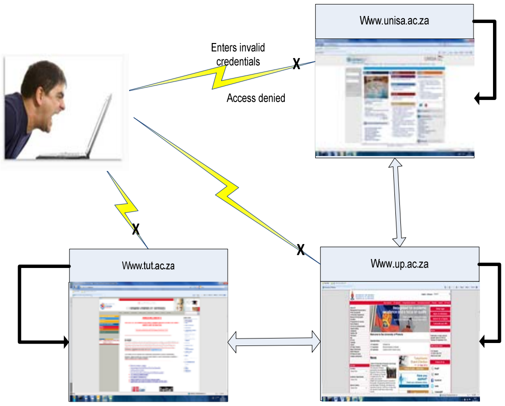


Fig 16: Access denied to the system

Figure 16 shows how Tebogo Makoe, an employee at ABC mining company, is denied access to the system. Tebogoleaves in the Dendron area in Polokwane. He is interested in enrolling in a part-time computer science course at UNISA or at a HEI such as Tshwane University of Technology (TUT) or the University of Pretoria, applying for admission online. He is not aware of any network security or threats that he might encounter. He simply ignores the security radar and does not check the level of security to see if it is safe to access the application.

The level of security is “red”, indicating that the network is in danger at that moment. He then proceeds to enter usernames and passwords. His credentials are incorrect and cannot be validated to allow him access to the system. After three failed attempts to use the usernames or passwords, the firewall proactively blocks access to the system and IPCS then disable his laptop to prevent any access. Now tebogo is dissatisfied and he never visits the website anymore. This implies that the network at UNISA might not be secure enough.

5.3 Comparative Evaluation Of Information Security Implementation Strategies

Table 2 shows a comparison of various technical security frameworks with the proposed technical security framework.

Table 2: Comparison of security framework.

FEATURES	SECURITY SERVICE AND TECHNICAL MODEL[46]	SECURITY SERVICE FRAMEWORK [47]	PROPOSED TECHNICAL SECURITY FRAMEWORK
Authentication	PKI	PKI, 2-Factor	Advanced authenticator
Encryption	Diffie-Hellman key exchange	RSA	Advanced encryption standard (AES)
Validation	No validation	No validation	Credential validator
User interface	Standard interface	Standard interface	Security level radar interface
Access control	Standard access control	Standard access control	Advanced Standard access control
Infrastructure	Standard infrastructure	Standard infrastructure	Advance infrastructure
Track awareness	No tracking	No tracking	Internet protocol(IP) address tracking awareness
IPCS	No IPCS	No IPCS	IPCS available
IDCS	No IDCS	IDCS available	IDCS available

From table 2, it was clear that the proposed technical security framework has more features to prevent unauthorized accessed compared to other frameworks. This implies that having to adopt the proposed technical security framework may reduce data losses and unauthorized access. The most three critical features of information security implementation strategies are discussed briefly in section 5.3.1 – 5.3.3.

5.3.1 Information Security Strategy Based On Track Awareness

[48] Indicated that security awareness is more effective when used appropriately. This might give users a sense of understanding early attacks or threats. Security awareness tracking strengthens security from application level through access level to infrastructure level.

Tracking of security awareness includes the use of IP address from the domain name server to determine if multiple users need training. If several users access certain resource from the system, it might mean that more emphasis on training is needed. The number of users who are trained on information security awareness has demonstrated the effectiveness of the training. The main benefit of security awareness is the minimized risk of attacks on the network and also on the ICT infrastructure at large [49].

5.3.2 Information Security Strategy Based On Intrusion Prevention Control System

An intrusion prevention detection system will be established in line with the following: creating systems with no susceptibility, taking good remedial action to discover vulnerabilities and repair them, and also detecting exploit efforts and blocking them before serious harm [50].The benefits of IPCS protection are that it protects ICT resources from existing and new attacks, it works in a real time environment and also with various enterprise products [51].

5.3.3 Information Security Strategy Based On Intrusion Detection Control System

According to [52], the benefits of intrusion detection systems are that they authenticate the success or failure of an attack, are able ability to monitor system and user activities, detect attacks in cases where there are failures on the network or protect against external users and are cheaper to maintain. The advantage of intrusion detection are improved integrity of the core information security infrastructure, improved system and application monitoring, tracing of user activity from start to end and ease of reporting modification of files [53].

6. OPEN RESEARCH ISSUES IN INFORMATION SECURITY IMPLEMENTATION STRUCTURE

We explored articles from Science direct and IEEE databases to describe different researchers' views on future work and challenges encountered. The main challenge seems to be lack of profound understanding of information security strategies. This hampers determination of security needs, monitoring of resources and the identification of security technologies and ways of securing technology management [54].Some of the problems might be caused by lack of a good approach tithe development of a security model [55].Problems might also be caused by regulatory laws, which differ from country to country in HEIs [56]. Regulatory frameworks might create difficulties in the implementation of information security strategies.

