UNIVERSITY STUDENT DATA PRIVACY, SECURITY AND POLICY MANAGEMENT

Mr. Wong Chee Kong[1]*, Assoc. Prof. Ts. Dr. Rajamohan Parthasarathy[2]

Abstract

The issue of data privacy, as well as its security and policy management has received a fair share of media attention since the introduction of the Personal Data Protection Act 2010 (PDPA) in Malaysia. Governments around the world have variously introduced similar laws such as the Australian Privacy Act of 1988, and the European General Data Protection Regulation of 2018. An understudied area in data privacy and security management is the way student data is managed in Malaysian private universities. This study aims to gain an in-depth understanding—within the context of a Malaysian private university—the various challenges of managing personal student data privacy and security; to better understand how student personal data privacy policies and related issues are being addressed within the regulatory requirements of the Personal Data Protection Act; and to propose a wholistic framework to address the management of student data privacy and security in Malaysian private universities given the pervasive presence of the Internet of Things. Through qualitative research methods such as interviews, qualitative content coding and thematic network analysis—this study has arrived at a thematic network map that consists of four organising themes—regulatory compliance, security, risk, and concerns as well as data privacy. We conclude that these four themes of data privacy management in a Malaysian private university would point the way to the next step in the creation of a comprehensive framework to address the management of student data privacy and security in Malaysian private universities.

Keywords: Strategic data management, data privacy, data security, data protection, internet of things (IoT), private university, data policy management, qualitative research

[1]*Research Scholar, Faculty of Engineering, Built Environment and Information Technology, SEGi University, Kota Damansara, Malaysia.
Email: cheekong@wongcheekong.org
[2]Associate Professor, Centre for Network Security and IoT, Faculty of Engineering, Built Environment and Information Technology, SEGi University, Kota Damansara, Malaysia.
Email: prajamohan@segi.edu.my

*Correspondence Author: Mr. Wong Chee Kong
*Faculty of Engineering, Built Environment and IT SEGi University, Malaysia.
Email: cheekong@wongcheekong.org

I. INTRODUCTION

In recent years, the breach of personal data has been a matter of frequent reporting in the international news media [1]. It has also been highlighted in some research that the lack of privacy awareness in Malaysia is worthy of attention [2]. An area that is understudied on the issue of data privacy breaches is the area of student data privacy breaches within the context of Malaysian private higher education institutions. Though not well studied, it is an issue of considerable importance since the Malaysian Government introduced data privacy laws in Malaysia with the implementation of the Personal Data Protection Act 2010 (PDPA) to govern the collection, use, storing and distribution of sensitive personal data [3]. This study intends to bridge this knowledge gap by performing a thematic network analysis on the qualitative data collected through interviews conducted with various business process owners (BPOs) in a Malaysian private university. This qualitative analysis serves as the basis for us to propose a wholistic framework for the improvement of student data privacy and security management.

II. SCOPE OF STUDY

This study is qualitative in nature and therefore the recommendations would be based on the understanding of the various business process owners (BPOs) being interviewed in a private Malaysian university. These BPOs are the university administrators dealing specifically with the collection, processing, retention, protection, and distribution of student personal data. The findings from this study therefore may not apply to contexts of universities that may be more complex or more simplistic in nature.

III. RESEARCH AIMS AND RESEARCH QUESTIONS

This study aims to achieve the following:
1) to gain an in-depth understanding—within the context of a Malaysian private university—the various challenges of managing personal student data privacy and security.
2) to better understand how student personal data privacy policies and related issues are being addressed within the regulatory requirements of the Personal Data Protection Act
3) to propose a wholistic framework to address the management of student data privacy and security in Malaysian private universities given the pervasive presence of the Internet of Things

With the aims above, the following research questions were derived:

1) In the current practice of student personal data collection, processing, storage, dissemination, and elimination, what are the relevant issues?
2) How do staff members ensure data privacy and security when handling students' personal data?
3) How is regulatory compliance addressed within the university?
4) What are the risks involved when dealing with student personal data privacy management, both internal and external?
5) How a wholistic approach to ensure that the students personal data privacy and security is properly managed can be developed, given the environment of the Internet of Things?

