Journal of Computer Science

Original Research Paper

An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector

[1]Melissa K. Chinyemba and [2]Jackson Phiri

[1]Department of Electrical and Electronics Engineering, School of Engineering, University of Zambia, Lusaka Zambia
[2]Department of Computer Science, School of Natural Sciences University of Zambia, Lusaka, Zambia

Article history
Received: 07-06-2018
Revised: 20-07-2018
Accepted: 26-10-2018

Corresponding Author:
Melissa K. Chinyemba
Department of Electrical and Electronics Engineering,
School of Engineering,
University of Zambia, Lusaka
Zambia
Email: melissa.kae@mctechz.com
kaemelissa@gmail.com

Abstract: Insider attacks are security breaches posed by an existing or former organizational stakeholder with unrestricted access rights to the resources who, with or without intent, compromises the confidentiality, integrity and availability of organizational data. Zambian public organizations are vulnerable to insider attacks due to a number of factors that include; technology complexity, understaffing, financial gains, lack of security policies and procedures, lack of adoption and implementation of international security frameworks and standards such as ISO 27000 and COBIT. Insider threats can be categorized into three dimensions namely; Information Technology (IT) Sabotage, Financial Fraud and Intellectual Property (IP) theft. This paper reports the results from three targeted public organizations in Zambia. These are among the few that seem to recognised cyber threats and have partially adopted some parts of security base practices and international information security standards such as COBIT 5.0 and ISO 27001 standard. The study aimed at assessing the security GAPs using ISO 27001:2013 Information Security Management System (ISMS) standard. The study approach used was quantitative and qualitative with survey questionnaires and interviews as assessment tools for empirical data collection. The study shows that Zambian public sector has related challenges in mitigation of insider attacks that calls for considered efforts in developing measures for mitigation of these challenges in order to ensure national cyber security readiness and enhancing data privacy. The study reviewed that majority of the organizations assessed lack insider security deterring policies such as access control, non-disclosure agreements (NDA), pre-employment screening and unacceptable use. Additionally, the findings indicated that majority of public organizations have not made any efforts towards cyber security readiness, while only about 33% have adopted some security base practices. Further, using Actor Network Theory (ANT) and Theory of Planned Behavior (TPB), the study proposed an expedient insider mitigation model with an emphasis on user awareness and access control considering that it is difficult to model human behavior.

Keywords: Insider, Security, ISO2001, Sabotage, Fraud, IP-theft

Introduction

The objective of information security is to ensure data confidentiality, integrity and availability at any given point including during data entry, processing, storage and transmission (Kabuya *et al*., 2012). This process cannot be overlooked due to the fact that technology has become a critical component of business operations in every organization (Agbinya *et al*., 2011; Mwanza and Phiri, 2016). Today Zambia's public organizations are reliant on technological infrastructure for handling, processing and transmission of all the business data and its related activities (Hunker and Probst, 2010; Chinyemba and Phiri, 2018a). Protection of information from unauthorised access and misuse, has become one of the main challenges faced by these

organizations (Chinyemba and Phiri, 2018a). This is because Information and Communication Technologies (ICT) has become more prevalent and complex, meanwhile the increase in the sophistication and volume of cyber-attacks by insiders are at an alarming rate. All insiders require access to the corporate resources for them to carry out their day to day tasks, however, some of them can take advantage of their access rights which an outsider doesn't have, to cause information security breach in an organization (Chinyemba and Phiri, 2018a).

An insider is a former business associate or employee with or had lawful access rights to the organizational resources (Hunker and Probst, 2010).

In information security, a threat is considered to be any mischievous deed that endeavors to acquire illicit access to organizational infrastructure. Therefore, the duo defines insider threats which are grouped into two namely; intentional (malicious) and unintentional insiders (accidental) (Hunker and Probst, 2010; Chinyemba and Phiri, 2018a).

An intentional insider is a malicious present or past business associate with access privileges to the system infrastructure but intentionally decides to abuse his/her access rights and harmfully affects the data confidentiality, integrity and availability for the organization (Cappelli *et al*., 2012). The intentional insider threats are further categorized into three namely; Fraud, IT Sabotage, Intellectual Property (IP) theft (Mat Roni, 2015; Trzeciak, 2012; CPNI, 2013).

Financial fraud includes instances where an insider performs a crime and or uses the available system to unlawfully modify organizational information for financial gain as a motivation. These are often caused when insiders see a chance to make a profit by abusing privileges or when outsiders offer money to steal personal information for identity crime and or modify information (Chinyemba and Phiri, 2018a; Smith, 2015).

Sabotaging is when an insider directs specific harm at a system, an individual or organization resources due to various willful reasons. This threat is inspired by vengeance due to job termination and disillusionment of employees by certain corporate decisions that do not favor them (Chinyemba and Phiri, 2018a; 2018b). Analyzing Sabotage using Actor-Network Theory (ANT) and the Theory Planned Behavior (TPB), it is deduced that sabotage is motivated by revenge and often caused by employees who become dissatisfied with the company's compensation, arguments, supervisors, co-workers, reprimands or job termination. This threat is usually executed by employees with high technical skills and access to critical assets, like ICT technologist, engineers and System Administrators (CPNI, 2013; Pitropakis, 2015).

IP theft involves instances where an insider uses the available system to steal proprietary information of an organization. These threats are usually inspired by competitive advantage. This can be when insiders steal property for a competitor or their own business. In the early 2000s all the way to 2004, IP theft from U.S.A companies due to espionage was predicted to cost about $250 billion per year, despite the fact that it wasn't specified as to what extent insider action contributed to the figures. The correct figure might not be known because most of organizations do not realize when they have been compromised and the majority of the few that are aware do not report the attacks for fear of losing customer confidence and competitive advantage (Musambo *et al*., 2017).

It is prudent to look at the three categories of insider threats unconventionally and conspicuously because their nature, as well as the mechanism for detection and prevention, can be diverse. For instance, a good number of IT sabotage incidents are usually committed by system administrators and engineers mostly after termination of contracts, whereas most IP theft incidents are usually committed by those whose job, once had something to do with that IP then, frauds are normally committed by lower management employees such as service desk, frontline and or customer services personnel (Chinyemba and Phiri, 2018a; Trzeciak, 2012; Musambo *et al*., 2017).

Unintentional insider is present or past business associate with access privileges to the system infrastructure who ignorantly passes over classified information to the perpetrators without consideration or clicks of dangerous links that can negatively impact the security of the organization (Hunker and Probst, 2010). These can lead to impairment or loss of the organizational resources despite the fact that the insider acted without the intent of financial benefit or sabotage but through ignorance, negligence and lack of awareness. These accidental threats are referred to as Unintentional Insider Threat (UIT) with the most common example being security incidents cause because of granting excessive access rights to wrong users (Chinyemba and Phiri, 2018a; CERT, 2013).

