

Abstract

Exploring the Influence of Organizational, Environmental, and Technological Factors on Information Security Policies and Compliance at South African Higher Education Institutions, with a Focus on Implications for Biomedical Research †

Oluwafemi Peter Abiodun, Dominique Anderson and Alan Christoffels *

South African Medical Research Council Bioinformatics Unit, South African National Bioinformatics Institute, University of the Western Cape, Bellville 7535, South Africa; 3614275@myuwc.ac.za (O.P.A.); dominique@sanbi.ac.za (D.A.)

* Correspondence: alan@sanbi.ac.za; Tel.: +27219593645

† Presented at the 5th African Conference on Emerging Infectious Diseases and Biosecurity, Abuja, Nigeria, 7–9 August 2019.

Published: 10 March 2020

Abstract: Globally, concerns over information security vulnerabilities are growing exponentially, fuelled by several headline reports of data breach incidents, which increase in size with each occurrence. On the Africa continent, South Africa is ranked among the most ‘at-risk’ countries for information security vulnerabilities, having lost approximately fifty billion rands to cybercrime in 2014. South Africa is currently considered to be the most cybercrime-targeted country in Africa. Worldwide, cyber vulnerability incidents greatly affect the education sector, due to the fact that this sector holds more Personal Identifiable Information (PII) than many other sectors. The PII ranges from (but is not limited to) ID numbers and financial account numbers to biomedical research data. In response to growing threats in South Africa, a similar regulation strategy to the European Union General Data Protection Regulation (GDPR), called the Protection of Personal Information Act (POPIA) will be implemented, with a view to mitigating cybercrime and information security vulnerabilities. The extent to which African institutions, and specifically the South African universities, have embraced and respond to these two information security regulations (GDPR and POPIA) is not yet clear and will be a matter of great importance for biomedical researchers. This research study aims to conduct a qualitative exploratory analysis of information security management across three universities in South Africa, by using a Technology, Organizational, and Environmental (TOE) model to investigate the factors which may influence the effectiveness of information security measures. This study is poised to make a significant contribution to the development of a Management Model for security practitioners and a framework for information management of biomedical data.

Keywords: biomedical data; GDPR; information security and management; South African universities; TOE framework; POPIA



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).