Chapter 13
Cybersecurity Management in South African Universities

Nkholedzeni Sidney Netshakhuma
https://orcid.org/0000-0003-0673-7137
University of Mpumalanga, South Africa

ABSTRACT

The study aimed to assess cyber security at South African universities. The researcher will use literature to assess the state of cybersecurity at South African universities. The results from the literature review revealed poor implementation and adherence of cyber security strategy and standards by employees and students; poor cyber security awareness relative to information communication technology (ICT) infrastructures and assets; and lack of strategy and framework to implement cyber security management. The study recommends continuous monitoring and evaluation of information management systems at various South African universities with the view to assess the state. A replica of the study may be studied in other part of the world.

INTRODUCTION

The study assessed the cyber security threats such as security of information faced by South African universities from 1994 until present. The security breach was caused by ineffectice cybersecurity policies, lack of cybersecurity management training and awareness, lack of information communication technology and ineffective infrastructure. The significance of cybersecurity in modern societies is undisputed. Numerous studies in diverse fields such as information communication technology, finance management, risk management, records, and archives management, and security management add value to cybersecurity management. This shows a relationship between cybersecurity and other disciplines. In this chapter, the term South Africa university was used interchangeably with the Higher Education Institution of South Africa.

DOI: 10.4018/978-1-6684-5827-3.ch013

The researcher used the case study of the South African universities to assessed the state of cybersecurity. The results from the literature review revealed ineffective development of cyber security policy by staff. Furthermore, students were not aware of the risk posed by a hacker in their internet environment. This study recommends organizations develop a cyber security management system. The study recommends universities develop a framework in compliance with national legislation.

BACKGROUND

Cybersecurity occurs as a form of hackers attacking business information in an electronic environment (Borgman, 2018; Moskai, 2015, p. 97; Villegas-Ch, Garges, Viteri 2021). Hackers accessed the organization's remote server to damage electronic contents management systems which store data in the networked and the physical infrastructure (Kundy & Lyimo, 2019). To prevent hacking, the security breaches requires organizations to enhance security systems by ensuring that a governance structure or committee was established to execute the oversight role over security management compliance. Executive management of the institutions were responsible to establish such committee. An organization developed systems and processes to ensure that measures were in place to control access to networked systems and the information contained. Cybersecurity threats required to be protected by various organizations all over the world.

Security of information was identified as one of the risks in the strategic or operational risk registers of universities (Abdulrauf & Fombad, 2017, p. 106). As a preventive measurement, universities developed an action plan to counter the threat posed by hackers. The effective way to implement an action plan was to facilitate cybersecurity workshops, and develop processes and procedures to comply with Legislation such as *the Protection of Personal Information Act no. 4 of 2013 (POPIA)* and *the Promotion of Access to Information of 2002 (PAIA)*.These legislations advocate for the protection of personal information. This implied that organisations should regularly clear content that was no longer active, such as data relating to a university program, and develop a data privacy breach management process, Universities should develop a cyber security policy to protect its data from attack. The policy should be developed in compliance with the above mentioned legislations. Process and procedure were to aligned with the organization's requirements. The retention schedule should be embedded in the university system, develop backup and restoration policies and procedures., provide user access management policies and procedures, and provide IT security policy. Protection of information applies to all employees and university stakeholders.

Higher education institutions in South Africa adopted content management systems to aid in teaching, learning, and research. Hackers used the internet to tackle their systems. Universities are not supposed to work in isolation with other universities on system sharing (Olatunbosun, Edwards, and Martineau, 2018, p. 07).

PROBLEM STATEMENT

In compliance with the PAIA and POPIA, universities were to balance access and protection of information lawfully. Furthermore, they were to champion the protection of personal information of data subjects. This so because South African universities were confronted with security threats to their information