Insiders have a high probability of parenthetically implicating the information of the organization to a high risk because they operate risky conventional work processes without the right awareness and training (Chinyemba and Phiri, 2018a). These include the sizeable impact from unintentional deeds like the less-frequent mistakes caused by programmers who introduce exposures during software development through bypassing the Systems Development Life Cycle (SDLC) steps. These can be caused by various reasons including; lack of user awareness, human error, age, fatigue, exhaustion, stress, moods, gender issues, drugs and the cultures (Chinyemba and Phiri, 2018a; CERT, 2013). The risks are aggravated when the attack is targeting a specific individual or organization and are

referred to as an Advanced Persistent Threat (APT). They are created to specifically enhance the success of the likelihood by impersonation. This is when an attacker sends an instant message or email to a user purporting to be a friend because it contains specific information and or is written in such a conversational style which the user uses so often. The targeted user is likely to trust the communication and be tricked into executing an act which may lead to an organizational security breach unintentionally (Chinyemba and Phiri, 2018a; CERT, 2013).

It is cardinal for the public organizations to know what brings about insider threats, the exact motivation behind the acts and the organization security posture which highlights the gaps to be able to mitigate this problem to an acceptable level (Pitropakis, 2015). The trajectory of insider attacks necessitates strategic attention just as much as the external threats because both categories, have proved to be a continuous and constant problem for ICT security management and Zambia is not an exception (Chinyemba and Phiri, 2018a; Musambo *et al*., 2017).

The ability of an ICT technologist, engineer and system administrator to monitor and audit device logs can potentially lead to the discovery of illicit insider activity or perhaps to indicate that an insider is about to go rascal. However, given the advancement of mobile technology, the number of devices connected to the network, number of employees with access to sensitive information, potential insider threats, as well as time and labour required to thoroughly investigate logs. These includes both in real time and historically. Such monitoring becomes an irresistible encounter in an absence of effective ICT security controls that requires coordinated efforts to implement (CERT, 2013).

The mobile technology advancement and lack of related procedures and policies in organizations to control the number of employees with access to critical data, devices connected to the network, the resources required to thoroughly investigate logs, has brought about insider threats (Phiri *et al*., 2011). A few organizations that have taken the head in combating this precarious issue through the adoption of International Standard Organizations (ISO) 27001 standard as a framework, has been concentrating on the prevention of outsider perpetrators (Chak, 2015).

With the above insider threat highlights, it was sort prudent that an investigation on Insider Threat Mitigation be carried out to ensure that the mitigation model is of high priority for all organizations

Literature Review

Insider attacks landscape has shown an exponential growth in the recent past. This can be evidenced by a number of research that has been done globally by both academics and big business players such as CERT, SANS, IBM, KPMG, Verizon, Price water house Coopers (PwC), Ernest and Young (EY), Deloitte and Touche, Microsoft as well as the uprising of the of Internet of things (Chinyemba and Phiri, 2018a**;** Smith, 2015). The challenge necessitates an understanding of ANT in order to have knowledge of the link between human and circumstantial factors that include; technological, sociological and social-technical domains in which the insiders operate. This is because technology alone has the potential of enhancing the challenge than otherwise. The predicament has led many researchers to endeavor in studying TPB and individual behavior, with an aim of mitigating insider threats. Despite all the global efforts and the results, no such research efforts have been employed in Zambia to address Insider threats mitigation.

Recent surveys by Forrester's Global Business Technographics showed that internal fraud risks are an area that has long been managed using forensic data analytics and ranked as the top use case at 77%. While Cyber breach and sabotage ranked the second-highest risk area at 70% (FGBTSSR, 2015; VSR, 2015). It is, therefore, imperative that internal attackers, generally accounts for approximately more than half of the risks that an organization is exposed to, whilst the external threats account for approximately above a third of the risks despite the gravity of the external consequences to an organization (GRBMJ, 2013).

The Defense Personnel Security Research Center (DPSRC), has a record of numerous incidences by insider attackers among others including (Cappelli *et al*., 2012; GRBMJ, 2013; Hanley and Montelibano, 2011; Trzeciak, 2011):

- *Social Media and email posting incidence*: In a case of a University of Tennessee professor who relayed sensitive data to China, while he emailed the other classified documents to his private email address
- *Cellphone Clones incidence:* In a case of a group of insiders at a wireless telecommunications company who cloned more than 16,000 customer cell phones. The insiders made approximately $15 million worth of unauthorized calls for a period of six months
- *Copier incidence*: In a case of an Army signals analyst for National Security Agency (NSA) who used a handheld scanner to copy 52 classified documents that he later passed to the Soviets
- *Printing Incidence*: A case of a South Korean born American computer specialist working for the Department of Navy (DON) at the Office of Naval Intelligence. He used his insider access to find classified documents, delete the classification markings and printed them out to mail to his South Korean contacts

- *SCADA incidence*: In a case of an electrical supervisor who developed an application for a SCADA system which was being used by the water firm. He installed a malicious program on one of the organization's critical systems, after his contract termination and damaged the SCADA system
- *Banking incidence*: A case of a manager for a branch of a banking institution who stole over $225,000 from the business account after running into family health problems, gambling and unforeseen expenses
- *WikiLeaks:* A case of Bradley Manning, an American Army soldier who leaked the largest set of classified documents to the public as he worked as an intelligence analyst

In the direction of adopting industry best practices for the stated solution and strengthening the insider threat mitigation program, we adopted some components from the CERT's Insider Threat program as shown in Fig. 1, that are necessary to produce a fully functioning insider threat program to suit Zambian public sector.

A study done by Jeffrey Hunker Associates LLC and Christian W. Probst in Denmark reviewed that Insider threat is not one problem, but various because modeling human behavior is close to impossible which is a recorded limitation. Most perpetrators commit the crime while on duty having planned their actions so well, due to the sophistication of technology and financial gain (Hunker and Probst, 2010).

Another study carried by Jason Smith in England reviewed that 87% of identified intruders into information systems are either employees or others who are internal to the organization. Insider threat mitigation is a complex problem and research is in its infancy, therefore, there are opportunities for further research in this area. The researcher's stated the most public organizational shareholders are more sympathetic to organizations who have security breaches caused by externals than internals (Smith, 2015).

