An Exploratory Study on Information Security Vulnerabilities in Higher Education: Case of University of Vocational Technology, Sri Lanka

H. A. Seneviratne[1], M. Thenabadu[2*], W.M.G.K. Wijerathne[3]

[1]*Department of Multimedia and Web Technology, Faculty of Information Technology, University of Vocational Technology, Sri Lanka*
[2]*Department of Agriculture and Food Technology, Faculty of Industrial Technology, University of Vocational Technology, Sri Lanka*
[3]*TECH- CERT, Pvt Ltd.,1 st Floor Bernard Business Park, N0106, Dutugemunu St, Dehiwala Sri Lanka.*
**Corresponding author*

***Abstract*: The study investigates the University of Vocational Technology's Information System's (IS) security vulnerabilities. Aim of the study is to investigate general system security vulnerabilities, staff opinion on potential vulnerabilities of the system in relation to the CIA Triad and to identify measures to address vulnerability issues. Multiple data collection methods, such as questionnaire, observation, and focus group discussion, are used in case-study approach. According to the findings, hardware and software vulnerabilities indicated the highest possible occurrence (22%) and the occurrence of emanation vulnerabilities indicated the least (2 %) under identified general vulnerabilities. Findings of staff opinion on the IS security implemented in the University information system in terms of CIA triad, revealed that, majority were dissatisfied with the confidentiality, integrity and availability factors Hence, overall IS security satisfaction among university staff was found to be inadequate.**

According to the results of the observations and focus group discussions the University of Vocational Technology's information system was discovered to be highly vulnerable. The system performed poorly in all aspects of the CIA Triad, indicating that the system's overall vulnerability is high. A number of recommendations are made based on focus group discussions to mitigate IS security vulnerabilities in the studied environment. The major recommendations are, improve information security awareness of staff, develop operator guidelines and develop and implement a successful vulnerability management programme for the University. Further, the study's findings add to the body of knowledge of empirical studies relevant to the CIA Triad.

***Keywords* —: CIA Triad, Information Systems Security, vulnerability**

I. INTRODUCTION

Information systems (IS) are critical for any organizations success. Most organizations consider information system security to be a critical issue. With the introduction of Information Technology (IT) and the widespread use of the internet and its services, the number of attacks on information systems has increased, necessitating the need to protect information systems [1] Maintaining the basic aspects of the information security phenomenon, namely confidentiality, availability, and integrity, known as CIA triad required to ensure the security of information systems. [2]

As early as 1975, there were concerns about the security and confidentiality of information systems (IS) in University computer network environment. [3] Given their increasing complexity, interconnections, uncertainties, and reliance on technology, academic organizations, according to literature [4] face the challenge of protecting vital information. There are two reasons why colleges and universities have become targets of security breaches: their vast computer power and their open access policies [5]. University information infrastructures are intended to serve both internal and external stakeholders such as faculty, students, visitors, and researchers from around the world. This facility is frequently used to share information, but it can compromise information security at times. Academic institutions must also ensure the confidentiality of student data, the availability and integrity of information, and the continuity of public services, many of which are mediated by technology [6]

Some researchers argue that higher education institutions in developing countries continue to struggle in terms of information security due to poor information technology platforms, limited funds and technical know-how.[4]Many developing countries around the world still lack adequate regulation and/or enforcement to protect users' data and privacy. Understanding the IT security threats and challenges confronting higher education is critical in this context to avoid potential loss of university information and knowledge assets. [1].

As per Hwang [7] it was highlighted that, technical improvement of information system security is not sufficient as information security is a multidimensional in nature. According to ENISA [8], approximately 77 percent of data breaches in companies are caused by the exploitation of human weaknesses. It was previously discovered that employees' poor information security compliance was responsible for more than half of all information security breaches.

Previous research has claimed that lack of employees' awareness on information security vulnerabilities was the primary cause of sensitive information mishandling [9].

Furthermore, awareness on information security vulnerabilities is widely accepted research area [10] owing to the discovery of multidisciplinary nature of many security breaches in Information systems and networks [11].

This is also one of the main reasons why the latest Cyber Security Breaches Survey 2019 shows that cybersecurity is a high priority for the senior management of organizations [12]

According to Jaeger [13] "research on information security vulnerability awareness is still a developing field with many uncharted areas to be explored" According to Marks [1], Information security vulnerability awareness studies in developing countries, particularly in the higher education sector, are insufficient.

