Evaluating the Actual Situation of Information Systems Security in Technical Colleges in KSA and Ways to Improve it

Mohammad Fhaid Alharby,[a]
[a] Buraydah College of Technology, Buraydah, Qassim, Saudi Arabia
Buraydah, Fourty street
malharby@tvtc.gov.sa

Abstract

The following paper explores and evaluates the existence, efficiency and adequacy of information systems security among sampled technical colleges in the Kingdom of Saudi Arabia. The author further explores the weaknesses and offers plausible remedies for the systems to detect, prevent and auto correct breaches in security. The researcher undertakes an empirical survey using self-administered questionnaire aimed at achieving these objectives. The researcher distributed three hundred questionnaires but ascertained two hundred and seventy-five responses valid and usable for analysis and decision making on the state of information security systems in Saudi Arabia's technical colleges. From the results, a number of inadequately effected security controls were highlighted and recommendations and suggestions introduced to strengthen the weak areas, close identified loopholes and correct breaches in the present security system controls. Based on the findings, the benefits of this research are mega fold extending across the different users of information system in technical colleges such as students, instructors, managers, auditors and practitioners alike. The findings, recommendations and conclusion could help them further advance their knowledge and secure their information systems to champion the next phase of Saudi Arabia's development, quality human resource.

Keywords: Information System Security, Empirical Study, Security Controls, Breaches, Kingdom of Saudi Arabia.

1. INTRODUCTION

The higher competitive environment especially in imparting technical skills and knowledge notwithstanding, technical colleges continue to gear up and gain competitive edge over their rivals. Most technical colleges across the globe, in KSA notwithstanding, employed latest technologies and especially at the turn of the 20th Century. Most notably, technical colleges continue to deploy usage of cloud computing and outsource complex Enterprise Resource Planning systems. Alongside expanded branch network of technical colleges in KSA, this usage among educational organizations presents new challenges, wide area networks, mega databases, virtual private networks and web interfaces usage. These features proliferate vulnerability of technical educational establishments to cyber space threats.

In their latest report on their website detailing statistics on IT security, WhiteHat reports that, a majority of websites received at least a serious vulnerability daily in 2015, or approximately 9 – 12 months in a year. According to WhiteHat, a meagre16% of educational establishments' websites were exposed less than 30 days in a year overall. Still, in an analysis of cyber hacks, threats and exposure across industries, WhiteHat reported 71% were in the education realm, 58% in social networking realm and 51% in retail websites. The following paper addresses Information System Security (ISS) in Technical Colleges in KSA. The researcher proposes a Two Tier model to enhance security in educational establishments in Saudi Arabia.

2. INFORMATION SYSTEM SECURITY (ISS)

According to Pattinson (2015) in Abu-Musa (2014, p. 354), ISS refers to the adequacy of management controls to detect, prevent, avoid and recover from a whole array of threats that can cause disruption or damage to computer systems. Singh (2016) in Abu-Musa (2014, p. 354), however, argues that no system can assure sound proof avoidance, prevention, recovery and detection from threats although any information security management action is most essential in cascading factors that motivate cyber threats and security breaches.

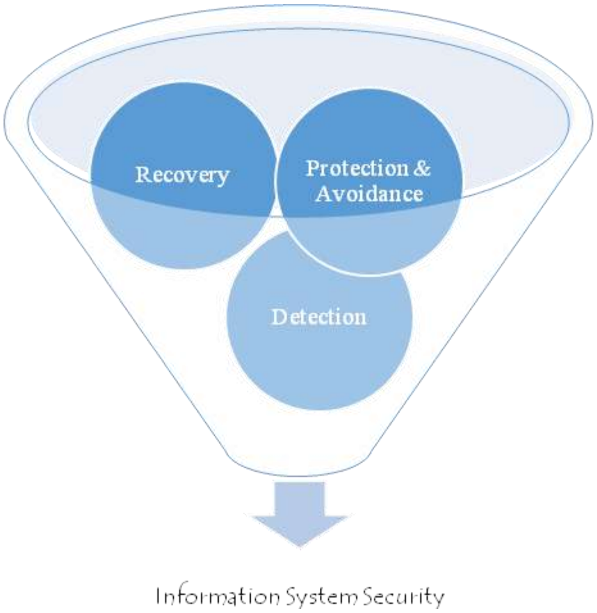

Fig. 1 Information System Security

3. INFORMATION SYSTEM IN TECHNICAL COLLEGES

According to Kudrass (2016) in Abu-Musa (2014, p. 354), information system in technical colleges just like in universities must provide scientific and research information, cooperation, courses on offer, locations, management, further education capabilities, profiles of key staff, captures student bio among others. Consequently, such information is both complex and confidential that usual information systems present in most commercial organizations and most succinctly, must pay detailed attention to its students and trainers (Luo & Warkentin, 2014).

