

SAMRC InfoSpace

Tomorrow's privacy: Information security at South African universities— implications for biomedical research

Item Type	Article
Authors	Anderson, D.;Abiodun, O.P.;Christoffels, A.
Citation	Anderson D, Abiodun P.O, Christoffels A. Tomorrow's privacy: Information security at South African universities—implications for biomedical research. International Data Privacy Law. 2020 May,10(2);180-186. doi.org/10.1093/idpl/ipaa007
DOI	10.1093/idpl/ipaa007
Publisher	Oxford University Press
Journal	International Data Privacy Law
Rights	Attribution 3.0 United States
Download date	2026-04-22 20:31:40
Item License	http://creativecommons.org/licenses/by/3.0/us/
Link to Item	https://academic.oup.com/idpl/article/10/2/180/5847957?login=true

Comment and Analysis

Tomorrow's privacy: information security at South African universities—implications for biomedical research

Dominique Anderson*, Oluwafemi Peter Abiodun* and Alan Christoffels*

Key Points

- In South Africa, a similar regulation strategy to the European Union General Data Protection Regulation, called the Protection of Personal Information Act (No 4 of 2013) (POPIA), will be implemented, with a view to mitigate cybercrime and information security vulnerabilities.
- A qualitative exploratory analysis of information security management at universities in South Africa, using a Technology, Organisation, and Environment model, highlights the need for maintaining the security infrastructure to facilitate management of security within the university network, while placing emphasis on information security management processes, such as risk analysis, architecture review, code inspection, and security testing.

- Organizational factors were the most critical factors when compared to the technological and environmental factors which appear to influence the effectiveness of information security measures and, subsequently, data regulation readiness.
- Universities will have to balance the implementation of tangible solutions to mitigate risks within the scope of their budget while promoting user compliance, despite perceived 'restrictions.'
- For biomedical researchers, questions remain on the impact of POPIA legislation on data sharing, open science, and collaborations.

Introduction

Information has become a common and valuable commodity, with increased attention being focused on how information is handled, stored, and distributed.¹ The role of universities as generators of knowledge

underscores the importance of information management through the data life cycle from generation, processing, analysis, access, and reuse. Comprehensive information and communication technology (ICT) frameworks exist, such as COBIT 5 and ISO27001, and are aligned to King IVTM for ICT governance, Prince2 for project management, and the NIST security framework.² Universities in general and particularly in South Africa, adopt these at different levels. A researcher or academic is one of the stakeholders in a university that

* South African Medical Research Council Bioinformatics Unit, South African National Bioinformatics Institute, University of the Western Cape, Bellville, South Africa. Email: alan@sanbi.ac.za. This study was funded by SA Medical Research Council and the South African Research Chairs Initiative of the Department of Science and Innovation and National Research Foundation of South Africa, award number UID 64751. The authors wish to thank the participants of this study for their valuable contribution to this work. This study was approved by the Research Ethics Committee of the University of the Western Cape with Ethics Reference Number: BM18/7/11. The authors declare that there is no conflict of interest concerning the publication of this article.

1 Ify E Aguilu, 'Accessibility of Information: A Myth for Developing Countries?' [1997] 98(1) *New Library World* 25, 29; Yulia Cherdantseva

and Jeremy Hilton, 'Information Security and Information Assurance' [2015] *Standards and Standardization* 167–98. doi: 10.4018/978-1-4666-4526-4.ch010.

2 NIST, 'Cybersecurity Framework' (2016) <<https://www.nist.gov/industry-impacts/cybersecurity-framework>> accessed 22 January 2020; Graham Croock, 'The Implications of IT Governance Outlined in King IVTM - Report - Insights - BDO' (2016) <<https://www.bdo.co.za/en-za/insights/2016/report/the-implications-of-it-governance-outlined-in-king-iv>> accessed 22 January 2020; Mary Lewinson, 'PRINCE2 Methodology Overview: History, Definition & Meaning, Benefits, Certification' (*PM Framework*, 2011) <<https://mymanagementguide.com/prince2-methodology-overview-history-definition-meaning-benefits-certification/>> accessed 22 January 2020.

would encounter these data-relevant policies at the level of a 'user', and the management of personal information of research participants is of direct relevance to biomedical researchers.

