Cyber-security Policy Framework and Procedural Compliance in Public Organisations

Dr. Edison Wazoel Lubua
Department of Informatics
Institute of Accountancy Arusha, Tanzania
elubua@iaa.ac.tz

Prof. Philip D Pretorius
School of Computing and Information Systems
North-West University, Vaal Campus, South Africa
Philip.pretorius@nwu.ac.za

Abstract
This study was motivated by the fact that many organisations in Tanzania and Africa in general fail to meet security requirements suggested through ISO 27001 security standards, due to the lack of a credible cyber-security policy. The purpose was to develop the policy framework suitable in the management of the cyber-security in organisation level. Also, the study determined the compliance of selected cases for study to procedures for cyber policy formulation and review. The study used the qualitative approach. It engaged the literature in the conceptualisation of the study, used the discussion between researchers to formulate themes of the new cyber-security policy, used the focus group to improve the cyber-security policy framework, and used a survey questionnaire to study procedures and the formalisation of the cyber-security policy. Fifteen (15) organisation were represented in the survey, while ten (10) participants from six (6) organisations and four (4) countries were engaged in a focus group discussion. Both purposive and convenient methods were used in sampling. This study formulated a framework for cyber-security policy with seven 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. Moreover, the study confirmed that few organisations engages stakeholders in policy formulation and conduct the policy review at the interval not exceeding three years. Moreover, many organisations uses cyber-security policies without the authorisation of the top authority of their organisation. The study recommends the formulation of a comprehensive cyber-security policy through the use of the Lubua’s cyber-security policy. Further to this, the policy formulation procedure must be inclusive, and guided by existing organisation guidelines. The maximum of three (3) years is recommended for policy review. The formalisation of the policy document must be approved by the top authority of the organisation.

Key words: cyber-security policy, policy framework, Cyber policy framework, Tanzania, developing countries

1. Introduction
The number of crimes conducted through cyber platforms is growing fast across the globe. Globally, cybercrimes are projected to cost economic investments about six (6) trillion US$ annually, by 2021. This projection suggests the increase in cyber incidents to individual users and organisations (Saunders, 2017; Herjavec Group, 2017). Unfortunately, nearly half of all attacks are committed to small businesses (Herjavec Group, 2017). The situation is more alarming because of undocumented incidents, hence, the situation is likely to be worse. It is unarguable that the prevalence of cyber offenses is not suitable for social, political and the economic activities, because users become preys to criminals (International Telecommunication Union, 2009). Cybercrimes may lead to the defamartion of the reputation of an individual, and/or loss of money (Lewis, 2018). Further to this, cybercriminals
can dictate the political direction of a nation. For example, while it is not completely confirmed by international bodies, there is an ongoing debate that the 2016 general election of the United States of America, was interfered (Ohlin, 2017).

Given the current state of affairs on the security of cyber users, both local and foreign platforms are investing on techniques relevant in strengthening the security of users. For example, the International Standards Organisation (ISO) makes the review of general acceptable security policies to assist all organisations to secure their cyber systems (International Standards Organisation, 2018). Moreover, government authorities across the world enact laws, policies and guidelines to safeguard their classified information from being misused. The same laws provide guidance on cyber use among individuals and organisations under their jurisdiction (Bendovschi, 2015). Both international and national efforts for curbing cybercrimes are relevant, but may not necessarily address every case in the field. Based on this reason, sectoral and organisational measures are necessary (Bendovschi, 2015; Lewis, 2018). Every single organisation must address its cyber platform uniquely, and develop the policy guiding users of the technology. It is the role of the cyber policy to ensure the business continuity through safeguarding all critical areas.

The ISO 27001 is meant to provide guidelines for information security management, through different codes of practices. Structurally, the ISO 27001 guides the localised cyber policy to consider its own environment in deciding on the type of controls suitable for the organisation. One area of emphasis is a proper allocation of roles and responsibilities among users of the information system (Kahyaoglu & Caliyurt, 2018). Individual roles are matched with duties to prevent inappropriate activities from users. Accordingly, the localised security policy must address the use of mobile devices, such as laptops, tablets, smartphones and different computer peripheral devices (Kahyaoglu & Caliyurt, 2018; Lu, Zhao, Zhao, Li, & Zhang, 2015). Moreover, teleworking must not be ignored, because cyber criminals may imitate legitimate users and compromise the system (Lu, Zhao, Zhao, Li, & Zhang, 2015). Although the level of cyber awareness in different organisations is increasing, many organisations are still in a dabbling investment toward establishing strong cyber policies. For example, policies which are incomprehensive and lack the support of the top management could pose a security challenge. Moreover, the cyber policy requires a regular review to accommodate new threats. These are the issues addressed by the current study in cyber security policy.