IV. SIGNIFICANCE OF STUDY

By addressing the research questions above, this study contributed to a better understanding of the subject of student data privacy, security, and policy management—resulting in a more informed approach towards policy making and the development of a more robust framework in the underlying IT infrastructures. Students' confidence towards the sound management of personal data in a university will also encourage greater transparency in the communication between the university staff members and students. Better compliance towards regulatory standards will also produce side benefits such as better university ranking in league tables and gaining intangible benefits such as enjoying a good reputation.

V. LITERATURE REVIEW

There are past studies in the context of regulatory environments outside of Malaysia that has informed the direction of the current study. These foreign studies indicated how models that have worked in Australia, European Union and Israel can point the way towards regulatory compliance practices within the context of the Malaysian PDPA. While laws may differ from country to country, such as Malaysia having one Act while the UK has two [4]—there are still common good practices that may be applicable globally. One such example is a study that Bandara conducted based on an extended antecedents privacy concerns outcomes (EAPCO) model [5].

The EAPCO model influenced this study in the way it addresses privacy management and considerations using semi-structured qualitative interviews. This model demonstrated that a person's attitudes, perceptions, and beliefs are influenced by sets of privacy concerns antecedents. These antecedents would therefore have an indirect impact on a person's risks/cost versus benefits balance, as well as a person's level of

trust. This model has also shown that a person's behavioural reactions based on privacy concerns can be further strengthened by phycological distance, privacy empowerment, expectations of contracts or conversely; weakened by construal level of privacy, learned helplessness or violations of privacy contracts. This line of logic has influenced the current study in the way the semi-structured questions were drawn up.

According to Muvingi and Mugadza, Zimbabwe is a country that has only recently passed their Data Protection Act on 3rd December 2021 [6]. Pioneers in the field of student data privacy in Zimbabwe, Maguraushe et al. proposed a model to gauge the perception of student privacy at their respective universities and institutions [7]. They named this model the Student Personal Information Privacy Culture (SPIPC) framework. Maguraushe et al. hoped that this model will provide better understanding to developing data privacy framework in universities. The current study utilises Maguraushe's model to surface key issues that may lead to the discovery of emerging themes. Maguraushe outlined key issues that included privacy consent, privacy education,

privacy policy, limitation of data use and collection, information quality and information notice and openness [8].

An aspect in the field of student personal data privacy that has added a dimension of complexity to the current study is the fact that student personal data is frequently used in environments where the Internet of Things (IoT) exists. According to Sadeeq and Zeebaree, IoT in essence is a network formed collectively by smart devices with the ability to inter-exchange and collect data, that may be a combination of tokens, sensors and popular consumer electronics such as smart phones [9]. Issues that are relevant to this type of IoT environment were also explored in detail as to how they would impact the management of data privacy and security in a university.

VI. RESEARCH DESIGN

The current study employed qualitative research methods such as interviews, qualitative content coding and thematic network analysis. The following (see Fig. 1) outlines the design of this research.
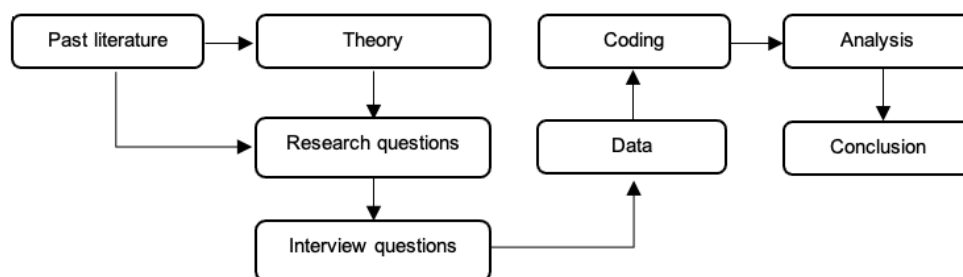

Fig. 1. The current study's flow of research design.

In the design of this research, past literature was used to inform the theories and relevant research questions pertaining to this study. This translated to interview questions that served to gather interview data that can be coded for thematic network analysis. Conclusions that would serve to propose a wholistic framework to address the management of student data privacy and security in Malaysian private universities can then be derived.

VII. PARTICIPANTS SELECTION AND DATA COLLECTION

The participants selected for this study were the business process owners (BPOs) in a Malaysian private university who delt with data collection, processing, and retention, as well as data dissemination and protection in their day-to-day business processes. Being BPOs, they had the say over their individual business processes and were

therefore most familiar with their part of the business process in the university compared with other staff members. They were individually interviewed in their respective offices and the interviews were voice recorded and subsequently transcribed into interview transcripts.