The Protection of Personal Information Act (No 4 of 2013) (POPIA) was signed into law on 19 November 2013 and at the time that interviews were conducted in this study, the implementation date was not yet known.³ Earlier this year, the office of the Information Regulator (IR) approached the President of SA requesting that 1 April 2020 be the declared date on which the remaining provisions of POPIA commence. Following this implementation date, a one-year grace period will be provided, and organizations would have to be POPIA-compliant by 31 March 2021.

In accordance with sections 40 and 65 of the POPIA, the IR is required to assist with development and approval of codes of conduct.⁴ These codes of conduct operate as additional requirements for POPIA and as such, do not limit the right to privacy of a data subject, which is outlined in the POPIA. The purpose of the code of conduct is to provide a mechanism for compliance and accountability, which is tailor-made to various sectors. However, any code of conduct, which has been developed, must still be approved by the IR to ensure that the requirements of Chapter 7 of the Act have been met.⁵ In 2018, Universities South Africa, a membership organization which represents public universities in South Africa, launched a project to draft a code of conduct for public universities. A task team of representatives from public universities in South Africa and an external expert were constituted and produced the first draft of the code of conduct which was distributed in May 2019 to the South African universities for comment. Once the code of conduct is approved by the IR, it will be legally binding and apply to the processing of personal information by all 'public higher education institutions' as defined in section 1 of the Higher Education Act 101 of 1997.⁶ As we await the outcome of this national consultative process, it is important to understand the factors that govern data security and how it impacts the implementation strategies of any national policy framework.

While South African universities are coming to terms with the need to establish effective governance of information security due to the external forces on the

institutional environment from data regulatory agencies, understanding the placement of security in an academic context remains problematic. Therefore, there exists an urgent need for improvement in the way data and information are collected, stored, and disseminated within university systems, and with greater reference to sensitive information and data. Security measures and policies must be in place to guarantee the integrity, confidentiality, and availability of information. To achieve this, technological, organizational, and environmental factors must be investigated without undervaluing any factor. Therefore, the research has used the Technology, Organisation and Environment (TOE) framework to investigate and analyse factors influencing the effectiveness of information security policies and compliance in the participating universities.

In order to assess whether SA universities had proper and reliable information security measures, practices, policies, and management in place, a TOE framework was applied to three SA universities. The analysis allowed for the identification of existing gaps within the university IT domain to provide a point of departure for further research, to develop comprehensive policies for information security at tertiary institutions, in line with POPIA compliance.

POPIA as a legal data protection framework

The POPIA is the South African data protection law, promulgated on 26 November 2013, with the aim of protecting identifiable personal information of natural persons, and juristic persons from malicious intent in accordance with privacy rights determined by section 14 of the Constitution of the Republic of South Africa (Act No 108 of 1996).⁷ The POPIA rests upon the establishment of a set of data protection standards to specify the satisfactory collection, handling, and utilization of data.⁸ The South African POPIA covers aspects that incorporates: legal or lawful processing of the personal information traversing South Africa, accountability, processing limitation, purpose specification, retention and restriction of records, information quality, security safeguards, data subject participation, transfer of personal information across national boundaries, and codes of conduct.⁹ Non-compliance with the directives

3 SAICA, 'Protection of Personal Information Act' (2016) <<https://www.pwc.co.za/en/services/advisory/pop.html>> accessed 16 July 2018.

4 Republic of South Africa, 'Protection of Personal Information, Act 4 of 2013' (Government Gazette 1 2013) <<https://www.gov.za/documents/protection-personal-information-act>> accessed 5 May 2020.

5 *ibid.*

6 Republic of South Africa, *Higher Education Act 101 of 1997* [1997].

7 John Hatchard, 'The Constitution of the Republic of South Africa' [1994] 38 *Journal of African Law* 70.

8 J. Eric Davies, 'Studies in Technical and Social Influences on Information and Library Management' <<https://hdl.handle.net/2134/32811>> accessed 27 February 2020.