Abuli (2016), a researcher from Kenya developed a framework for assessing insider threats in Kenya's parastatals. He further recommended that Kenyan Parastatals should customize their mitigation strategies according to their organizations' goals so as to enable a multi-tiered insider threat plan of action.

A study by Collins Kachaka on cyber readiness in Zambia appraised that implementing cybersecurity programs in Zambia cannot be successful without careful consideration of the legal and regulatory implications. Therefore, organizations need to adopt a risk-based approach, identify physical locations of their critical data assets, advocate for user awareness on access, management hygiene and establish business rules of information management (Kachaka, 2016).

Another independent study in by Wesley Cornelissen of Finland recommended that, there is need for improvements in classification of information assets and accompanying handling policies. He said stated that most information security process are not embedded in the organizations, therefore, there is no insight in the actual threats to information security (Cornelissen, 2009).

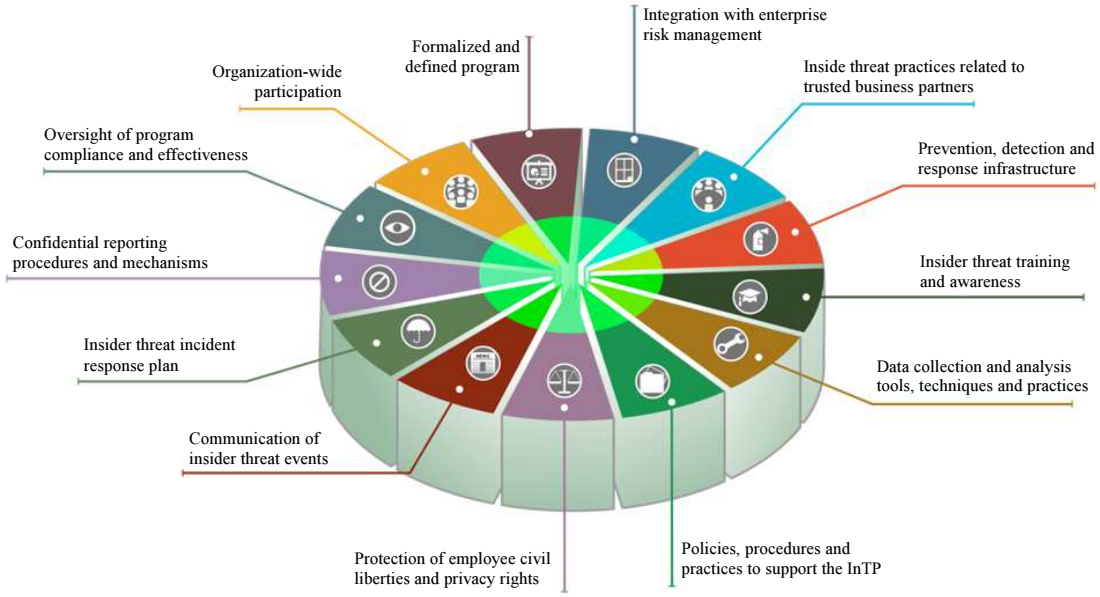


Fig. 1: CERT insider threat components (Trzeciak, 2012)

DOI: 10.3844/jcssp.2018.1389.1400

Benjaminsen's (2017) study on the Norwegian downsizing approach in terms of insider threats suggested that 76% of the cases were self-initiated, primary motivation for insider activity was financial gain (47%), ideology (20%)and desire for recognition (14%), loyalty to friends/family/country (14%)and revenge (6%).

An analysis of insider attacks mitigation strategies, reviewed that anyone with access to the cloud storage component is able to take snapshots or alter data in the storage. Therefore, insider security is one of the biggest issues in cloud computing as it offer storage services on a remote location that the consumers generally only need to trust the cloud provider and are unaware of what happens to their data. Among security threats in the cloud, malicious insider threats pose a serious risk to clients (Yusopa and Abawajy, 2014).

Methodology

The fruition of data collection in this study was achieved by the use of quantitative and qualitative methods which employed survey questionnaires both physical and online as well as face to face interviews of selected companies in Zambia's public sector.

The interview questions were designed to give the organizational maturity level status in the adoption and or implementation of ISO27001 standard. This gave a Gap analysis so as to be able to recommend the right controls for the mitigation of insider threats. ISO 27001 was chosen as the preferred standard of reference and hence the questions were based on the standards domains as listed in the Annexure A.

The targeted population in the organizations where the ICT asset owners as well as process owners, that included; Chief Information Security Officers (CISO), finance Human Resources (HR), Administration, Information Technology (IT), Software Development (S/W) Top management, Finance, Legal and Training.

Extensive Questionnaires were generated in line with the required research information. These included questions for assessing the extent to which internal Cyber/ICT security controls' assurance enhances corporate governance, assessing the influence of Cyber/ICT security recommendations on corporate governance and insider threats as well as security activities in the organization (Chinyemba and Phiri, 2018a; Yusopa and Abawajy, 2014).

The statistical values of the obtained results were analyzed, processed and verified using Microsoft Excel. Thereafter, an insider mitigation model was adopted with the concentration on user awareness, using the designed assessment activity roadmap in Fig. 2 (Chinyemba and Phiri, 2018a).

Findings

Baseline Assessment

In addressing the research objectives, a GAP analysis was conducted for three public organizations in Zambia to assess the ICT Security readiness and the gaps using ISO 27001 standard. The findings are as represented in the graphs that follow. Figure 3, show the number and size of the organizations that were assessed.

Figure 4 presents the roles of the respondents for the three organizations that were assessed.