Figure 16 categorizes open research and labels the work to be done in future, numbered from 1 to 11. The categories of open research should follow in sequence, i.e. before determining the security needs; the information security strategy has to be understood first. Therefore, we have categorized open research in figure 16.

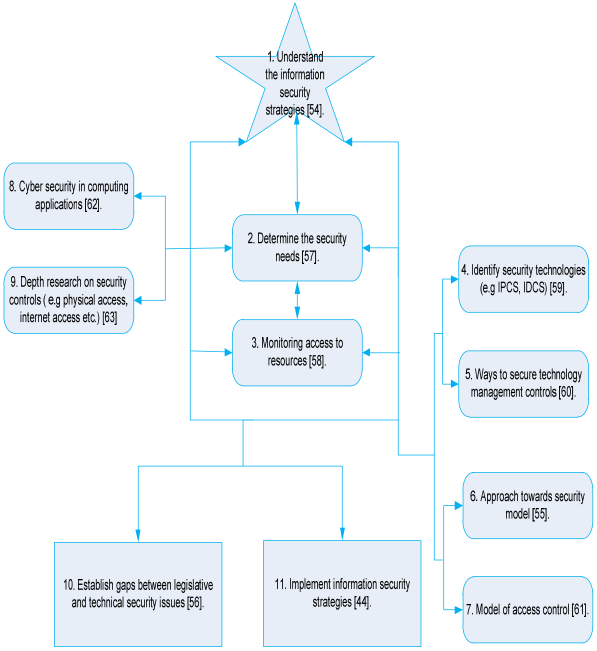

1. Understand the information security strategies [54].
8. Cyber security in computing applications [62].
9. Depth research on security controls (e.g physical access, internet access etc.) [63]
2. Determine the security needs [57].
3. Monitoring access to resources [58].
4. Identify security technologies (e.g IPCS, IDCS) [59].
5. Ways to secure technology management controls [60].
6. Approach towards security model [55].
7. Model of access control [61].
10. Establish gaps between legislative and technical security issues [56].
11. Implement information security strategies [44].

Fig 16: Categorization of open research.

7. CONCLUSION

We have proposed a technical security framework and outlined all of its components in order to secure data in a HEI. In the literature, what has been achieved in creating awareness of information security seems insufficient, but the experimental results using real-life publicly available educational records and data gathered from Capricorn FET College shows that awareness and development of information security could be the best option in improving security in the HEI.

We discussed in detail a comprehensive survey of different security attacks on information systems and categorized them as general organizations-related and specific HEI-related attacks. Our findings indicate that employees are encountering challenges in terms of ICT infrastructure and applications to secure data. The major challenge in this research is the inability to experiment with this system on real-life educational records from Capricorn FET College because of confidentiality issues.

However, our approach enabled us to experiment with the management of employees, since we were allowed access to employee's records. One can see that creating information security awareness can minimize security breaches. In this paper, we investigated and explained the status of information security implementation strategies used in Capricorn FET College and internationally and compared them on the basis of security policy coverage and security awareness coverage in Science direct research databases.

This paper further described deployment analysis on how the proposed strategy could be used or implemented through real-life scenarios categorized as user-allowed access and user access denied. We also surveyed the information security implementation strategies currently in use and compared them on the basis of track awareness, IPCS, IDCS and others. The scalability and reliability of our approach to information security strategies guarantee that the proposed security system will provide HEIs throughout the world with a more secure, flexible, effective and efficient environment.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the financial support of Tshwane University of Technology and resources made available by the University of South Africa, South Africa.

REFERENCE

[1] The New York Times Company, "Information Security," 2012. Retrieve 21 April 2012. From http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity.htm.

[2] A. McIlwraith, Information security and employee behavior, How to reduce risk through employee education, training and awareness. Gower Publishing, 2006.

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

[4] M.E. Whitman and H.J Mattord, Principles of information security. 2nd ed. Thomson, 2005.

[5] B. O. Omotayo and N. A. Ajayi. An appraisal of security measures in Hezekiah Oluwan Sanni Library, Obafemi Awolowo University, Ile Ife. Nigerian Libraries, 2004, Pp39, 65 - 78.

[6] R. Rezgui andA. Marks, Information security awareness in higher education: An exploratory study. School of Engineering, Queen's Buildings, The parade 4th, CF24 3AA, Salford, Cardiff, United Kingdom, 2008.