9 SAICA (n 3).

of POPIA may result in the IR imposing fines of up to ZAR10 million, depending on circumstances.¹⁰

POPIA is derived from a version of the General Data Protection Regulation (GDPR) of the European Union (EU) and both regulations address the protection of personal information of residents from unauthorized access; however, there are differences between them.¹¹ The GDPR has gone through several versions of review and modification, expanding applicability to real-world problems. POPIA derived some concepts of earlier iterations of the GDPR and as such, POPIA compliance does not necessarily indicate GDPR compliance. In practical terms, and considering that Europe is South Africa's predominant trade partner, GDPR non-compliance could have a negative impact on scholarly and global research partnerships and coupled with the possibility of fines (the upper limit of which is 20 million euro, or 4 per cent of global turnover) the financial implications of non-compliance would be disastrous for South African Universities.¹²

TOE framework analysis

Recent research has recognized that technological factors are not the only key to effective information security controls; there is also a need to understand the impact of human and organizational factors.¹³ A better understanding of how different factors such as technological, organizational, and environmental factors influence the implementation and effectiveness of information security policies and compliance is essential, as this may elucidate how different factors could lead to potential sources of security breaches and vulnerabilities within organizations.¹⁴ A TOE IT/IS adoption framework that was developed by Tornatsky &

Fleischer based on assumption that IT/IS adoption in organizations is influenced by three elements—technology, organization, and environment—was used in a small comparative case study based on findings from interviews with ICT professionals from three SA universities.¹⁵

Study methodology

The TOE framework is a recognized adoption framework in the information systems field with several researchers having employed this framework in studies. For this qualitative research study, a questionnaire was designed using concepts of the TOE framework as a basis to guide semi-structured interviews. The purposeful sampling design used for this study in order to select participants in accordance with the research objectives.¹⁶ Purposeful sampling ensures that the study population delivers adequate information needed for the study, and research by Baskarada surmised that with purposeful sampling, three individual participants would be sufficient to provide reliable, adequate, and valuable data that are appropriate for a study, thereby negating a reliance on a large sample set.¹⁷ While the current study involved one respondent from each university who participated in the semi-structured interviews, the participants have a high level of expertise and are involved in all day-to-day functional activities within the IT/IS domains at the universities.

Only consenting participants were interviewed. Interviews were digitally recorded and transcribed by two individuals in the research team to ensure accuracy. The transcribed interviews produced over 29,000 words of text, responses were grouped and coded, and themes were formulized to facilitate a rich data set for analysis. Interview text was analysed with ATLAS.ti and the

10 Republic of South Africa (n 4).

11 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119/1.

12 Nkholodzeni Sidney Netshakuma, 'Assessment of a South Africa National Consultative Workshop on the Protection of Personal Information Act (POPIA)' [2019] Global Knowledge, Memory and Communication.

13 Rayford B Vaughn Jr, Ronda Henning, Kevin Foxb, 'An Empirical Study of Industrial Security-Engineering Practices' [2002] 61 Journal of Systems and Software 225; David Botta and others, 'Towards Understanding IT Security Professionals and Their Tools' [2007] *Proceedings of the 3rd Symposium on Usable Privacy and Security* 100–11. <https://doi.org/10.1145/1280680.1280693>; Konstantin Beznosov and Olga Beznosova, 'On the Imbalance of the Security Problem Space and Its Expected Consequences' [2007] 15 Information Management and Computer Security 420.

14 Liene Kreicberga, 'Internal Threat to Information Security - Countermeasures and Human Factor within SME' (2010) <[http://www.](http://www.diva-portal.org/smash/record.jsf?pid=diva2:1019129)

[diva-portal.org/smash/record.jsf?pid=diva2:1019129](http://www.diva-portal.org/smash/record.jsf?pid=diva2:1019129)> accessed 21 June 2018.