VIII. DATA ANALYSIS AND TRIANGULATION

The interview transcripts with the BPOs were subsequently coded into a code book to arrive at the basic themes. These basic themes were then grouped into emerging organising themes. When the organising themes emerged, a global theme can then be formed. This forms a complete thematic network analysis that can then be use as insight to propose a a wholistic framework to address the management of student data privacy and security. The following (see Fig. 2) shows how this method is used in a visual form.
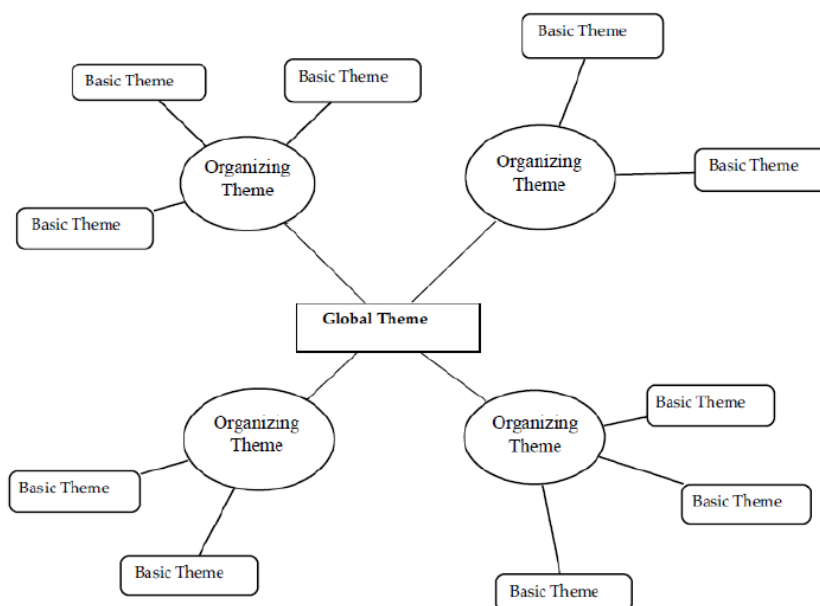
Fig. 2. Visual representation of a thematic network, according to Attride-Stirling [10].

Carter et al. emphasized that the validity of a study is to be achieved via data source triangulation. This type of triangulation was done in this study by ensuring that BPOs across different jobs functions and across departments were being interviewed [11].

Reliability of this study was achieved with the measuring of replicability of results by having different coders going through the same textual input. This technical approach was introduced by Krippendorff and is called the inter-rater reliability testing [12].

IX. FINDINGS FROM THE CURRENT STUDY

The current study as arrived at the following thematic network map (see Fig. 3) after performing a comprehensive thematic network analysis on the coded interview transcript.
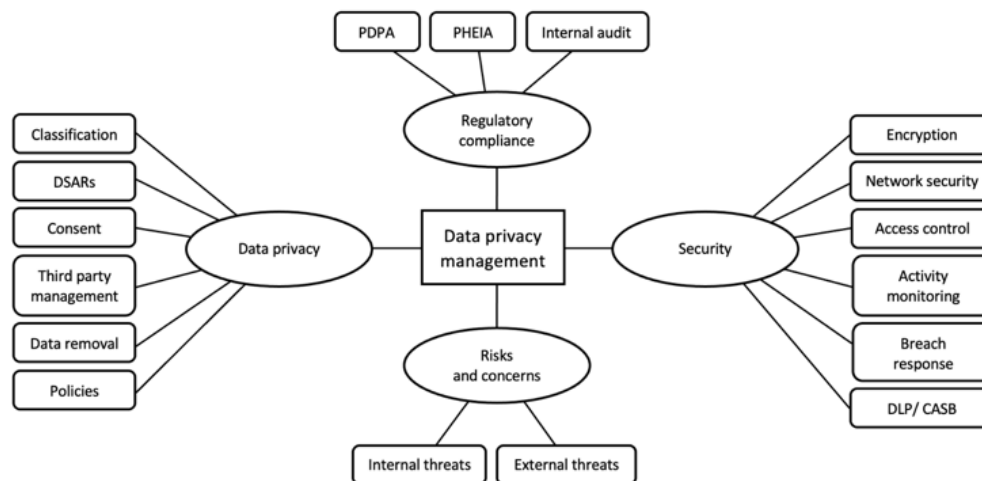

Fig. 3. Thematic network map of the current study.