2. Research Context

This paper is developed with the knowledge that the cyber security policy is meant to provide guidelines for the security of an organisation. Hence, in this study researchers concentrated on establishing the cyber security framework relevant for organisation’s level security. Moreover, the study determined whether cyber security policies in public organisations are comprehensive, and their formalisation process is the one recommended by the literature. These are important aspects for ensuring the security of users of the cyber infrastructure (Galinec, Možnik, & Guberina, 2017). In general, this study supports observation by Dawson (2018) who suggested that the security of cyber users must come first for an assured business continuity. Less secure environment are detrimental, both economically and socially (Dawson, 2018; Lu, Zhao, Zhao, Li, & Zhang, 2015). Worldwide, above 600 billion USD were stolen through cybercrimes in 2017 (Lewis, 2018). Further to this, there is an increase of interferences in different political processes, which push the society to a critical information warfare era (Ohlin, 2017). The current status requires individual organisations to manage their risks, through deploying necessary controls on cyber use (International Standards Organisation, 2018). One way to address risks posed to the organisation due to the use of cyber infrastructure, is to establish cyber policies and guidelines relevant to a particular organisation, regardless of existing universal cyber norms (Saunders, 2017; Kahyaoglu & Caliyurt, 2018). Hence, the current study is relevant because it contextualises itself to the public sector of Tanzania, where it addresses the following objectives:-

i.) To develop the cyber policy framework relevant in addressing modern cyber security issues.

ii.) To determine the fitting of the chosen case for study (cyber security policy) to the proposed cyber policy framework.

iii.) To evaluate the formalisation of cyber security policies in the context of Tanzania public sector.

iv.) To evaluate the relevance of procedures for formulating and updating the cyber policy

3. Literature

Organisations spend a large amount of money in establishing the cyber infrastructure supporting their business operations. This includes the fund for purchasing hardware, software, managing data and hiring experts for managing the infrastructure. Data repositories form a virtual segment of the asset, which is equally valuable to the organisation. In the case where the organisation fails to protect its information asset, likeliness of not meeting its strategic objectives is high organisation (Järveläinen, 2012). Competitors may use the available information © IEOM Society International
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 in 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 dictionary¹ considers the policy framework as a set of principles and long term goals which form basis for making rules and guidelines. The law dictionary² 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data privacy</td>
<td>Ensuring data security</td>
<td>Accountability</td>
</tr>
<tr>
<td>2</td>
<td>Password management policy</td>
<td>Monitoring and compliance</td>
<td>Network services policies</td>
</tr>
<tr>
<td>3</td>
<td>Governing internet usage</td>
<td>Governing of network services</td>
<td>System policies</td>
</tr>
<tr>
<td>4</td>
<td>Manage email usage</td>
<td>Scanning for Vulnerabilities</td>
<td>Physical security</td>
</tr>
<tr>
<td>5</td>
<td>Uses of company owned devices</td>
<td>Managing patches</td>
<td>Incident handling and response</td>
</tr>
<tr>
<td>6</td>
<td>Uses of private devices</td>
<td>System data security</td>
<td>Acceptable use policy</td>
</tr>
<tr>
<td>7</td>
<td>Social media</td>
<td>Acceptable use</td>
<td>Security training</td>
</tr>
<tr>
<td>8</td>
<td>Software copyright and licensing</td>
<td>Response to incidents</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>Reporting security incidents</td>
<td>Accounts monitoring and control</td>
<td>-</td>
</tr>
</tbody>
</table>

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/
conducting an investigation on the issue which requires the policy intervention, engaging stakeholders in the formulation process and revising the policy are key aspects of the formulation process (Aiafi, 2017; Shojaie, 2018). In the current study, our interest is to investigate the compliance of public organisations to the policy formulation process. In particular, our interest is vested on the involvement of stakeholders and the timeline for policy review.