[7] D. Oblinger, IT security and academic values. Educause leadership strategies: Vol 8 Computer and network security in higher education. San Francisco, CA: Jossey-Bass, 2003. pp.31-44.

[8] R. Marchany, "Conduction a risk analysis," 2003. Retrieve 12 May 2012. From http://net.educause.edu/ir/library/pdf/pub7008g.pdf.

[9] N. Sklovos and P. Souros, "Economic models and approaches in information security for computer networks," International Journal of Network Security, 2006, 2(1):243–56.

[10] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating it security investments," Communications of the ACM, 2004, 47(7): 87–92.

[11] B. Jung, I. Han, et al, Security threats to Internet: a Korean multiindustry investigation. Information and Management, 2001, 38:487–98.

[12] Innova, "Information Security Management Framework Implementation," 2011. Retrieve 12 April 2012. From http://www.innova-sa.eu.

[13] USLegal,"Safety Law & Legal Definition,"2012. http://definitions.uslegal.com/s/safety/.

[14] RM Education, "e-safety," 2012.Retrieve 07 August 2012. From http://www.rm.com/shops/solutionsandservices/Product.aspx?cref=PD2392344.

[15] National School Safety and Security Services,"National School Safety and Security Services,"2012.Retrieve 07 August 2012. From http://www.schoolsecurity.org/.

[16] Oxford University Press,"Safety,". 2012. Retrieve 07 August 2012. From http://oxforddictionaries.com/definition/english/safety.

[17] M.Shariati, F. Bahmani, F. Shams, "Enterprise information security, a review of architectures and frameworks from interoperability perspective," Proc Computer Science 3 (2011) 537–543.

[18] S. Posthumus and R. Von Solms, A framework for the governance of information security. 2004. Computers & Security (2004) 23, 638 – 646.

[19] A. Zuccato, Holistic security management framework applied in electronic commerce. Computers & security 26 (2007) 256 – 265.

[20] A. Da Veiga, N. Martins, and J.H.P Eloff, Information security culture – validation of an assessment instrument. Southern African Business Review, 2007; 11(1):146–66.

[21] J.O., Aagedal, et al, "Model-based risk assessment to improve enterprise security," Proc. Sixth International Enterprise Distributed Object Computing Conference (EDOC 02), 2002.

[22] Scholtz, T., Structure and Content of an Enterprise Information Security Architecture. 2006, Gartner Inc.

[23] S. Jianguang, and C. Yan,"Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture," Future Information Technology and Management Engineering (FITME 08),. International Seminar on, 2008.

[24] R. Vernik, T. Blackburn, and D. Bright, Extending interactive intelligent workspace architectures with enterprise services. Internal publication at the School of Computer and Information Science. University of South Australia, 2003.

[25] B. Chapman and E.D. Zwicky, Building Internet Firewalls. O'Reilly, Sebastopol, 1995.

[26] F.H. Katz,"The effect of a university information security survey on instructing methods in information security,"Proc.Second annual conference on information security curriculum development, 2005, pp 43–8.

[27] C.C. Wood, What do the recent terrorist attacks mean for the American information security profession? Computers & Security, 20 (2001) 667-670.

[28] K.R. Sarkar, Assessing insider threats to information security using technical, behavioural and organisational measures. Information security technical report 15(2010)112 – 133.

[29] D.W. Straub and W.D. Nance, Discovering and disciplining computer abuse in organization: a field study, MIS Quarterly 1990, pp. 45–55.

[30] T.R. Peltier, Information Security Risk Analysis, Auerbach, New York, 2001.

[31] Open Security Foundation,"Data Loss Statistics," 2012.Retrieve 07 July 2012. From http://datalossdb.org/statistics.

[32] SCIENCEDIRECT, "Top Articles," 2012. Retrieve 14 August 2012. From http://www.sciencedirect.com

[33] G. Stewart, A safety approach to information security communications. Information security technical report 14, 2009, pp 197- 201.

[34] H.S. Chana Alan, H. Sung Han, W.Y. Annie, P. Wonkyu,"Hong Kong Chinese and Korean Comprehension of American security safety symbols," International Journal of Industrial Ergonomics 39 (2009) 835–850.

[35] A. Da Veiga and J.H.P. Eloff, A framework and assessment instrument for information security culture. Computers & Security 29(2010) 196 – 207.

[36] A. Sidiropoulos and Y. Manolopoulos, "Generalized comparison of graph-based ranking algorithms for publications and authors" The Journal of Systems and Software 79 (2006) 1679–1700.