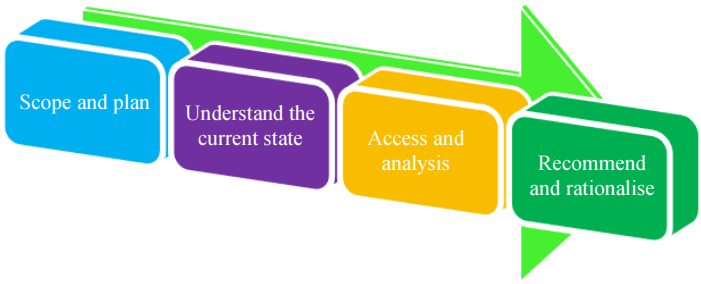


Fig. 2: Assessment activities

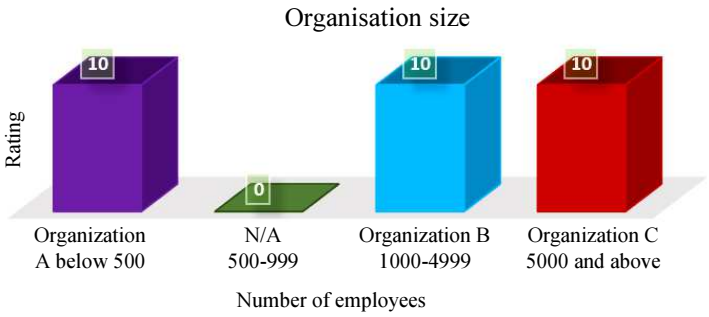


Fig. 3: Number and size of the organizations

DOI: 10.3844/jcssp.2018.1389.1400

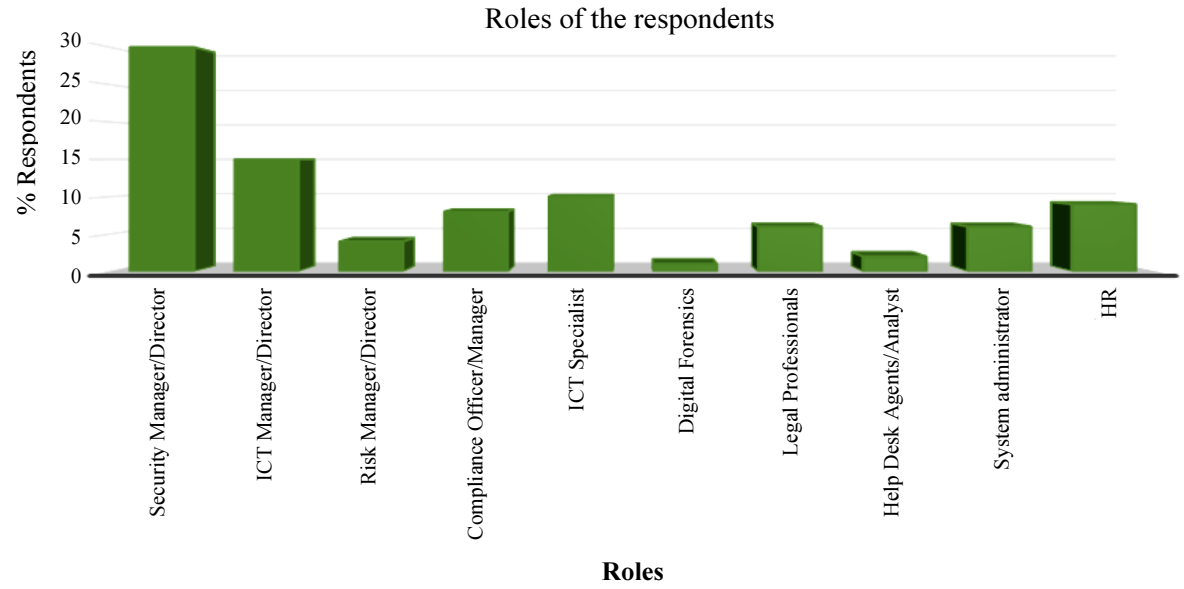
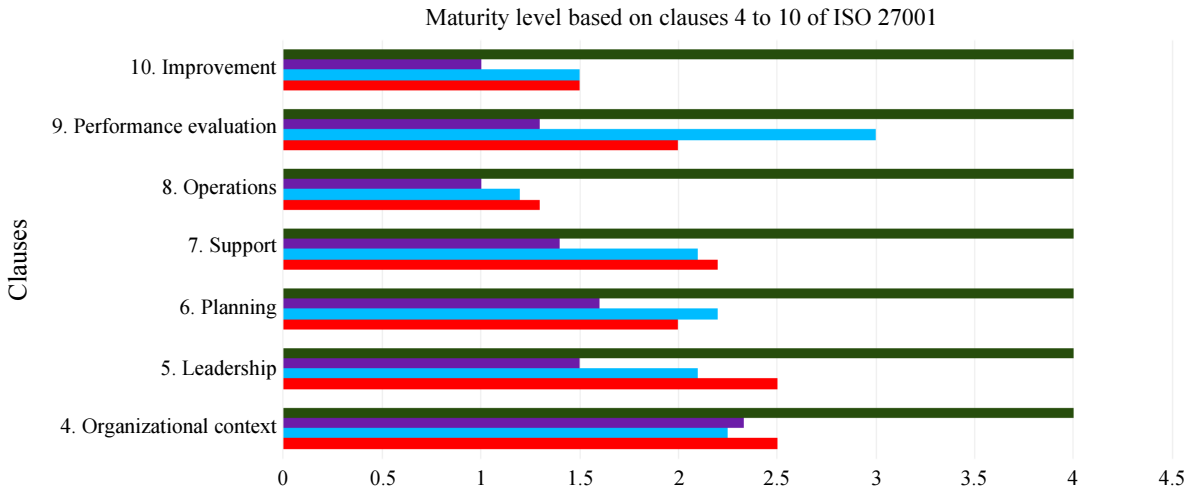


Fig. 4: Roles of respondents



	4. Organisational context	5. Leadership	6. Planning	7. Support	8. Operations	9. Performance evaluation	10. Improvement
Target score	4	4	4	4	4	4	4
Org C Avg Score	2.33	1.5	1.6	1.4	1	1.3	1
Org B Avg Score	2.25	2.1	2.2	2.1	1.2	3	1.5
Org A Avg Score	2.5	2.5	2	2.2	1.3	2	1.5

Fig. 5: Clauses 4 to 10 maturity level for organizations A, B and C

A.) Clause 4 to 10 Assessment Results

The following graph in Fig. 5 show the results of the assessment for the three organizations based on the ISO 27001 Clause 4 to 10 that includes:

6. Organization context
7. Leadership
8. Planning
9. Support

- 8. Operation
- 9. Performance evaluation
- 10. Improvement

DOI: 10.3844/jcssp.2018.1389.1400

Overally, all the three assessed organizations results were below average of the standard measure of 4. The current status poses a serious vulnerability of the organizations information.

B.) State of Security Base Practices

The following graph in Fig. 6 show results of the current status of Information Security base practice adoption of the three organizations as per ISO 27001:2013.

Overaly, all the three assessed organizations results were below average of the standard compliance measure of 100. The current status poses a serious vulnerability to the organizations information which is supposed to be protected.

C.) ISO 27001: ISMS Annex A

The following graph in Fig. 7 show results of the baseline assessment for security maturity level based on ISO 27001: Information Security Management System (ISMS) Annex A domains that includes:

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

Overaly, all the three assessed organizations results were below average of the standard compliance measure of 4. The current status poses a serious vulnerability to the organizations information which is supposed to be protected.