Figure 1: Policy development cycle (Open Educational Resources Africa, 2018)

3.3 Formalizing the Cyber Security Policy
Before 2010 many African countries did not have policies guiding cyber activities at the national level. This status was a reflection of individual organisations doing business in these countries (Lubua & Maharaj, 2012). Today, more organisations are aware of the presence of cyber threats, which must be controlled for ensured business continuity (Makoza & Chigona, 2013). Unguided cyber use endangers the security of users and associated organisation (Lubua & Maharaj, 2012; Lu, Zhao, Zhao, Li, & Zhang, 2015). In Sub Saharan Africa, none is ranked among top 30 countries (of the world), with the cyber security ISO 27001 certificate of compliance (Shojaie, 2018). Further to this, Tanzania has 0.02 certificates of compliance in every population of 15,982,380 people (Shojaie, 2018). This is a very low level of compliance, given ISO standards. A relevant cyber security policy is an important indicator for an organisation to become ISO 27001 certified. Different bodies of professional advise that the cyber policy must draw its legitimacy from its stakeholders, but get formalised through the approval by the top authority of the organisation. Traditionally, the central government uses the so called Top Management, while private organisation and government agencies uses the Board of Directors to approve any new policy, or policy statement. Hence, all cyber security guidelines must be approved before they get used (Add reference here). Part of this study analyses practices for formalising the cyber security policy and associated among public organisations of Tanzania.

4. Methodology
This study follows the qualitative approach in addressing the knowledge gap. Its different areas of study were established through ISO 27001 guidelines (the 2018 review), and expounded through the support of related literature. Based on the assessment tool issued by the Integrated Assessment Services (2018) on ISO 27001 guidelines, four areas of focus were identified: The need to establish the cyber security policy framework suitable for organisations in modern times, the compliance of the chosen case for study to the proposed cyber-security framework, the relevance of the policy formulation procedure, and the policy formalisation.

Two methods were used to develop the cyber-security framework. The first method was the review of the literature on the cyber-security policy framework. The main criteria was for the framework to be research based and indorsed by a company specialising on cyber policy development. Figure 1, presented the summary of cyber-security policy frameworks used in formulating basis for this aspect of the study. Further to this, the study grouped similar elements to a common theme. Developed themes were combined to form entries to the new cyber-policy framework. After this phase, the new cyber-security policy framework was presented to a group of specialists attending two weeks training on cyber security at the Eastern and Southern Africa Management Institute (ESAMI) for further refinement or possible extension. Below is the composition of the focus group.

Table 2: Focus group composition

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Country</th>
<th>No</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tanzania Communication and Regulatory Authority</td>
<td>Tanzania</td>
<td>1</td>
<td>Cyber specialist</td>
</tr>
</tbody>
</table>
The remaining part of our objectives were achieved through the use of structured interviews, conducted to fifteen (15) representatives of government agencies in Tanzania. Because, many organisations hesitate to engage in studies of this nature, due to security reasons, researchers chose to engage public organisations represented through the 2017 Master of Information Security class, of the Institute of Accountancy Arusha. These organisations carries specialised activities on behalf of the government, therefore, they handle data which are sensitive to the development of the nation, and their operations significantly depends on the use of the cyber. The current study makes the identity of these organisations anonymous for security purpose. Data collection through structure interviews focused on themes presented in table 3.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Questions used in data collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>The formality of the policy</td>
<td>Do you have a formal cyber policy?</td>
</tr>
<tr>
<td></td>
<td>What authority is responsible in approving the cyber policy?</td>
</tr>
<tr>
<td></td>
<td>Do you have other guidelines (oral or written) for cyber use, apart from the main policy?</td>
</tr>
<tr>
<td></td>
<td>How many past years since the current policy existed?</td>
</tr>
<tr>
<td>The procedure for establishing the policy statement</td>
<td>What procedure do you follow in formulating the cyber policy?</td>
</tr>
<tr>
<td></td>
<td>Is the procedure acknowledged in any organisation’s guiding documents?</td>
</tr>
<tr>
<td></td>
<td>What procedure do you use in addressing emergent cases, not addressed by the current cyber policy?</td>
</tr>
<tr>
<td>The nature of policy review</td>
<td>What us your opinion on the adequacy of the cyber policy in managing the security of users?</td>
</tr>
<tr>
<td></td>
<td>Given the nature of Technology change, how many years do you recommend before a formal cyber policy review is conducted?</td>
</tr>
<tr>
<td></td>
<td>Do you personally know the procedure for conducting the review of the cyber policy or its guidelines within your organisation?</td>
</tr>
<tr>
<td></td>
<td>How do you generally evaluate the usefulness of the cyber policy of your institution in addressing your security and that of the organisation?</td>
</tr>
<tr>
<td></td>
<td>Considering the delicacy of the cyber security, do you consider the frequency of policy and guidelines reviews sufficient?</td>
</tr>
</tbody>
</table>

