against such an organisation. With regard to this, the cyber policy is expected to monitor and control all related activities to protect information and physical assets (International Standards Organisation, 2018). This section establishes the position of the literature on issues such as the cyber security policy framework, the formalisation of the cyber policy, and the procedure for formulating the cyber policy. These elements are important is ensuring the development of the cyber policy suitable to the organisation.

3.1 The cyber policy framework

The literature provides numerous definitions on policy framework. For example, the business dictionary[1] considers the policy framework as a set of principles and long term goals which form basis for making rules and guidelines. The law dictionary[2] defines it as a set of guidelines and long term goals which are taken to account when policies are made. In this study, we concentrate on elements guiding key contents of the policy. Hence, it is the interest of this sub-section to address key components of the cyber policy. Table 1 presents key components of the cyber policy based on three (3) authors. We choose the three (3) frameworks as our cases for study because they are research based, and indorsed by organisations specialised in cyber policy formulation.

Table 1: Elements of an effective security policy

No	Travellers Indemnity Company, 2018	The Security Magazine, 2018	Taylor, 2001, indorsed by Zdnet Tech. Co.
1	Data privacy	Ensuring data security accountability	Security accountability
2	Password management policy	Monitoring and compliance	Network services policies
3	Governing internet usage	Governing of network services	System policies
4	Manage email usage	Scanning for Vulnerabilities	Physical security
5	Uses of company owned devices	Managing patches	Incident handling and response
6	Uses of private devices	System data security	Acceptable use policy
7	Social media	Acceptable use	Security training
8	Software copyright and licencing	Response to incidents	-
9	Reporting security incidents	Accounts monitoring and control	-

Based on table 1, while some elements are common to all authors, the difference is evident too. For example, all frameworks talk about incident handling, while physical security is not given the same importance. The framework which do not adequately address all security issues is not fit for business continuity (Asgary, 2016). While businesses have the responsibility of evaluating their environment, and identify security needs (Bruijn & Janssen, 2017; Asgary, 2016); it is the plan of this study to formulate a comprehensive framework suitable for cyber security policies across Tanzania, and other African context. The study used three frameworks provided in table 1 and the focus group discussion to establish the new framework.

3.2 The relevance of the Procedure for Formulating and Updating the Cyber Security Policy

The Information and Communication Technologies (ICTs) field receives frequent changes. Innovative activities by ICT specialists (across the world) sophisticate such systems for better, through bringing updates to existing technological platforms (Dawson, 2018). In the same manner, new cyber threats emerge due to similar activities among cyber criminals. The emergence of new technologies require relevant methods of addressing security concerns (Thakur, Qiu, Gai, & Ali, 2015). This is the reason why cyber policies need to be comprehensive and updated regularly to carter for new criminal developments. Some organisations conduct the review of the policy once external changes are noticed. The changes may be brought through local and international regulatory bodies, or even the change in technology (Heeks & Stanforth, 2015). Other organisations agree on the time allowed for the policy to operate before it receives a comprehensive review. In the case where the organisation follows a certain timeframe, it is necessary to match the pace of technological changes for ensured business continuity. The study by (Lubua & Maharaj, 2012) suggests the maximum of three (3) years, of which the cyber policy must have received an extensive review. Challenges such as the lack of relevant policy knowledge, management support, and fund, are acknowledged to impede the review process.

Generally, there is no one principle guiding the cyber policy development or review process. Studies by Atoum, Otoom and Ali (2014), and Aiafi (2017) put emphasis on the following activities: Arriving to consensus on issues which require policy intervention, agreeing on the policy team, developing the policy through consulting stakeholders, validating the policy through due processes, adopting, and reviewing (refer figure 1). Arguably,

[1] http://www.businessdictionary.com/definition/policy-framework.html
[2] https://thelawdictionary.org/policy-framework/

policies do not adequately address security issues. Therefore, a total reliance to them would jeopardise the organisation. This study, in support of other studies such as Gagliardi, Hankin, Gal-Ezer, McGettrick and Meitern (2016), strongly support the formalisation of all cyber guidelines, through a process that solicit opinions from stakeholders, and finally receive approval from the top authority of the organisation.

6. Conclusion and Recommendation

This study addressed three key aspects of the cyber-security policy. First, the study developed the framework suitable for policy formulation. The study concludes by suggesting a cyber policy framework with seven key themes: Data security, Internet and network services governance, uses of company owned devices, physical security, incident handling and reporting, monitoring and compliance, and policy administrative issues. This study recommends the use of this framework in ensuring that the cyber-security policy is comprehensive. Moreover, study observed that the suggested case for study did not meet the framework's expectations. This observation is equally supported by representatives of other organisations. Factors contributing to the lack of comprehensive policy, as per this study, includes the lack of knowledge on policy formulation procedures, failure to involve key stakeholders, the lack of formalised guidelines, and the lack of policy review. It is the recommendation of this study that all of these activities must be guided by the cyber-security policy or other guidelines of the organisation.