D.) Annex A Adopted Security Controls

The following graph in Fig. 8 show results of the ISO 27001: ISMS Assessment of Annex A implemented security controls based on ISO 27001:2013 Annex A as required by the standard.

Overaly, all the three assessed organizations results of the security controls implemented were below average of the standard compliance measure of 100. The current status poses a serious vulnerability to the organizations information which is supposed to be protected.

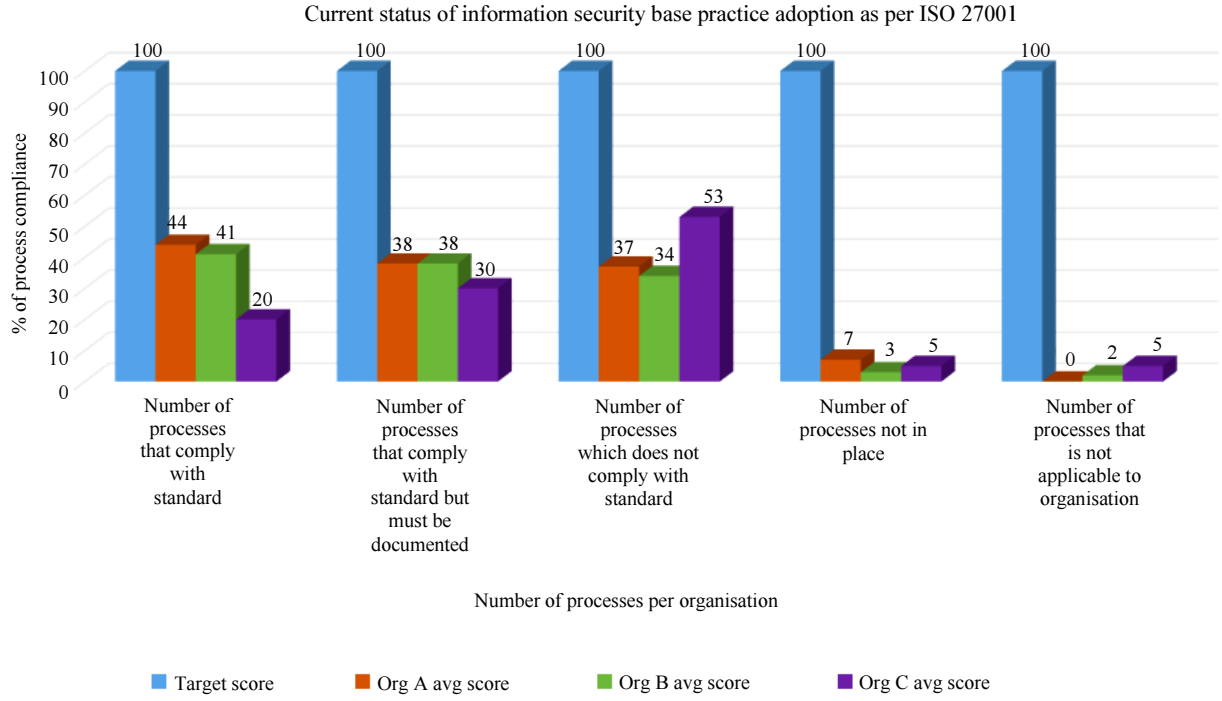


Fig. 6: Status of security base practices for Organization A, B and C

DOI: 10.3844/jcssp.2018.1389.1400

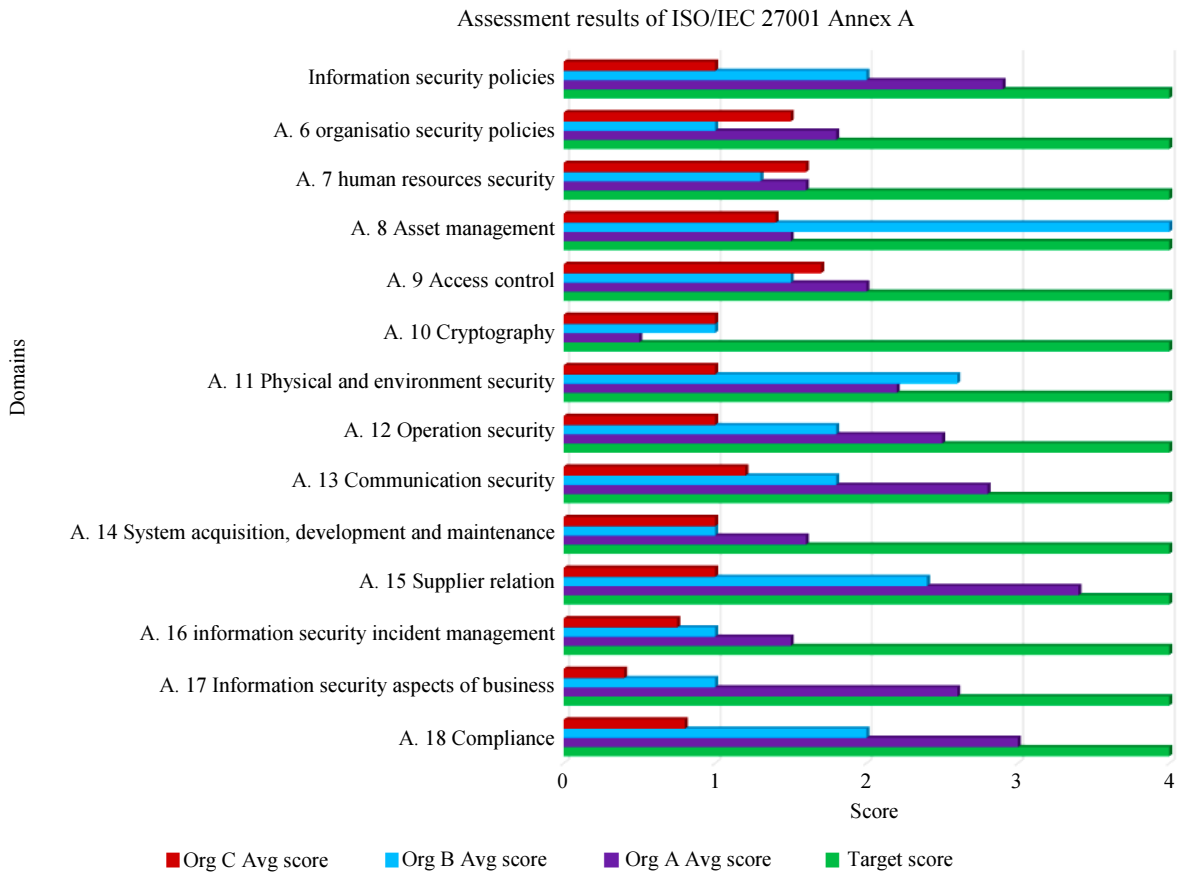


Fig. 7: Results of the baseline assessment - Annex A for Organizations A, B and C