Generally, the position of the current study on the nature of the cyber-security policy framework was arrived through consensus during a focus group discussion conducted at ESAMI, involving ten (10) cyber-security professionals. On the other hand, the common themes of structured interview questions were identified and grouped together. The information was applied to draw different conclusions from the study. The analysis was based on frequencies.

5. Results

The literature provides different information on fundamental objectives of corporate cyber security policy. For example, studies by Alqahtani (2017), Galinec, Možnik and Guberina (2017), and Metvier (2017), suggested that the cyber security policy is meant to ensure the confidentiality, availability and integrity of the information available on the cyber infrastructure. The current study supports these fundamental objectives, however, it equally acknowledges that the policy may incorporate other objectives. In order to meet these security expectations the cyber policy must comprehensively incorporate key subjects, through following the formal policy development procedure (International Standards Organisation, 2018). Moreover, it must get communicated to key stakeholders and receive reviews on a regular basis, as the result of technological changes. This section provides the cyber security framework suitable in different organisation settings. Moreover, the section evaluates the
comprehensiveness of the chosen case for study in addressing security issues in modern times. Further to this the study provides results on the formalisation process and the relevance of procedures for cyber policy development.

5.1 Cyber Policy Framework, Comprehensiveness and Adequacy
This subsection responds to two basic questions: First, what are the key elements of the cyber policy framework, relevant for modern security? To what extent is the case chosen for this study compliant to this framework?

Key elements of the cyber security policy framework
This study establishes the cyber-security policy framework suitable in the Tanzanian context, through two main stages. First, researchers identified three frameworks (refer figure 1) through google search. These are the only frameworks developed based on research activities and supported by companies specialising in cyber security policy development. Through the use of these three frameworks, researchers grouped common elements to same category. Overall, seven categories of elements were established in the first phase of the cyber policy framework. Table 4 presents categories of the resulting framework and their entry based on researchers’ view.

Table 4: 1st Draft of Lubua’s Framework of the Cyber Policy Elements

<table>
<thead>
<tr>
<th>Entry to the Lubua’s Cyber Policy Framework</th>
<th>Extraction from three frameworks used as basis for this study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Ensuring data security accountability (security magazine, 2018), System data security (security magazine, 2018), Security accountability (Taylor, 2001), Data privacy (Travellers Indemnity Company, 2018), Password management (Travellers Indemnity Company, 2018)</td>
</tr>
<tr>
<td>Physical security</td>
<td>Physical security (Taylor, 2001)</td>
</tr>
<tr>
<td>Incident Handling and Reporting</td>
<td>Incident Handling and Reporting (Taylor, 2001), Response to incidents (Security Magazine, 2018), and Reporting security incidents (Travellers Indemnity Company, 2018)</td>
</tr>
<tr>
<td>Monitoring and Compliance</td>
<td>Monitoring and Compliance (Security Magazine, 2018), Account monitoring and control (Security Magazine, 2018), and Software licencing (Travellers Indemnity Company, 2018)</td>
</tr>
<tr>
<td>Policy and Administrative Issues</td>
<td>Policy administration and review and Training of system users (Taylor, 2001)</td>
</tr>
</tbody>
</table>

The framework proposed in table 3, was presented to experts (Information Systems Auditors and Cyber Security specialists) who were attending a cyber security workshop at the Eastern and Southern African Management Institute (ESAMI) between 10th and 21st September 2018, for their input. Table 2, provided details about their composition. Through series of discussions conducted on the 12th of September 2018, the framework in table 4 received few modification. First, the scanning of vulnerabilities was moved from the category for uses of company owned devices to incident handling and reporting. Managing patches is another element moved from the category for uses of company owned devise to the category for monitoring and compliance. Further to this, the focus group discussion introduced a new element known as forensic auditing and risk management to the incidents handling and reporting category. Table 4 presents a modified framework, which receives the approval of researchers. The new framework can be referred as Lubua’s framework of key elements of the cyber-security policy.