University of Vocational Technology is established under the Parliamentary Act No 31 of 2008 with the vision to be the leading University of Vocational and Technical Education sector in Sri Lanka. The University of Vocational Technology hosts four Faculties, nine departments, and teaches about 1800 students in the fields of mechatronics, manufacturing, IT(software/network/multimedia & web), food technology, film and television production, building services technology, construction technology, industrial management and teaching. [14]

The proposed research contributes to the body of knowledge by addressing the above identified gaps. The study looks at the factors that influence the awareness on information security vulnerabilities in particularly based on three pillars of information security (CIA Triad), Confidentiality, Integrity and Availability with among University of Vocational Technology staff. After the introduction, the methodology and analysis of the case-study results are provided. Finally, the paper concludes with a set of recommendations for promoting awareness of information security vulnerabilities in the investigated environment.

II. METHODOLOGY

The general aim of the research is to explore the awareness of Information system security vulnerabilities of higher education institutions in Sri Lanka. An interpretive case-study approach is employed to conduct the research. The case-study is represented through University of Vocational Technology, Sri Lanka.

The research addresses the following three main research questions:

1. What are the general information system vulnerabilities faced by University of Vocational Technology?
2. What is the level of satisfaction among University of Vocational Technology staff with the IS security implemented?
3. What are the ways to overcome vulnerabilities and improve information security in University of Vocational Technology?

In order to identify risk factors influencing Information Security measures and vulnerabilities of the University, the study design to be incorporated with three research methods: a quantitative field survey, qualitative one-on-one interviews, and an empirical assessment of University network activity to portray a holistic view of the participants and provide interpretive reflections.

The data collection period was extended from March 2021 to April 2021, a one-month period during which questionnaires were distributed, documents were collected, observations were made, and interviews were conducted. The study was carried out with the necessary ethical approvals, and participants' consent was obtained, as well as the right to decline participation and anonymity. Furthermore, the research's objective, purpose, and nature were clearly explained to all respondents.

Questionnaire:

For the quantitative component of this study, which in terms of Confidentiality, Integrity and Availability (CIA Triad) the questionnaire method was selected. The questionnaire was adapted from previous literature and pre-tested by expert panel. The study sample included 40 employees in the University representing different sub units of the University. Sample was selected based on purposive sampling technique where relevance to study is concerned. Response rate achieved was 90%. The data was analyzed with descriptive analysis such as mean, frequency and percentage.

Interviews:

Five Information Systems personnel at University of Vocational Technology were participated for the focus group discussion on evaluating vulnerabilities associated with university information system.

Documents:

Several documents were analyzed to support research findings such as University systems logs, Information System policies, reports and system manuals

III. RESULTS AND DISCUSSION

The respondents were asked to identify key general vulnerabilities faced by university based on given list of vulnerabilities [19] namely; physical vulnerabilities, natural vulnerabilities, hardware/software vulnerabilities, media vulnerabilities (e.g., stolen/damaged disk/tapes), emanation vulnerabilities---due to radiation, communication vulnerabilities and human vulnerabilities.

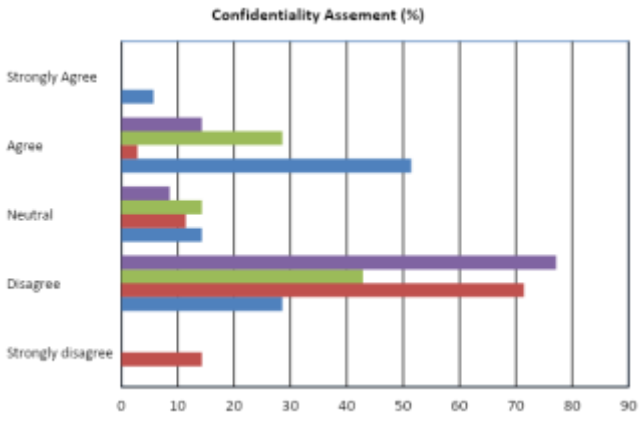
As per the respondents' views, "Hardware and Software vulnerabilities" have the highest possible occurrence in the university information system which is 22%.The lowest possible occurrence (2%) is identified as emanation vulnerabilities.20% respondents identified "physical vulnarabilities";13% identified natural vulnerabilities; 16% Media vulnerabilities ;17% communication and Human Vulnerabilities identified as 10% respectively.