15 Edward WN Bernoider and Patrick Schmöller, 'A Technological, Organisational, and Environmental Analysis of Decision Making Methodologies and Satisfaction in the Context of IT Induced Business Transformations' [2013] 224 European Journal of Operational Research 141; Luis F Luna-Reyes and J. Ramon Gil-Garcia, 'Understanding the Co-Evolution of Institutions, Technology, and Organizations: The Enactment of the State Government Portal of Puebla' [2013] The Proceedings of the 14th Annual Conference on Digital Government Research, 214; Hsin-Pin Fu and Hsiang-Ting Su, 'A Framework for a Technology-Organization-Environment Implementation Model in Taiwan's Traditional Retail Supermarkets' [2014] 6(3) International Journal of Organizational 121–29; Osdan Jokonya, 'A Framework to Assist Organisations with Information Technology Adoption Governance' (Thesis, 2014) <<https://pdfs.semanticscholar.org/749f/7a0fbeda39e5277a7182bf52b6dad08bb663.pdf>> accessed 21 June 2019

16 Saša Baškarada, 'Qualitative Case Study Guidelines' (2014) 19 *The Qualitative Report* 1; Robert K Yin, 'Validity and Generalization in Future Case Study Evaluations' [2013] 19 SAGE Journals 321.

17 John H Maindonald, *Qualitative Research from Start to Finish* by Robert K. Yin (Blackwell Publishing Ltd 2011); see also Baškarada, *ibid*.

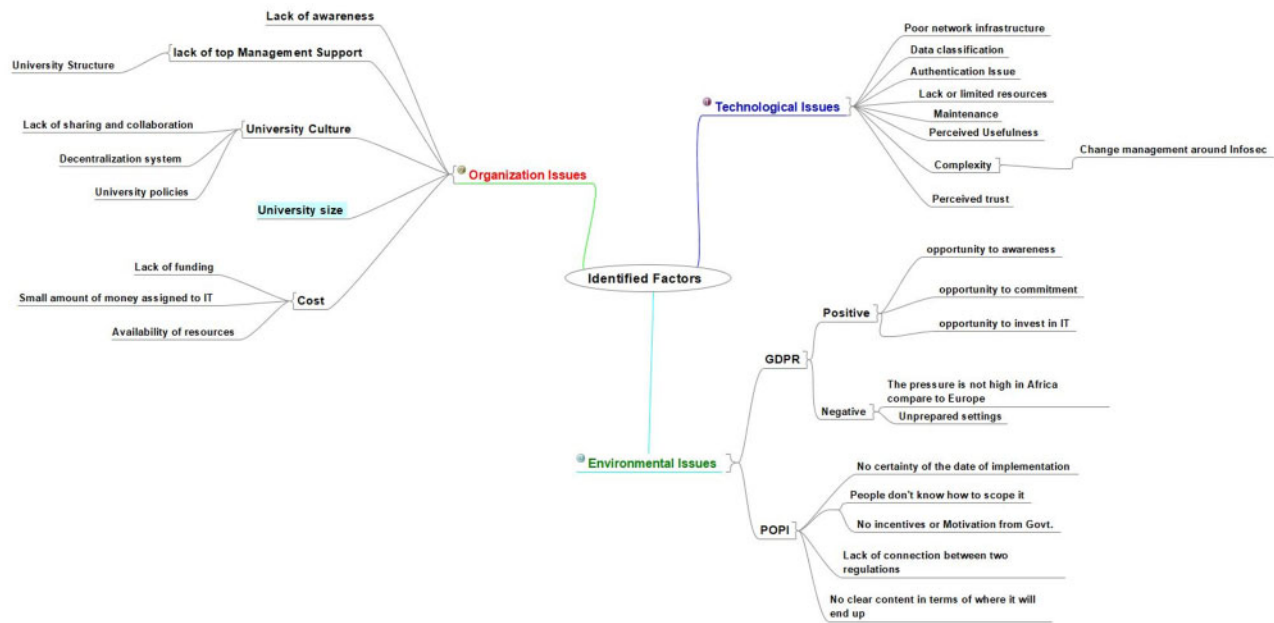


Figure 1: Graphic illustration of a common identified trait from responses of the respondents (all the participated universities)

graphical representation of data was performed using the Freeplane application.¹⁸ To maintain agreed confidentiality with the participant institutions, the three universities were labelled A–C.

Below, the issues which occurred in common at the three participating universities are presented (Figure 1).