The global theme that has emerged from the study was *data privacy management*. This global theme was formed after the various basic themes were organised into the four organising themes of *regulatory compliance*, *security*, *risk and concerns* as well as *data privacy*. The basic themes were issues that a comprehensive framework to address data privacy, security and policy management must address. These issues cover broad areas from encryption, network security, access control, activity monitoring, breach response, data loss prevention/cloud access security broker (DLP/CASB), internal and external threats, data classification, data subject access requests (DSARs), consent, third party management, data removal, data and privacy policies; to the Personal Data Protection Act

(PDPA), Private Higher Educational Institutions Act (PHEIA) and internal audit.

X. CONCLUSION

This study has brought to light four key issues of data privacy management in a Malaysian private university, which are—regulatory compliance, security, data privacy, as well as risks and concerns. These important findings would point the way to the next step in the creation of a comprehensive framework to address the management of student data privacy and security in Malaysian private universities wholistically, given the pervasive presence of IoT.

ACKNOWLEDGMENT

REFERENCES

1. V.H.S.E. Robertson, "Excessive data collection: Privacy considerations and abuse of dominance in the era of big data," Common Market Law Review, pp. 161–190, 2020, doi: 10.2139/ssrn.3408971.
2. N. H. Hashim, Y. Kamarulzaman, M. J. M. Hasim, and N. A. A. Rahman, "SEARCH Journal of Media and Communication Research 'Sharenting': A study of Malaysian parents' use of social media platforms," SEARCH Journal of Media and Communication Research, vol. 13, no. 3, pp. 125–140, 2021.
3. Government of Malaysia, "Laws of Malaysia Act 709 - Personal Data Protection Act," Jun. 10, 2010. https://www.kkmm.gov.my/pdf/Personal%20 Data%20Protection%20Act%202010.pdf (accessed Jan. 30, 2023).
4. J. J. Turner and S. P. Amirnuddin, "Social media privacy and the law: Perspectives from Malaysia and UK consumers," SEARCH: The Journal of the South East Asia Research Centre, vol. 10, no. 2, pp. 31–58, 2018.
5. R. Bandara, M. Fernando, and S. Akter, "Explicating the privacy paradox: A qualitative inquiry of online shopping consumers," Journal of Retailing and Consumer Services, vol. 52, no. May, p. 101947, 2020, doi: 10.1016/j.jretconser.2019.101947.
6. Muvingi and Mugadza, "General Overview of the New Data Protection Law in Zimbabwe," Dec. 2021. https://www.mmmlawfirm.co.zw/general-over view-of-the-new-data-protection-law-in-zimba bwe/?utm_source=rss&utm_medium=rss&ut m_campaign=general-overview-of-the-new-data-protection-law-in-zimbabwe (accessed Apr. 11, 2022).
7. K. Maguraushe, A. da Veiga, and N. Martins, "A conceptual framework for a student personal information privacy culture at universities in Zimbabwe," in Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019, 2019, vol. 12, pp. 143–156. doi: 10.29007/wts6.
8. K. Maguraushe, "Development of a diagnostic instrument and privacy model for student personal information privacy perceptions at a Zimbabwean university," Thesis, University of South Africa, 2021. [Online]. Available: http://hdl.handle.net/10500/27557
9. M. A. M. Sadeeq and S. Zeebaree, "Energy Management for Internet of Things via Distributed Systems," Journal of Applied Science and Technology Trends, vol. 2, no. 02, pp. 59–71, Apr. 2021, doi: 10.38094/ jastt20285.
10. J. Attride-Stirling, "Thematic networks: An analytic tool for qualitative research," Qualitative Research, vol. 1, no. 3, pp. 385–405, 2001, doi: 10.1177/1468794101001003 07.
11. N. Carter, D. Bryant-Lukosius, A. Dicenso, J. Blythe, and A. J. Neville, "The use of triangulation in qualitative research," Oncology Nursing Forum, vol. 41, no. 5. Oncology Nursing Society, pp. 545–547, Sep. 01, 2014. doi: 10.1188/14.ONF.545-547.
12. K. H. Krippendorff, Content Analysis: An Introduction to Its Methodology. Sage Publications, Inc., 2003.