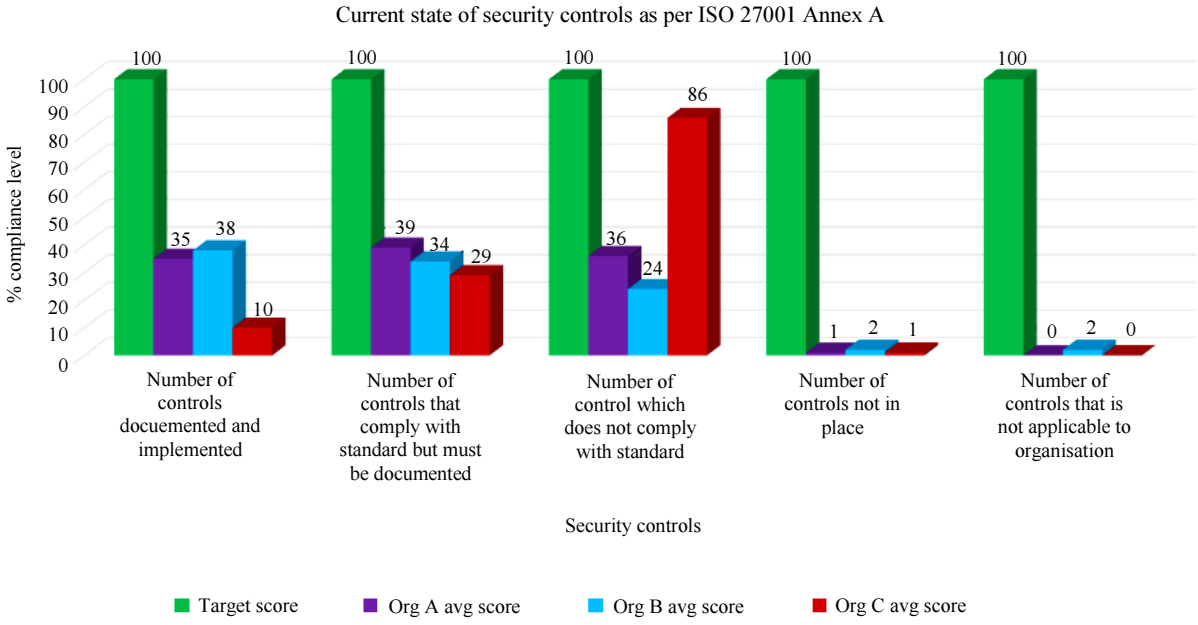


Fig. 8: Results of the current state of the security controls - Annex A for organization A, B and C