Technology factors

The major concern highlighted by two of the three participants under technological factors relates to poor security infrastructure at their institution. The focus of security infrastructure relates to the ability to best use new or existing technological solutions to monitor security processes such as authorization mechanisms, system patching, firewalls, and anti-virus software. At the time of the interviews, participants indicated that both the application and network patches were not in good standing. Some of the factors identified by the respondents which contributed to this included: network patches not being updated as they ought to be, authentication challenges, complexity of the systems, poor data management, lack of classification mechanism, lack of adequate budget to acquire needed tools, staff, and mechanisms to perform routine maintenance. With regards to data classification, the authors suggest that the first practical solution required is the development

of a universally applied data classification scheme with special personal information having a separate and defined classification. All data types cannot be given the same level of data encryption, due to the cost and risk (a successful breach attempt on one database exposes the encryption key of other databases). Applying the same encryption to biomedical data and other sensitive data such as study participant metadata, as is applied to financial records, for example, is not acceptable practice.

The results from the study highlighted the value of maintaining the security infrastructure as it facilitates the management of security within the university network. Tools such as firewalls, encryption mechanisms, authentication mechanisms, and non-repudiation mechanisms are essential for a university system. Security measures must be taken to ensure that data quality and integrity and these measures must be continuously checked for consistency and proper functionality. In order to achieve this, the authors highlight the need to place increased emphasis on the information security management processes such as risk analysis, architecture review, code inspection, and security testing. In addition, the above processes need to be monitored on a regular basis, as malfunction of these tools can lead to failure of effective security management and drive up costs associated with Information Technology, which

18 Atlas.ti, 'Qualitative Data Analysis & Research Software' (2015) <<https://atlasti.com/qualitative-analysis-data/>> accessed 7 June 2019; see

also Freeplane, 'Freeplane/Freeplane' (2018) <<https://github.com/freeplane/freeplane>> accessed 7 June 2019.

will negatively influence compliance to information security practices.

Digital transformation in the university environment has seen a shift in Bring Your Own Device (BYOD) to Bring Your Own Everything (BYOE).¹⁹ All respondents in the study eluded to BYOD policy on IT capacity and security with one respondent speaking to the fact that, on average, a student may own between three to four internet-enabled devices, each of which can be connected to the university network at any time. It is predicted that the number of connected devices on campus networks will continue to increase each year, as smartphones, laptops, tablets, and wearable devices become ubiquitous in daily life.²⁰ BYOD policy not only burdens IT teams in the areas of authentication, explosive bandwidth consumption, access control, and university server security, but also in terms of protection of information. In addition, interviewees made mention of IT risk associated with mobile computational devices. Users often switch between devices for work purposes and commonly make use of hardware elements, such as external drives, to transfer data, including sensitive data. Users frequently travel externally with these devices, increasing information security risk through physical theft and data corruption when connected to untrusted networks. There is, therefore, a need to provide tangible solutions to mitigate this externally driven risk, and this may involve imposing a level of control on users—which would undoubtedly be perceived by users as ‘too restrictive’.

From responses in the interviews, it was noted that formalized data management policy and strategy was lacking, and this had negative implications not only on internal compliance but also on legislative compliance. It is the authors’ strong suggestion that for successful data security implementation and maintenance, management structures should equip the IT teams with the necessary tools and mechanisms to overcome the challenges faced on a daily basis. This can, however, only be achieved if management starts to perceive security and privacy issues as a universal problem and understands the true (though mostly indirect) benefits of prioritizing information security. As such, the addition of security and related IT issues to the institutions’ core function and mandates will enable IT teams to deliver the needed technical support and insight, aligned with mission and

vision of the university and leading to a successful digital transformation journey.

Organization factors

Organizational factors define the influential factors that contribute to the success or failure of information security according to the users. Findings from the analysis of interview responses in the current study showed that organizational factors were the most critical, when compared to the technological and environmental contexts examined. Some of the major issues highlighted by respondents within the organizational context include: lack of top management support, funding, or financial constraints; lack of effective awareness training, information security practices not being part of the management core priority functions; lack of coordinated functions among units and departments; long approval times for IT policies by the councils, decentralization of systems, staff behaviour, and perception towards information security processes; lack of competent staff as a result of limited resources, IT directors and managers not being a part of university decision-making bodies; and difficulties in quantifying return of investment for information security spending.