7. References

Aiafi, P. R. (2017). The Nature of Public Policy Processes in the Pacific Islands. *Asia and Pacific Policy Studies, 4*(3), 451-466.

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science, 124*(1), 691–697.

Atoum, I., Otoom, A., & Ali, A. A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22*(3), 251-264.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*(1), 24-31.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7.

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review, 35*(2), 60-67.

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). *Advancing Cybersecurity Research and Education in Europe.* New York: Association for Computing Machinery.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatica, 58*(3).

Heeks, R., & Stanforth, C. (2015). Technological change in developing countries: opening the black box of process using actor–network theory. *Development Studies Research, 2*(1), 33-50.

Herjavec Group. (2017). *2017 cybercrimes report.* Retrieved Aug 21, 2017, from https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

International Standards Organisation. (2018). *ISO 27000 Standards* (5th ed.). Geneva: ISO.

International Telecommunication Union. (2009). *Cyber Security in Tanzania.* Geneva: ITU. Retrieved Aug 21, 2018, from https://www.itu.int/osg/spu/cybersecurity/contributions/Tanzania_Ulanga_paper.pdf

IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive* (Vol. 2nd). Illinois: ISACA.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332-349.

Kahyaoglu, S. B., & Caliyurt, K. (2018). Managerial Auditing Journa. *Managerial Auditing Journal, 33*(4), 360-376.

Lewis, J. (2018). *Economic Impact of Cybercrimes-No slowing down.* Santa Clara- CA: McAFee. Retrieved August 6, 2018, from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf

Lu, T., Zhao, J., Zhao, L., Li, Y., & Zhang, X. (2015). Towards a Framework for Assuring Cyber Physical System Security. *International Journal of Security and Its Applications, 9*(3), 25-40.

Lubua, E. W. (2014). Cyber Crimes Incidents in Financial Institutions of Tanzania. *International Journal of Computer Science and Business Informatics, 14*(3), 37-48.

Lubua, E. W., & Maharaj, M. (2012). ICT Policy and e-Transparency in Tanzania. *IST-Africa Conference Proceedings* (pp. 1-10). Dar Es Salaam: IST-Africa.

Makoza, F., & Chigona, W. (2013). Review of challenges in national ICT policy process for African countries. *Proceedings of ITU Kaleidoscope* (pp. 1-5). Kyoto: IEEE.

Metvier, B. (2017, 4 17). *Fundamental Objectives of Information Security.* Retrieved Aug 29, 2018, from Sage Data Security: https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad

Ohlin, J. D. (2017). *Did Russian Cyber Interference in the 2016 Election Violate International Laws?* Texas: Cornell law. Retrieved Aug 22, 2018, from https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2632&context=facpub

Saunders, J. (2017). Tackling cybercrime – the UK response. *Journal of Ceber Policy, 2*(1), 4-15.

Shojaie, B. (2018). *Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different Culture.* Hamburg: Universitat Hamburg. Retrieved Aug 23, 2018, from http://ediss.sub.uni-hamburg.de/volltexte/2018/9005/pdf/Dissertation.pdf

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An Investigation on Cyber Security Threats and Security Models. *IEEE 2nd International Conference on Cyber Security and Cloud Computing* (pp. 1-5). New York: IEEE.

Tuyikeze, T., & Flowerday, S. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. *HAISA* (pp. 11-20). Plymouth: HAISA.

Biographies

Dr. Edison W Lubua is a Senior Lecturer at the Institute of Accountancy Arusha, under the Department of Informatics. Prior to his academic position, he worked as the IT Administrator with the Mzumbe University and the University of Arusha. His experience extends to working with external Universities (Institutions) such as Coventry University, Bradford University, North-West University and the Tanzania Military Academy. Generally, Lubua, has published journal and conference papers which carry international reputation, together with serving as an editorial member and reviewer. Lubua is a certified IT Auditor, with a Master of Science in Human Resources Management (Mzumbe University), Master of Commerce in Information Systems (University of Cape Town), and PhD in Information Systems and Technology (University of KwaZulu Natal)

Prof Philip D Pretorius is Professor in the School of Mathematics and Statistics, with links to the School of Computer Science and Information Systems, in the Faculty of Natural and Agricultural Sciences of The North-West University of South Africa. He obtained his BSc in Mathematics and Mathematical Statistics, Hons BSc in Mathematical Statistics, MSc and PhD in Operational Research, all from the Potchefstroom University for Christian Higher Education. He published conference and journal papers, and lead postgraduate students. He also did projects in industry. Prof PD Pretorius research include the following areas; Management of projects, Operational Research Methodologies, Statistics, Experimentation and Simulation.