Vulnerabilities specific to University information System in terms of Confidentiality, integrity and availability (CIA Triad) were assessed using 5 point Likert scale with 1- Strongly Disagree 5- Strongly Agree. [15] Based on the checklist with questionnaire items [16]

Table 1: Check list on Confidentiality, integrity and availability (CIA Triad) measurements Bidgoli, H. (2016).

Confidentiality Assessment	
Q1	Your IS is providing access to the authorized person only
Q2	Your IS is using up-to-date tools of authorization
Q3	IS has measure or procedure to identify if any unauthorized access occurs in your system
Q4	You satisfy with the personal security of your IS
Integrity Assessment	
Q1	Your IS users have different access levels(Access control list)
Q2	You satisfy with access control provided in your IS, that no overrides possible once access control is given
Q3	Your IS has proper encryption and decryption process when storing and transferring of information
Availability Assessment	
Q1	Your IS has Comprehensive backup plan for both the data in servers and individual computers
Q2	You satisfy with the measures used to achieve physical security of your IS (Locked doors, Physical intrusion detection systems, Secured equipment, Environmental monitoring)
Q3	You satisfy with the Information security policy of your organization
Q4	You satisfy with data, software as well hardware to available for authorized users on demand regardless of time and location and any other disruptions such as power outage, hardware failure or software upgrades

Figure 01: Confidentiality Assessment



According to the results obtained from the survey, it was revealed that 51% agree that the system provide access to only authorized personnel. But 29% disagree and 14% remained neutral on the question asked. Second question was asked whether the system uses up-to-date tools for authorization which as disagreed by 71%. Majority of respondents (43%) disagreed on the availability of procedure for detecting if any unauthorized access occurs in the system. 29% agreed that such detection system available. Overall, confidentially aspect of the System, majority (77%) was not satisfied.

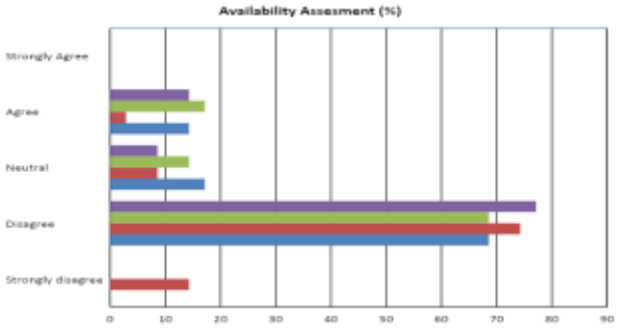
Figure 02: Integrity Assessment

As per the survey results, majority of respondents agreed (71%) that the system has Access control list.

Second question in this category seek response on whether overrides possible in the system once the access control is given, which majority (57%) of respondents were not satisfied with this aspect.

Majority (57%) respondents disagreed on the availability of proper encryption and decryption process when storing and transferring of information.

Figure 03: Availability Assessment



According to the survey results, the majority of respondents opposed having a comprehensive backup plan for both data on servers and individual computers. The vast majority of respondents (74%) were dissatisfied with the measures taken to ensure the physical security of your MIS (Locked doors, Physical intrusion detection systems, Secured equipment, Environmental monitoring) The information security policy did not satisfy respondents (69%). The majority (77 %) were dissatisfied with data, software, and hardware being available on demand for authorized users regardless of time or location,

as well as any other disruptions such as power outages, hardware failure, or software upgrades.

Based on the documentation researched, it was observed that there are no proper procedures to identify and respond to security events, identification, notification, and response to suspected attacks procedures for the containment of security concerns was lacking. Vulnerability identification and correction is not in place and no any network intrusion detectors (NID) on the system is observed. Also it was identified lack of methods in place to ensure hardware integrity, software integrity and to ensure the confidentiality of the information system. Configuration management of Information System is identified as a major vulnerability as many related aspects with reference to Configuration management is lacking in the University information system.

Lacks of encryption, lack of integrity of the data during transmission are aspects which identified as vulnerabilities.

