Chapter 12
A Human-Centric Cybersecurity Framework for Ensuring Cybersecurity Readiness in Universities

Blessing Gavaza
Africa University, Zimbabwe

Agripah Kandiero
https://orcid.org/0000-0001-8201-864X
Africa University, Zimbabwe

Chipo Katsande
Manicaland State University of Applied Sciences, Zimbabwe

ABSTRACT

The escalating number of cyberattacks on universities worldwide resulted in universities losing valuable information assets leading to disruption of operations and loss of reputation. The research sought to explore a framework for human-factor vulnerabilities related to cybersecurity knowledge and skills, which enabled cybercriminals to manipulate human elements into inadvertently conveying access to critical information assets through social engineering attacks. Descriptive and inferential statistics were used to test the data, and Pearson's correlation statistics were used to measure the statistical relationships and association of variables. The results revealed that students and staff are vulnerable to social engineering attacks and their ability to protect themselves and other information assets is limited mainly due to poor cybersecurity knowledge and skills resulting from poor cybersecurity awareness and education.

DOI: 10.4018/978-1-6684-9018-1.ch012

INTRODUCTION

For all organisations that are committed to the fourth industrial revolution paradigm, Cybersecurity risks pose a complex challenge. (Lezzi, Lazoi, & Corallo, 2018). It is therefore important for Universities and academic institutions around the world to be diligent against these cyber-risks as they have been lucrative victims of cyber-attacks in recent years with several high-profile incidents. Cybercriminals can manipulate unaware humans by exploiting human factored vulnerabilities and involving them to contribute to such offenses.

Universities manage large amounts of valuable research and sensitive personal data, financial information and manage infrastructure resources such as servers, bandwidth capacity, and hosting making up a rich network of critical information assets (Ulven & Wangen, 2021) making universities an attractive target for cybercriminals, espionage, and hacktivists. These critical assets are available to both students and staff to facilitate teaching, learning, and administrative work. The free flow of the workforce and annual rotations of new students, employees, and guests creates security challenges in protecting the information assets and their different users whilst balancing these security measures with the academic openness and free flow of information that universities are trying to promote.

These cybercrime statistics and examples of cyber-attacks on universities around the world are the basis for this research and the development of a human-centric cybersecurity framework to deter potential cybercriminals from successfully attacking universities by exploiting the human vulnerabilities of students and staff. Cybersecurity frameworks help minimise the danger of harmful cyberattacks on applications, computers, and infrastructure, cybersecurity protects computer networks and the information they contain from intrusion and malicious harm or interruption (Craigen, Diakun-thibault, & Purse, 2014).

However, this research also adds humans as an asset that also needs to be protected from intruders with malicious intent. This research proposes a human-centric cybersecurity framework which is a collection of the necessary knowledge and skills required to create a capable workforce that can provide security safeguards, and develop, implement and enforce policies, standard operating procedures, tools, technologies and guidelines for best practices.

BACKGROUND TO THE STUDY

In Zimbabwe, the Cyber-Security and Data Protection Act [Chapter 11:22] draft specifies in Clause 5 that the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is designated as the Cyber Security Centre in Zimbabwe (Channon, 2019) and one of several functions of the Cyber Security Centre which this study is focusing on is providing guidelines to public and private sector interested parties on matters relating to awareness, training, enhancement, investigation, prosecution and combating cybercrime, and managing cyber security threats.

As a result, there is a demand for well-trained cybersecurity workers, and these specialists are developed in universities. Universities must invest in establishing cyber security expertise, which may be assessed by the number of initiatives, training and certification programs, and certified professionals of teams. This is also necessary to close the education-to-workforce gaps that are hindering efforts to fill cybersecurity jobs with qualified workers. These include gaps in competency, professional experience, and education speed-to-market (Milller & Molina-Ray, 2014).