Respondents additionally spoke to the substantial contribution and impact of human error to the information vulnerabilities or threats, which occurred in organizations. These human error events may be due to negligence or a lack of awareness. Vulnerabilities or breaches occur not because security is difficult, but rather because people *think* security is not difficult. A lack of knowledge on information security has also been identified as the greatest threat to information security in other studies and human behaviour was again identified in the current study.²¹ The authors recommend that universities should implement consistent user awareness training which should address issues such as recognizing phishing scams, email hygiene, password hygiene, Internet usage best practices, security practices (eg locking of PCs or laptops when unused), and drive awareness of existing information security legislation. In addition, security should not be perceived as simply an IT problem but rather as a social problem. If this can be achieved, then the decision makers will possess the knowledge to add information security to their core functions as an issue, which must be addressed.

19 Joanna Lyn Grama and Kim Milford, ‘Ahead of the Curve: IoT Security, Privacy, and Policy in Higher Ed’ in *Women Securing the Future with TIPPSS for IoT* [2019] <http://link.springer.com/10.1007/978-3-030-15705-0_5> accessed 25 May 2019.

20 SevOne, ‘5 Top IT Challenges in High Education SevOne’ [2018] <<https://www.sevone.com/white-paper/5-top-it-challenges-high-education>> accessed 25 May 2019.

21 ME Thomson and Rossouw Von Solms, ‘Information Security Awareness: Educating Your Users Effectively’ [1998] 6 *Information Management and Computer Security* 167; Johan F Van Niekerk and Rossouw Von Solms, ‘Information Security Culture: A Management Perspective’ [2010] 29 *Computers and Security* 476.

Interestingly, one of the participants had identified additional challenges with regards to human behaviour. The IT team at this facility has been less pre-occupied with substantial financial constraints, thereby allowing them to gain insight into other risks to policy implementation and compliance. The authors observe that if the financial issues at the other two universities were resolved, there is a high possibility that they would experience similar problems brought about by human behaviour. This presents a unique opportunity for the universities to discuss shared experiences and for those who are less well resourced to learn from advancements and knowledge gained by well-resourced facilities. Solutions to information security challenges could be developed by collaborative efforts at these facilities, where teams gain insight from each other and collectively identify future risks which may not currently exist.

Lastly, the authors recognize the need for security professionals to present security issues to the management in a language they will understand (in form of business-oriented metrics and not in technical, operational metrics). To this end, it may be beneficial for non-IT managers and executives to participate in basic IT courses in order to better understand the technical jargon used in the information security sphere. In information security, communication is key, and effective communication of the implications of poor IT strategies would be a motivation for high-level structures to ensure that this area is prioritized.

Environmental factors

Environmental factors measure how pressures of international and national standards and government regulations impact security implementation, and examine the audit, security policies, and standards imposed to manage information security in a proper and acceptable way.

With regards to POPIA, information management is not outlined in the Act itself but must be implemented for compliance. At the time of the interviews, there was still no certainty on the date of implementation of POPIA and it appeared that there was no external pressure from government. Participants in the study made mention to how the early stage of adoption and a lack of policy context had resulted in a lack of understanding of how to frame POPIA inception. Furthermore,

respondents highlighted that no incentive or motivation from the government existed to encourage its adoption, leaving organizations at a loss as to how to fund the interventions required for compliance. The authors reiterate that the cost of compliance will differ greatly from one institution to another and have identified this financial burden as a key issue that is already preventing the implementation of basic information security measures and may result in low prioritization of POPIA compliance.

Responses from participants demonstrate a general lack of practical regulatory guidance and training from POPIA IR and government, which may lead to poor implementation and unenforceable security controls. Moreover, since there are inadequate training and awareness from the law enforcement and judiciary fraternity, respondents felt that fining of this regulation would be near impossible. We conclude that POPIA might not be taken seriously until such time that non-compliance is 'punished' and that on the part of the IR, more effort needs to be focused on engagement with all stakeholders. The authors believe that this engagement would be mutually beneficial in that universities would be able to obtain greater clarity on requirements for compliance, and raise practical concerns related to the current format of the legislation and drafted codes of conduct. In this study, it was noted that participants appeared to be more familiarized with the GDPR than with POPIA, which may be due to the intense public exposure to the European legislation. It is the opinion of the authors that harnessing a multitude of platforms to increase awareness of the POPIA regulation may serve to highlight the need to enhance security measures by individuals, universities, and organizations in South Africa.