Table 5: Lubua’s cyber-security policy framework

<table>
<thead>
<tr>
<th>Entry to the Lubua’s Cyber Policy Framework</th>
<th>Extraction from three frameworks used as basis for this study and the focus group discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Ensuring data security accountability (security magazine, 2018), System data security (security magazine, 2018), Security accountability (Taylor, 2001), Data privacy (Travellers Indemnity Company, 2018), Password management (Travellers Indemnity Company, 2018)</td>
</tr>
<tr>
<td>Uses of Company Owned Devices</td>
<td>Company owned devices (Travellers Indemnity Company, 2018 and Acceptable use policy (Taylor, 2001)</td>
</tr>
</tbody>
</table>
The compliance of the chosen case for study to Lubua’s cyber security framework

This study received the permission to access and use one of the cyber policy as a case for study. Other organisations admitted that their policies were meant for internal use or formal auditing exercise. The accessed policy came from a higher learning Institution, where the name was requested to remain anonymous. The intention for using this case for study was to determine the comprehensiveness of the policy, through understanding its fitting to the framework proposed in table 5. The policy used as the case for study was organised to the following sections: the introduction which offered the general information about the policy, internet guiding principles, internet access and use, website creation and maintenance, user responsibilities, confidentiality, obligations of users, obligations of technical staff, and helpful suggestions. Basically, the organisation of this policy document do not meet the standard framework presented in table 4. For example, it is the requirement to organise elements of the common theme together (Lubua & Maharaj, 2012), however, the policy under study separated elements such as internet guiding principles, internet access and use, and website creation. Putting elements with a common theme simplify the referencing (Alqahtani, 2017; Aiafi, 2017). Table 6 summarised the components of the case for study, and their fitting to the Lubua’s framework. Apparently, only two aspects of the Lubua’s framework are represented, that is, internet and network services governance, and data security. Issues about user responsibilities, user obligations, and obligations of technical staff, as provided by the case for study, do not belong to a specific section within the Lubua’s framework. In every aspect of the policy, there is something about the user, therefore they are cross-cutting. Categories presented in the Lubua’s cyber policy framework are important for business continuity; their absence to the studied case makes the policy narrow and inadequate. Issues related to incident handling and reporting, and monitoring and compliance were completely ignored by the case for study, thus, the business continuity is in jeopardy (Dawson, 2018; Galinec, Možnik, & Guberina, 2017).

Table 6: the fitting of the case for study to the proposed cyber framework

<table>
<thead>
<tr>
<th>Elements of case for study</th>
<th>Elements in Lubua’s Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet guiding principles, internet access and use, and website creation and maintenance</td>
<td>Internet and network services governance</td>
</tr>
<tr>
<td>User responsibilities, user obligations, obligations of technical staff</td>
<td>These are cross-cutting issues, they get reflected in all categories based on the context of discussion</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data security</td>
</tr>
</tbody>
</table>

Further to this, the analysis of the case for study unveiled the following areas of weakness, which require consideration:-

- The administrative structure acknowledged by the policy is not existing. This makes it difficult to implement. It is necessary that administrative positions acknowledged by the policy, are the one in practise; this is useful for a smooth implementation of the policy.
- The IT Committee is responsible for reviewing and approving new aspects of the policy. This is against acceptable Information Systems Audit and Assurance norms. The board of directors (or the top management in government settings) is responsible for the review and approval of the policy. The approval by the board of directors brings the sense of responsibility to the rest of employees, including those at the top management level.
- The policy gives the ICT Director the power to formulate rules and guidance on the use of information systems. The current study is against this proposition, and strongly suggest that the policy must be the fundamental document for all rules and regulations, and the approval must come from the board of directors. Multiple guidelines may confuse users.
- There is no warrantee of the security, confidentiality and integrity of data. This statement deny users their key information rights, and impose danger to their social and economic status.

As stated in proceeding paragraphs the study did not have access to cyber policies from other organisations. Therefore, the study used a survey question to understand the perception of ICT systems administrators on the adequacy of their respective cyber policies for security purposes. The analysis shows that five (5) respondents out of Fifteen (15) suggest that their policy is adequate in addressing security issues. Their position is demonstrated
as the result of using the policy in managing security issues within their respective organisations. At least 2/3 of the ICT administrators of different organisations are not comfortable with the adequacy of their policy in managing security incidents. This suggests that the business continuity of these organisation is not well addressed by the cyber security policy (Shojaei, 2018; Thakur, Qiu, Gai, & Ali, 2015).