[37] E.Tomura and Y.M. Ertenb, Application of temporal and spatial role based access control in 802.11 wireless networks. Computers & security 25 (2006) 452 – 458.

[38] S. Preda, F. Cuppens, N. Cuppens-Boulahia, J. Garcia-Alfaro and L. Toutain, "Dynamic deployment of context-aware access control policies for constrained security devices," The Journal of Systems and Software 84 (2011) 1144–1159.

[39] B. Blobel,"The European Trust Health Project experiences with implementing a security infrastructure," International Journal of Medical Informatics, 60 (2000) 193–201.

[40] M. Castruccia, A. Nerib, F. Caldeirac, J. Aubertd, D. Khadraouid, M. Aubignye, C. Harpese, P. Simõesc, V. Suracif, and P. Capodiecig, "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," International journal of critical infrastructure protection 5(2012) 86 – 97.

[41] N. Doherty, L. Anastasakis, H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," International Journal of Information Management, 29 (2009) 449–457.

[42] J. Kenneth Knapp, R. Morris, and E. Thomas. Marshall, T. Byrd, Information security policy: An organizational-level process model. Computers & security 28 (2009) 493 – 508.

[43] L. Karadsheh, Applying security policies and servicelevelagreement to IaaS service model to enhance security and transition. Computers & security, 31 (2012) 315 – 326.

[44] M. gaoglu , Erdem, S. Eren, The positive outcomes of information security awareness training in companies: A case study,Information security technical report1, 2009, pp223 – 229.

[45] R.S. Shaw, C. Chen, L. Albert Harris, and H. Huang, The impact of information richness on information security awareness training effectiveness. Computers & Education 52 (2009) 92–100.

[46] NASSCOM, "Security Services and Technical Model," 2012. Retrieve 14 April 2012. From http:// www.dsci.in/framework/358.

[47] G. Stoneburner, Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology (NIST). Special Publication 800-33, 2001.

[48] P. Kumaraguru, Y.Rhee, A. Acquisti, L.Cranor, J. Hong, E. Nunge, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," Proc. SIGCHI conference on Human factors in computing systems. San Jose, California, USA, 2007, pp. 905 – 914.

[49] T.N. Jagatic, M. Johnson, M.Jakobsson, and F. Menczer, "Social Phishing,". Communications of the ACM. Vol. 50, Issue 10, 2007, pp. 96 – 100.

[50] C. Iheagwara, F. Awan, Y. Acar, and C. Miller, "Maximizing the Benefits of Intrusion Prevention Systems: Effective Deployments Strategies," 18th Annual FIRST Conference. 2006.

[51] Enterasys Networks, "Intrusion Prevention System," 2011. Retrieve 20 August 2012. From: https://www.enterasys.com/company/literature/ips-ds.pdf .

[52] SANS Institute,Intrusion Detection Systems: Definition, Need and Challenges Institute. 2001. InfoSec Reading Room.

[53] ICSA, Assessment Intrusion Detection for System and Network Security Management. 2001.

[54] F. Olav Sveena, J.M. Torresa,, J.M. Sarriegia, "Blind information security strategy,"International Journal of critical infrastructure protection 2(2009) 95 – 109.

[55] H. Tanaka, K. Matsuura, and O. Sudoh,"Vulnerability and information security investment," Journal of Accounting and Public Policy, 24 (2005) 37–59.

[56] P. Sangkatsanee, N. Wattanapongsakorn, and C.l Charnsripinyo, Practical real-time intrusion detection using machine learning approaches. Computer Communications 34 (2011) 2227–2235.

[57] Y. Banga, D. Leeb, Y. Baec, J Ahnc, and A. Desautels, "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure,"International Journal of Information Management, 2012, pp207-43.

[58] J. Chea, Y. Duanb, T. Zhanga, and J. Fan, "Study on the security models and strategies of cloud computing," Proc. China Engineering, 23 (2011) 586 – 593.

[59] L. Xiao, B. Hu, M. Croitoru, P. Lewis, and S. Dasmahapatra, A knowledgeable security model for distributed health information systems. University of Southampton, UK. Computers & security 29 (2010) 331 – 349.

[60] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel, "Model-driven business process security requirement specification," Journal of Systems Architecture 55 (2009) 211–223.

[61] T. Doan, A framework for software security in UML with assurance. PhD thesis, The University of Connecticut, 2008.

[62] G. David-Rosado, E. Fernández-Medina, and J. López, “Security services architecture for Secure Mobile Grid Systems,” Journal of Systems Architecture, 57 (2011) 240–258.

[63] L. Fuchs, G. Pernul 1, and R. Sandhu, Roles in information security: A survey and classification of the research area.Computers & security 30 (2011)748 – 769.