According to the Technical and Vocational Training Corporation (TVTC) (2012), the information system in use in most technical establishments is akin to the Land Grant University System. True, the King Abdulaziz University uses a replica information system.

The information system's features can be grouped into three parts based on the stakeholders, namely, student, member and employee. A student, employee or trainer can view the above systems provided they have a unique username and password generated by the system administrator immediately they are admitted, employed or engaged (Ahmad, 2013). Previously, the information system was supported by a complex server system hosted within the technical colleges premises. However, some colleges have outsourced to save on costs such as infrastructure and have adopted cloud computing providers such as Google and Microsoft . The system enhances connectivity between and among satellite campuses and main campus across the kingdom ensuring fast internet connectivity among the three groups.

4. METHODOLOGY

The researcher set out the answer the following research hypothesis

HI: The implemented security controls in safeguard information system in Technical Colleges in KSA are adequate

H2: Decisions relating to the security of information system in KSA's technical college are made by managers outside the IT department leading to insufficient controls

H3: There are no substantial differences among Technical Colleges in Saudi Arabia with regard to the adequacy of effected security controls to safeguard information systems

4.1 Data Collection

The researcher undertook an empirical survey using a self-administered questionnaire tool to investigate and examine the presence and adequacy of security controls to safeguard information system in technical colleges. The researcher sent out three hundred questionnaires to staff members of technical colleges specialist, employees as well as administered questionnaires to students at sampled technical colleges. Two hundred and seventy-five responses were certified valid and usable for analysis and decision making on the state of information security systems in Saudi Arabia's technical colleges. The security controls were classified into physical access and hardware, organizational, data and data integrity, electronic access and software, offline programs, bypassing normal access, division of duties, user programing, periodic, and output security controls.

The researcher adopted a "yes" or "no" set of questions to simplify the respondents' clarity and obtain honest clear and articulate responses. The author arranged the questions meticulously for respondents to answer smoothly sequentially. The author exposed the responses to Alpha Cronbach's model to test its reliability and explore internal consistency relative to average inter-item correlation. The response was an Alpha value of 0.8735 which was considerably high level of reliability and internal consistency. Students' responses were also analyzed to identify any significant differences between the early respondents (120) and the late respondents (85). The results showed no significant difference at a significance level of p = 0.05. Consequently, the researcher concluded that there was no evidence of misrepresented and unbiased data based on the selected sample.

Table 1 Research Sample As per Classification of Respondents

Research Sample As per Classification of Respondents		
Respondents Classification	**Frequency**	**%**

Student – Recently admitted (Less than 3 months)	61	22.2
Student – Ongoing (over 3 months)	34	12.4
Student – Awaiting graduation	20	7.3
Training technical college specialist– Executive	22	8.0
Training technical college specialist – Middle level	41	14.9
Training technical college specialist– Entry Level	25	9.1
Other staff – Administration (Finance, HR, Admin, Logistics, Front Office, Training specialist)	18	6.5
Other staff - Permanent	37	13.5
Other staff – Temporary & consultancy	17	6.2
Total	275	100

Collected data was further analyzed using Statistical Package for Social Sciences software version 12 (SPSS 12.0). The author represented the information using descriptive statistics such as percentages and frequencies to identify notably traits of the research variables. The Kruskal – Wallis non-parametric test was done to test the hypothesis. Such tests are most suitable for ordinal, nominal, scale ranked and categorical researches such as this one because they are distribution free, do not ask for normal distribution data and can deal with small samples efficiently.

5. FINDINGS

From the analysis, 74.5% of respondents identified management's positive attitude towards instituting solid and formidable security for their information system. Prevalent security controls highlighted included job rotations (63.3%), personnel policies (73.5%) including background checks, trainings (55%, adequate documentation (54.9%) and mandatory vacations (45.5%). However, 66% of respondents cited unlimited access to private and confidential organization data as a highly probable threat.