5.2 The Relevance of the Procedure for Formulating and Updating the Cyber Policy
The quality of the cyber policy is partly dependent on adhering to the procedure for formulating it. One of the key elements for the formulation procedure is the level which policy stakeholders are engaged in the process, refer figure 1. Some organisations rely on a team of experts who use their experience and expertise to come-up with the policy document, while some rely on the engagement of different stakeholders who contribute to the contents of the policy. Arguably, the engagement of experts (especially external to the organisation) without internal stakeholders’ consultations limit access to inputs (Lu, Zhao, Zhao, Li, & Zhang, 2015). Inadequate inputs make the resulting policy unfit for managing the security of cyber users, within the organisation. In this study, eight (8) organisations (out of 15) uses a team of internal experts to develop the policy, based on their experience. Using internal experts is a good practise because they have a general understanding of business environment. Nevertheless, this must not ignore input from other stakeholders. The interview with one of respondents suggested that limiting consultations is meant to decrease the cost. The use of experts’ own experience as the only source of input, ignore the wealth of information available to other members of the organisation (Dawson, 2018; Shojaei, 2018).

Moreover, the study noted that six (6) organisations (out of 15), admitted not to have a formal statement guiding the procedure for formulating policy statements. Moreover, respondents from these organisation did not know what would be the procedure for formulating the policy, or amending the existing policy. This puts the organisation in the danger of remaining without a proper policy. The organisation which is currently having a cyber policy, may stay for a long period of time without changes. Studies suggest that the policy which provide guidance on how cyber activities are to be carried-out, and that which explains when and who is to initiate the policy formulation process make the operationalisation easy (Tuyikeze & Flowerday, 2014; Bendovschi, 2015). Moreover the study by Tuyikeze and Flowerday (2014) recommends that the policy must make a provision guiding the process for updating it. All respondents accepted the maximum of three (3) years for the policy to be reviewed. The timeline for updating the policy is equally supported by studies by Bendovschi (2015) and Saunders (2017). In our analysis, only seven (7) out of fifteen (15) organisations admitted to meet this condition. In an interview with respondents whose policy has not received a review in a period of time, beyond 4 years, they admitted that the extended review (period) is characterised by the lack of a guiding statement on when and who is to initiate the review process. Based on their experience, only four (4) respondents admit that their cyber policy adequately support security activities within the organisation.

5.3 Formalization of the Cyber Policy
The cyber policy is a formal document which provides guidance on cyber related matter. It is expected to follow a strict procedure during its formulation and formalisation to ensure that stakeholders’ opinions are accommodated. Moreover, it ensures that the policy attain the right mandate to guide all cyber activities within the organisation (IT Governance Institute, 2006). Based on data from fifteen (15) public institutions, the study learned that nine (9) organisations (60 percent of our enquiry) had a formal ICT policy. Moreover, only five (5) organisations receives the approval from the board of directors. According to the IT Governance Institute (2006) and Alqahtani (2017), the cyber policy must be approved by the highest authority available before its application. The approval by the highest authority of a given organisation provides the right mandate for enforcing the policy to all ranks, within that organisation. According to Aiafi (2017) and Lubua and Maharaj (2012), the policy must state and acknowledge the authority to review and approve the policy in the future.

Generally, ten (10) organisations, including those with a formal cyber policy, admitted to have other forms of guidelines for cyber use. Moreover, all admitted to use oral guidelines as well. The interview with a respondent with both formal and informal guidelines suggested that the later was an intervention from the Information Technology Unity, in their effort to safeguard the organisation from arising issues. This is the result of inaction or delayed approval from the top authority of the organisation (IT Governance Institute, 2006). Overall, six (6) organisations did not have a formal cyber policy, therefore, they relied on informal policies for guidance. In a focus group discussion, a consensus was arrived suggesting that informal guidelines offer a partial assurance to the security of users and that of the organisation because of the following reasons: they are not comprehensive, they do not draw their authority from the highest body of the organisation, and they are unlikely to follow professional procedures for policy formulation. Moreover, the focus group argued that cyber users have basis to debate against informal policies as they emerge from a lesser mandate. Accordingly, the fact that seven (7) out of ten (10) approved policies required other informal guidelines is suggesting that many of these approved cyber
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


**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.