DOI: 10.3844/jcssp.2018.1389.1400

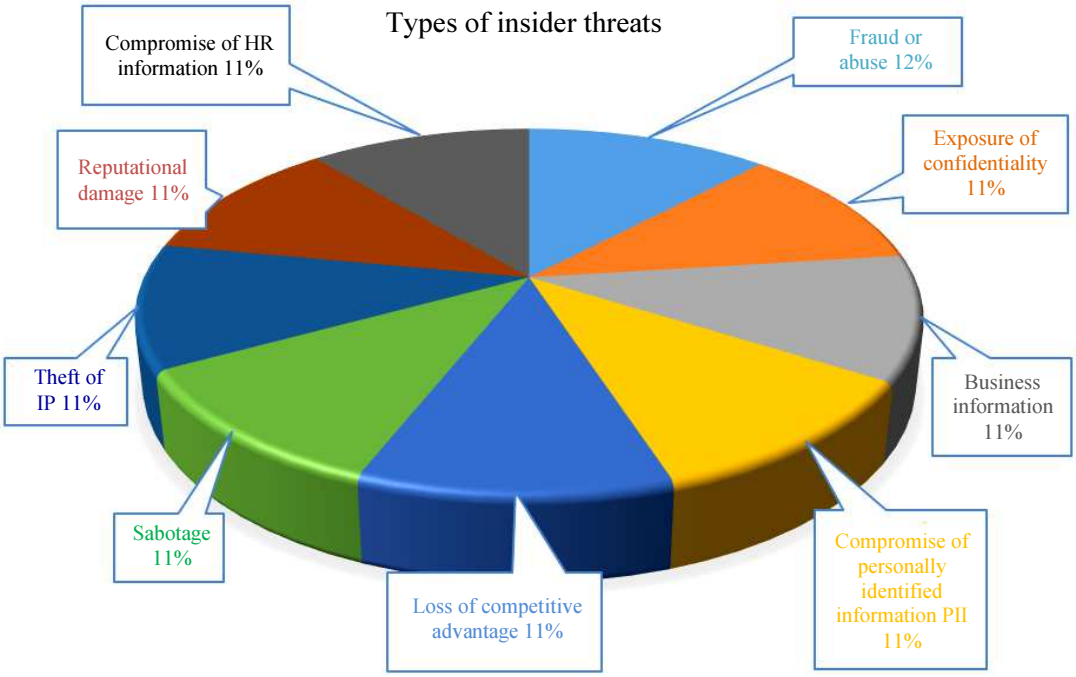


Fig. 9: Types of Insider threats

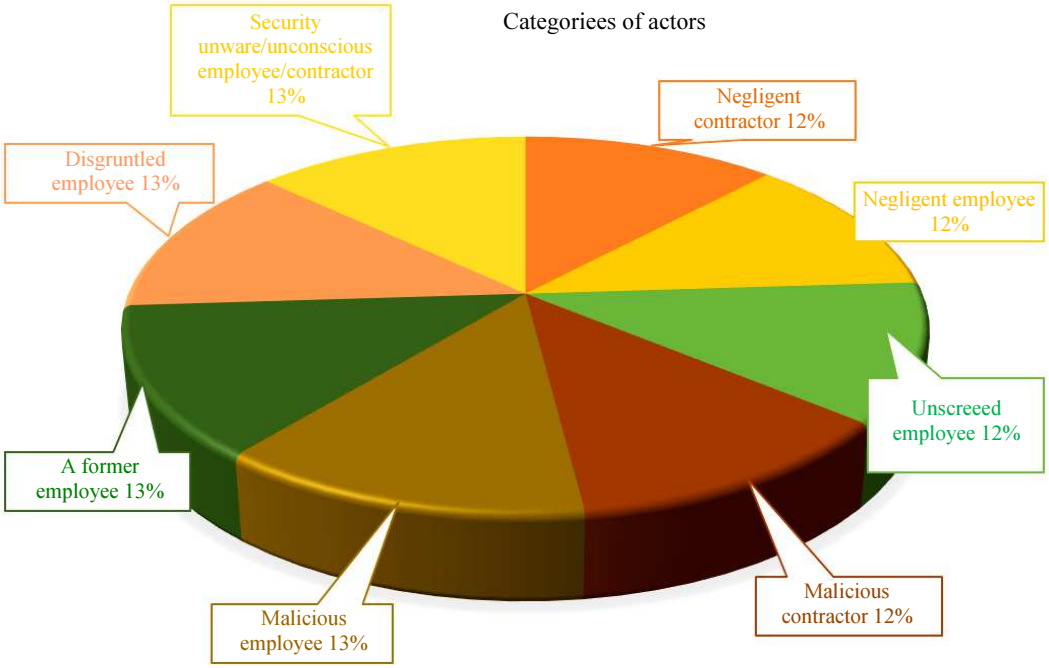


Fig. 10: Categories of insider actors

E.) Types of Threats

The following pie chat in Fig. 9 show the common types of threats posed by insiders in the three organizations under review.

The following pie chat in Fig. 10 show the common categories of insider threat actors in the three organizations under review.

Results Analysis

The three assessed organizations have knowledge of the importance of securing organizational data. They all have the Cyber/ICT Security Policies that aligns with the organization's corporate objectives and also defines security measures. However, these organizations need improvement based on the basic required documents of

DOI: 10.3844/jcssp.2018.1389.1400

the security departments to address the mitigation of insider threats (Chinyemba and Phiri, 2018a). These are mandatory documents for a cyber-ready organization in combating insider threats including; Cyber/ICT security policies, strategy, business continuity policies, classification of information procedure, classification of assets procedure, incidence handling procedure, pre-employment screening policies, Leavers interview policies, Comprehensive Non-disclosure agreements, Clear desk clear screen policies, Mobile device management policies and information handling and transfer policies, user awareness policies among others.

The assessed organizations are also cognizant of the international ICT security standards and have since adopted a number among them being ISO 27001: Information Security Management System (ISMS), ISO 9001: Quality Management System (QMS) and ISO 33001 Risk Management System (ERM), Control Objective for Information and Related Technologies (COBIT) 5.0., Information Technology Infrastructure Library (ITIL) among others. However, compliance has proved to not be adhered too. There is a need for enhancements together with consistency in order to address insider threats. The adopted standards necessitate some policies, procedures, guidelines and processes to be formulated, approved and distributed to the users so as to ensure compliance which initially has not been the case at the time of this study.

During the baseline assessment, it was evidenced that the access control policies are not fully implemented and enforced for compliance purposes, this leaves a doorway to malicious insiders by leaving valuable information susceptible to attacks. This, in turn, makes the entire infrastructure vulnerable as insiders are able to explore the ANT and TPB for their planned attacks.

There is no proper alignment of information security and ICT risk management, leaving ICT Risk management unclear to the stakeholders. No Risk plan, neither risk registers nor risk treatment plans are in place. All these vulnerabilities point to insider threats.

Information security effectiveness and performance requires an evaluation and redesign of an ISMS as so as to comply with the adopted standards and frameworks.

These assessments identified gaps in the existing organization ISMS which all points to the fact that they are operating in a vulnerable environment to insider threats. The perpetrators may leverage on the adverse effect of ANT and the TPB leading to Insider Crimes.

Discussion

The above findings have evidenced the fact that despite the organization's effort on combating external attacks, the enemy is just within. The systems are not secure enough to defend from insider threats. Notwithstanding the element of the organizations' effort of securing critical data, the environment is vulnerable and requires urgent attention. There is a need for extensive awareness so that, as the corporations' budgets for systems and put security tools in place, users should be made aware so they can help with the prevention and detection of the vulnerabilities.

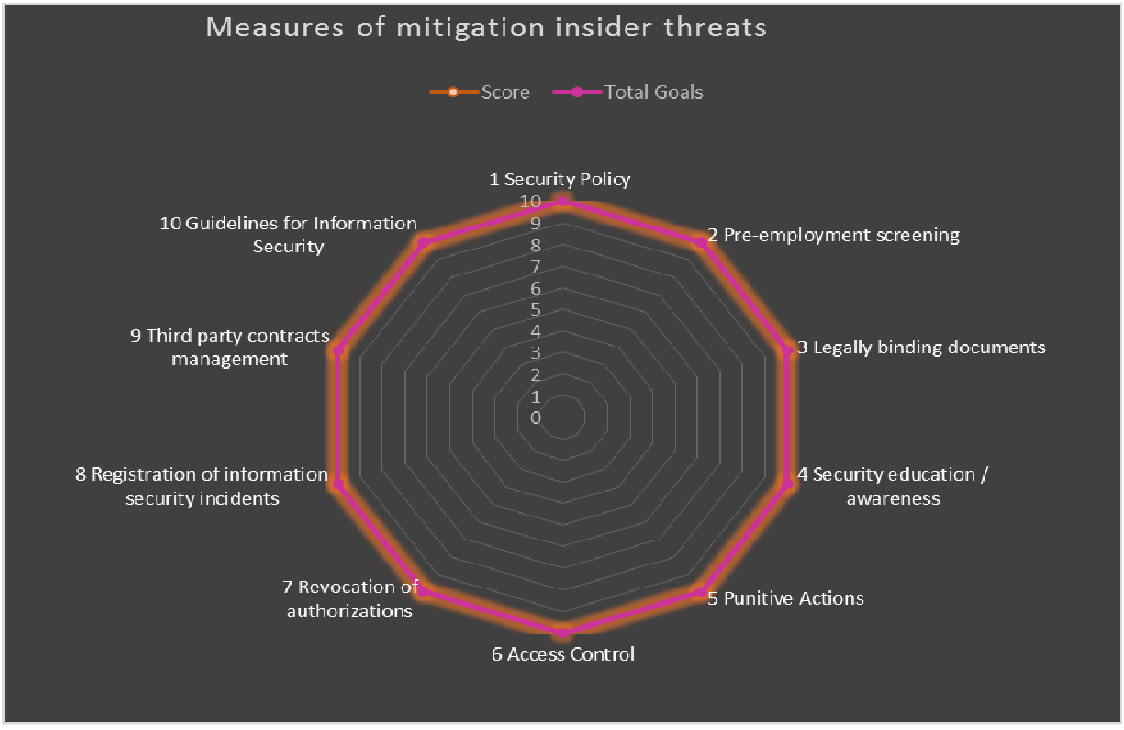


Fig. 11: Insider Threat mitigation model

For the mitigation and countermeasures, we wish to propose the following mitigation model because it's very applicable to the Zambian environment. Presented in Fig. 11 are the proposed steps of measures that must be considered in order to avert the insider threat with the top being user awareness.