Interviewed participants highlighted that an organization's compliance to GDPR would make compliance to POPIA easier but not vice versa. This is a challenge to organizations in South Africa, considering the perceived need to comply with both regulations. At this point, institutes that have or intend to include distance learning programmes as part of the educational offering may prioritize one framework over another. One participant suggested that the South African government needs to take a similar approach to these regulations as Japan has, with the EU. These two entities settled on a cooperative agreement that allows the Japan policy privacy legislation to be recognized as equivalent to the GDPR.²² If

22 European Union, 'Official Journal of the European Union L 107' [2015] 22 (ISSN 1977-0677) Publications Office of the European Union <<https://op.europa.eu/en/publication-detail/-/publication/903df42b-eb14-11e4-892c-01aa75ed71a1/language-en>> accessed 17 October 2019; C Wigand and S Soumullion, 'Joint Statement by Haruhi Kumazawa,

Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission' (*Statement*, 2018) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_4548> accessed 7 June 2019; Ulrich Kirchhoff and Tobias Schiebe,

a similar concession can be proposed for POPIA, the operational effort required for compliance would be decreased and the adoption rate among universities and other organizations could increase. In conclusion, the authors identify that the first step which must be undertaken by university IT/IS departments to comply with the requirements of POPIA is to communicate the business value of information to all stakeholders. Understanding this may result in all users becoming more aware of sensitivities, risks, and responsibilities when handling, storing, processing, and distributing data during their day-to-day activities. In addition, this would also demonstrate the value of prioritizing information security and data management compliance to decision-making executives of the university, thereby changing the perception that funding in this sector is simply a 'grudge spend'.

Concluding remarks

Recent research has recognized that technological factors are not the only key to effective information security controls, there exists an additional need to evaluate the impact of human and organizational factors.²³ Universities are becoming more dependent on their networks and information infrastructure than ever before and as this dependence grows, so too, does the strategic importance of their IT teams. Information security is not solely a technical issue and technical controls can only be effective if end users adhere to policy control. Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them.²⁴ It is of paramount importance for university

management and IT departments to collaborate efficiently and effectively to provide solutions that not only solve current needs but also future proof the institutions as the technology age continues its rapid evolution. In accordance with data security policy, universities must safeguard personal information from data breaches, using both technological and organizational measures. POPIA compliance will require that universities develop and implement policies and procedures, clearly define roles and responsibilities, and introduce focused training while considering the information security and management standards. A better understanding of how different factors such as technological, organizational, and environmental factors influence the implementation and effectiveness of information security policies and compliance at tertiary education institutions is invaluable, as it sheds light on the current, and real-world, challenges being faced by these facilities. The effort required to identify and implement practical solutions for basic data collections can be exponentially amplified when dealing with biomedical data collections. Without first identifying and addressing how these critical issues impact the entirety of the data collection, institutions of higher learning are left with minimal resources to navigate complexities associated with the POPIA regulation. Finally, the authors suggest that future studies conducted in this area should include evidence-based research on the impact of POPIA with regards to the use of biomedical data in universities. These studies should be undertaken in order to properly measure POPIA's impact, adequacy, and operation in practice.

doi:10.1093/idpl/ipaa007

'The Reform of the Japanese Act on Protection of Personal Information From the Practitioner's Perspective' [2017] 22(44) *Journal of Japanese Law* <<https://www.zjapanr.de/index.php/zjapanr/article/view/1178>> accessed 25 May 2019.

23 Vaughn, Henning, Foxb (n 13); David Botta and others, 'Towards Understanding IT Security Professionals and Their Tools' [2007]

Proceedings of the 3rd Symposium on Usable Privacy and Security 100–11. <https://doi.org/10.1145/1280680.1280693>.

24 Johan van Niekerk and Rossouw von Solms, 'A Holistic Framework for the Fostering of an Information Security Sub-culture in Organizations' [Information Security South Africa Conference (ISSA), 2005] Pretoria, South Africa.