Table 2 Krusal Wallis Test Findings Based on Type of Security Control

IS Security Contr	**Hardware**	**Organizational**	**Data**	**Software**	**Offline Data & Progr**	**By Passing**	**Utility**	**User Programming**	**Output**	**Division of duties**

ols					**am**					
Chi – Square Test	14.581	22.498	12.474	14.649	13.109	15.700	12.386	26.644	29.403	31.156
Df	8	8	8	8	8	8	8	8	8	8
Asymp Sig.	0.068	0.04	0.131	0.066	0.108	0.047	0.135	0.001	0.000	0.000

On physical access and hardware security controls 82.5% of respondents identified hazard and theft insurance security measures as present and adequate. Presence of uninterruptible power supply units was also identified as a key security control to ensure uninterrupted power supply and therefore coordinated and smooth running. Still, 79% of respondents certified physical access to computer terminals, computer rooms, high ground clearance and sealed in ducts communication lines to limit tapping, limiting taking hardware outside computer rooms such as modems and network switch gears were adequate security control features (Alhogail & Berri, 2015). However, reported potential security breaches included unbolted to desks computers, unavailable lockable computer covers and unavailable trip alarms and motion detectors.

Most respondents (82.9%) confirmed presence of reputed antivirus software, original software to run programs and policies to curb unauthorized copying of licensed software on computers (Ablushi, 2016). Still, both students and staff reported presence of collaborated and backed up storage in the clouds such as One Drive, Dropbox and Google Drive, allowing accessing to files on the go. Use of user- IDs, access cards and passwords was also confirmed as an adequate security control to limit, allocate and withdraw access to special facilities (Wright & Wright, 2014). For instance, smart students' card limited those who had not met their financial obligations accessing tuition and library blocks until they cleared their tuition balances (Khaddaj, Fares, Joujou, Kabalan, & Kayssi, 2014). Similarly, non – students, visitors and outsides could not access certain areas such as hostels, tuition, library, mesh and workshop facilities such as the garage. Overall, the researcher identified security controls in output, segregation of duties, user programming, utility and bypassing security controls present in technical colleges in Saudi Arabia.

6. CONCLUSION

The researcher through an empirical survey to analyze, examine, evaluate and recommend for information system security revamping in technical colleges in Saudi Arabia. The statistical results identify strongly executed IS security controls, although a number of areas are inadequately implemented. Mandatory vacations, limiting physical access to specified areas, employee, and student training among other controls will provide a near sound proof security system for technical colleges. Establishing trip and motion detectors in strong computer and database rooms is essential. The researcher recommends further research within the Gulf Region to identify potential threats and provide adequate recommendations in future researches.

7. ACKNOWLEDGMENTS

The author is most grateful to Allah for giving the researcher the will, energy, determination and wisdom to accomplish this research. In addition, the researcher is most grateful to Technical and Vocational Training Corporation for their financial support and their encouragement. Moreover, the researcher is most grateful to his parents and family for their support and encouragement.

References

Ahmad.a, A. (2013). Information Security Management System: Emerging Issues and Prospect. IOSR Journal of Computer Engineering, 12(3), 96-102. doi:10.9790/0661-12396102

Abu-Musa, A. A. (2014). Investigating the security controls of CAIS in an emerging economy. Managerial Auditing Journal, 19(2), 272-302. doi:10.1108/02686900410517867

Alhogail, A., & Berri, J. (2015). Enhancing IT security in organizations through knowledge management. 2015 International Conference on Information Technology and E-Services. doi:10.1109/icites.2012.6216677

Ablushi. (2016). Evaluating the Security Controls of CAIS in Developing Countries: The Case of Saudi Arabia. The International Journal of Digital Accounting Research. doi:10.4192/1577-8517-v6_2

Khaddaj, S. I., Fares, D. A., Joujou, M. K., Kabalan, K. Y., & Kayssi, A. (2014). How Best You Can Utilize Your Computer to Tackle Engineering Problems. IJIET International Journal of Information and Education Technology, 4(5), 405-410. doi:10.7763/ijiet.2014.v4.439

K., & K. (2016). Strategic Priorities for Information Technology Program. Retrieved October 2, 2016, from http://admission.kau.edu.sa/GetFile.aspx?id=52768

Pattinson, C. (2015) “The Resource Costs of Network Management” Chapter for Encyclopaedia of Information Communication Technology Eds A Cartelli, M Palma.

Warkentin, Merrill and Xin Luo. (2014). Malware and Anti-Virus Technologies and Procedures,â€• Encyclopedia of Multimedia Technology and Networking, Idea Group Publishing.

WhiteHat. (2015). Website Security Statistics Report 2015. Retrieved October 2, 2016, from https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf

Wright, S., & Wright, A. M. (2014). Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations. Journal of Information Systems, 16(S-1), 99-113. doi:10.2308/jis.2002.16.s-1.99

Wu, L., & Zhang, Y. (2011). Automatic Detection Model of Malware Signature for Anti-virus Cloud Computing. 2011 10th IEEE/ACIS International Conference on Computer and Information Science. doi:10.1109/icis.2011.73