Recommendations

We recommend that top management should exhibit commitment and support in managing information security by approving policies and ensuring that the required budget for the ISMS and tools are approved. ICT risk management should also be integrated into the enterprise risk management program. Management should ensure that they support all ISMS initiatives and walk the security talk because only then will the rest of the corporation comply. ICT security should be a fundamental fragment of all developments and procedures organizational wide. ICT security user awareness programs should be the top of the security agenda for all business associates in a quest to mitigate insider threat.

Conclusion

The information security solutions and controls adopted in the organizations are ineffective due to the fact that they are lacking comprehensive implementation for ease of compliance. It is evidenced that ISMS can be quiet pricey, but management should never look at it as an unnecessary cost because the damage that can be caused when any of the vulnerabilities are exploited, can be very grave and costly than expected. It is for this reason that we propose the designed mitigation model in Fig. 11 which is cheap and sustainable to the Zambian environment. For higher risks that cannot be mitigated by the proposed model, it would be prudent to transfer them to an insurer. However, when budget allows it is even better to fully implement the ISMS so as to ensure information security. All in all, information must be secured from the insiders as much as it is secured from the outsider.

Acknowledgement

Authors would like to acknowledge Dr. Collins Kachaka, Director of Center for ICT and Dr. Mwanaumo Assistant Dean both of the University of Zambia for the motivation and encouragement throughout the research process.

Authors Contributions

All the authors contributed for the fruition of this research.

Ethics

The corresponding author hereby confirms that ethics were considered for this research. And that the article is original and its contents are unpublished. The co-author has read and approved the manuscript for submission.

References

Abuli, M.J., 2016. A framework for assessing the insider threat in Parastatals in Kenya. MSc Thesis, Published on School of Computing and Informatics.

Agbinya, J.I., N. Mastali, R. Islam and J. Phiri, 2011. Design and implementation of multimodal digital identity management system using fingerprint matching and face recognition. Proceedings of the 7th International Conference on Broadband Communications and Biomedical Applications, Nov. 21-24, IEEE Xplore Press, Melbourne, VIC, Australia, pp: 272-278. DOI: 10.1109/IB2Com.2011.6217932

Benjaminsen, T., 2017. The Norwegian downsizing approach in terms of the insider threat-an interpretive study. MSc Thesis, Norwegian University of Science and Technology.

Cappelli, D., A. Moore and R. Trzeciak, 2012. The CERT Guide to Insider Threats: How to Prevent, Detect and Respond to Information Technology Crimes. 1st Edn., Addison-Wesley Professional, ISBN-10: 0321812573, pp: 432.

CERT, 2013. Unintentional insider threats: A foundational study. CERT Co-ordination Centre/SEI, Pittsburgh.

Chak, S.K., 2015. Managing cybersecurity as a business risk for small and medium enterprises. MSc Thesis, Johns Hopkins University.

Chinyemba, M.K. and J. Phiri, 2018a. Gaps in the management and use of biometric data: A case of Zambian public and private institutions. Zambia ICT J., 2: 35-43.

Chinyemba, M.K. and J. Phiri, 2018b. An investigation of information security threats from organisational insiders and how to mitigate them using a user awareness and access control model. Proceedings of the International Conference, (IC' 18), pp: 71-76.

Cornelissen, W., 2009. Investigating insider threats: Problems and Solutions. MSc Thesis, University of Twente.

CPNI, 2013. Centre for the Protection of National Infrastructure (CPNI), managing the insider threat. CPNI. London, Security Industry Authority (SIA).

FGBTSSR, 2015. Forrester's Global Business Technographics Security Survey report.

GRBMJ, 2013. The guardian report on Bradley Manning Judgenent.

Hanley, M. and J. Montelibano, 2011. Insider threat control: Using centralized logging to detect data exfiltration near insider termination.

Hunker, J. and C.W. Probst, 2010. Insiders and insider threats - an overview of definitions and mitigation techniques. Springer J.

Kabuya, C., J. Phiri and T. Zhao, 2012. Metric Based Technique in Multi-factor Authentication System with Artificial Intelligence Technologies. In: Future Wireless Networks and Information Systems, Zhang, Y. (Ed.), Springer Berlin Heidelberg, pp: 89-97.

Kachaka, C.C., 2016. An investigation into factors determining cybersecurity preparedness in Zambian commercial banks.

Mat Roni, M.S., 2015. An analysis of insider dysfunctional behavours in an accounting information system environment. http://ro.ecu.edu.au/theses/1640

Musambo, L.K., M.K. Chinyemba and J. Phiri, 2017. Identifying botnets intrusion and prevention-a review. Zambia ICT J., 1: 63-68.

Mwanza, M. and J. Phiri, 2016. Fraud detection on bulk tax data using business intelligence data mining tool: A case of Zambia revenue authority. Int. J. Adv. Res. Comput. Commun. Eng., 5: 793-798. DOI: 10.17148/IJARCCE.2016.53191

Phiri, J., T.J. Zhao and J.I. Agbinya, 2011. Biometrics, device metrics and pseudo metrics in a multifactor authentication with artificial intelligence. Proceedings of the 7th International Conference on Broadband Communications and Biomedical Applications, Nov. 21-24, IEEE Xplore Press, Melbourne, VIC, Australia, pp: 157-162. DOI: 10.1109/IB2Com.2011.6217912

Pitropakis, N., 2015. Detecting malicious insider threat in cloud computing environments. PhD Thesis, University of Piraeus.

Smith, J.A., 2015. Mitigating the cyber threat. Technical Report, RHUL–ISG–2015–12.

Trzeciak, R., 2011. Insider threat blog. The CERT Insider Threat Database, CERT Coordination Center/SEI.

Trzeciak, R., 2012. CMU-the insider threat center: Thwarting the evil insider the CERT top 10 list for winning the battle against insider threats.

VSR, 2015. Volumetric survey report, InsiderThreat.

Yusopa, Z.M. and J. Abawajy, 2014. Analysis of insiders attack mitigation strategies. Proc. Soc. Behav. Sci., 129: 581-591. DOI: 10.1016/j.sbspro.2014.03.716