According to focus respondents, the most serious security threats in recent years have been mainly due to software and hardware failure, human error, people deliberately extorting information and deficiencies in technological knowhow. Focus group discussions revealed that, there are no clear policy statements and controls concerning the intent of the University to protect the data resources from accidental or deliberate unauthorized disclosure, modification, or destruction. Also serious drawback pointed out by focus group was lack information security awareness of staff. It was observed that the staff personnel been not fully briefed on how to mitigate system security risks. Lack of procedure is observed to check background or reference checks used for individuals who have routine access to sensitive information. It was observed that the system does not have operations guidelines (Hours, location, and type of work; user access and login privileges restricted to duty hours and is there no inactivity timeout on the system. The system currently not set to an audit and System does not have audit log requirements for workstations

IV. CONCLUSION

The study's first research question seeks to investigate general vulnerabilities in the University information system. According to the findings, hardware and software vulnerabilities have the highest possible occurrence, which is 22 percent. Emanation vulnerabilities have been identified as having the lowest possible occurrence (2%).

The second research question sought to investigate was the level of satisfaction among University of Vocational Technology staff with the IS security implemented in the University information system in terms of CIA triad. The majority (77 %) were dissatisfied with the confidentiality of the existing System. As a result, the confidentiality of the University information system was concluded inadequate. According to the survey results, the majority of respondents (71 %) agreed that the system has an access control list but overall satisfaction with the integrity aspect was also low. According to the survey results, the system's availability factor also exhibited low satisfaction. As a result, overall IS security satisfaction among university staff was found to be inadequate.

Based on the findings of the observations and focus group discussions I was revealed that, the University of Vocational Technology's information system is highly vulnerable. The system performed poorly in all aspects of the CIA Triad, implying that the system's vulnerability is high in general.

Reflecting on the research, the first two objectives were met successfully, but the third requires further knowledge from IT experts in order to develop a successful vulnerability management programme.

The findings of this research are very significant for the University because no vulnerability assessment has been performed in a similar capacity. The study's findings add to the body of knowledge of empirical studies relevant to the CIA triad. This research positively contributed to identifying the loopholes and drawbacks of the existing system.

.5. Limitations and future directions

This study took an exploratory approach and used simple descriptive data analysis with frequency distributions. The focus group observations were qualitatively analyzed. As a result, additional research in this field is required to conduct more in-depth research based on more statistically rigorous research design in order to reach solid conclusions.

A further investigation is required to develop and implement a successful vulnerability management programme for the University of Vocational Technology.

Conflict of interest:

The authors declare that they have no conflicts of interest.

ACKNOWLEDGEMENT:

The study was self-funded by the authors and they would like to thank the respondents who took part in the study.

REFERENCES

[1] 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; 2007.

[2] Sadaf Hina & P. Dhanapal Durai Dominic (2018): Information security policies' compliance: a perspective for higher education institutions, Journal of Computer Information Systems, DOI: 10.1080/08874417.2018.1432996

[3] Kerievsky B. Security and confidentiality in a university computer network. ACM SIGUCCS Newsletter Archive 1976;6(3):9–11. New York, NY: ACM.

[4] Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & security, 27(7-8), 241-253.

[5] Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. In Proceedings of the 2nd annual conference on Information security curriculum development (pp. 43-48).

[6] Ahlan, A. R., & Lubis, M. (2011). Information security awareness in university: maintaining learnability, performance and adaptability through roles of responsibility. In 2011 7th International Conference on Information Assurance and Security (IAS) (pp. 246-250). IEEE.
[7] Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. Journal of Computer Information Systems, 61(4), 345-356.
[8] ENISA. (2019). ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends. Heraklion: european Network and Information Security Agency (ENISA)
[9] Ernst, Y., (2018- 2019). Global Information Security Survey, New York
[10] Haeussinger, F., Kranz, J. (2017). Antecedents of employees information security awareness-review, synthesis, and directions for future research.
[11] Ingham, L. (2018). 88% of UK data breaches caused by human error, not cyberattacks. The Verdict Magazine.
[12] Vaidya, R. (2019). Cyber security breaches survey 2019. Department for Digital, Culture, Media and Sport, 66.
[13] Jaeger, L. (2018). Information security awareness: literature review and integrative framework. In Proceedings of the 51st Hawaii International Conference on System Sciences.
[14] UoVT | UNIVERSITY OF VOCATIONAL TECHNOLOGY. (2022). Retrieved 05 May 2022, from http://www.uovt.ac.lk/
[15] Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. Journal of extension, 50(2), 1-5.
[16] Bidgoli, H. (2016). Integrating real life cases into a security system: Seven checklists for managers. *American Journal of Management*, *16*(4), 9.