AN INVESTIGATION OF INFORMATION SECURITY THREATS FROM ORGANISATIONAL INSIDERS AND HOW TO MITIGATE THEM USING A USER AWARENESS & ACCESS CONTROL MODEL

Melissa K. Chinyemba
Department of Electrical and Electronics Engineering
University of Zambia
Lusaka, Zambia
kaemelissa@gmail.com

Jackson Phiri
Department of Computer Science
University of Zambia
Lusaka, Zambia
jackson.phiri@cs.unza.zm

***Abstract* - Today, insider attacks are the most hazardous threats faced by most organizations and is an overwhelming task to avert because, employees need legitimate access privileges to organisational resources for their daily works. If they misuse this trust accidentally or intentionally, it can cause breaches in the confidentiality, integrity and availability of the resource, thereby, negatively impacting the corporations' reputation, productivity and eventually finances. Using the Actor Network Theory (ANT) and the Theory Planned Behavior (TPB) as a foundation for research on user awareness and training backed with access control, this study, addresses information security related threats from insiders and ascertains the circumstantial factors that gives inspiration to insider threat lead behaviors as well as what exactly motivates an employee to attack their own employers. The findings of the research, enriches the body of knowledge by backing a theory that explains mitigation of information security threats by insiders using an adaptive awareness model. This study also affords a procedural groundwork for future research to account for insider threat factors while helping a broad range of organizations in mitigating insider threats.**

Keywords: Insider confidentiality, integrity, availability, ANT, TPB and Theory.

I. INTRODUCTION

Information Security has become an integral part of both public and private organisation's business processes, in maintaining the confidentiality, Integrity and availability of information, because ICTs play an important role in business operations [1][2]. Majority of these business and or organisations can no longer be imagined without the underlying digital systems and technological infrastructure for information handling [3]. Protection of information from unauthorised access and misuse, including resilience of the underlying ICT infrastructure to various sorts of attacks, has become one of the main technological challenges faced by business houses today [3][4]. This is because ICT has become more prevalent and complex, meanwhile the increase in the sophistication and volume of cyber-attacks by both insiders and outsiders are at an alarming rate [2].

A. Insider

An insider is an existing or former stakeholder with unrestricted access rights to sensitive organisational resources, who with or without intent compromise the resource security [3]. Insider threats are grouped into two categories including; malicious (intentional) and non-malicious (accidental) [3].

B. Threat

In information security threats are deemed to be any malicious act that attempt unauthorized access to organisational information, communication systems, network and or infrastructure, with or without the consent of the system or process owners. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet [3].

C. Malicious insider

A malicious insider is a current or former employee or any business associate who has or had access rights to the network system and intentionally abuse the same privileges in a manner that adversely affects the organisation's information systems confidentiality, integrity or availability [4]. Malicious insider threats includes; IT sabotage, Fraud and IP theft [5][6]. Basically, one does not become a malicious insider until they abuse their access rights and or committed a crime [7]. They are simply an insider, however, it is worthy probing the track taken from being an insider to malicious insider [8].

D. Non Malicious

These insider threats includes; unintentional, voluntary rule breakers, self-benefiting without malicious intent [3]. These are insiders who can cause damage to an organisations resources by their actions unintentionally, through negligence, ignorance and lack of training and or awareness. Insiders are capable of incidentally putting the organisational information at risk due to the fact that the accepted work processes they operate, are risky or simply because there are no right tools in place or the right training and awareness has not been provided. For instance, it may be a common practice that employees put alternative email addresses on their business cards and also carbon copy their work to themselves on these consumer grade web based email systems including Yahoo, icloud, Hotmail or Gmail. They can also share documents with others using personal storage solutions like Google drive,

Evernote, Icloud, Dropbox. These personal Internet hosted systems takes the organisational resources beyond the system of control which can put it at risk of compromise [8]. There is also a substantial impact from unintentional acts such as sending sensitive documents to a wrong recipient, as well as less-frequent mistakes by system administrators and programmers [8].

The Computer Emergency Response Team (CERT) states that, non-malicious insiders cause ICT security incidents accidentally for different reasons that includes; human error, lack of user awareness, drugs, fatigue, stress, moods, gender issues, drugs, age and or cultures. These accidental threats are referred to as "Unintentional Insider Threat (UIT)" the most common examples includes security incidents, which insiders can cause such as excessive access rights being granted to wrong users, introducing vulnerabilities during software development when Systems Development Life Cycle (SDLC) steps are bypassed, leaving an unencrypted portable storage device unattended to, system configuration errors, inactivating security controls [8].

These risks are aggravated when the attack is targeting a specific individual or organisation, they are referred to as an Advanced Persistent Threat (APT). These are created to specifically enhance the success of the likelihood by impersonation, where 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 a security breach unintentionally [8].

II. BACKGROUND

In the recent past, organisational insider attacks has grown exponentially. Take for instance, in 2007, a study by KPMG reviewed that only 4% of the total recorded cyber incidents were instigated by malicious insiders [9]. Three years later the figure increased to 20% and 2013, Verizon's extensive review stated that 69% of information security incidents were ascribed to insider threats [2]. The growing dimension of threats to insider can be evidenced by the revolution of internet and the growth of Internet of things (IoT). However, knowing what exactly motivates inside threats is the right path in finding a strategic solution of how to mitigate the problem to an acceptable level [10].

One of the well-known insider related cyber-attack of a growing spectacle involved Target in 2013, in which 40 million customers' credit card number and about 70 million of personal data was stolen by cyber criminals. This incident saw the Chief Information Officer (CIO) and Chief Executive Officer (CEO) out of employment as well as company reputation for competitive advantage [10]. The worst case scenario is that, despite the fact that the perpetrators were outsiders, the accessed the system using credentials of an insider being one the organisations refrigeration's vendors [9]. Considering the fact that every business house has its trusted employees, business associates, contractor, vendors and all related stakeholders, with whom corporations do business with and are have access to the systems and high opportunity. If not well mitigated, they may cause so much damage or harm to the corporation. According to a review of the Danger from within by Harvard Business review, it is clear that most organisations admit that they don't have enough security controls to detect, prevent and mitigate insider attacks due to the fact they are yet to accept the degree of the Risk [10]
Insider threat which is motivated by the technology complexity and Internet of Things (IoT) as stated above is growing by the day cannot be left unattended to. This is the simple most reason behind this study [10].

Insider threats are a progressive attack vector that requires an integrated defense-in-depth strategy due to the intricacy of technology and human beings today, this makes handling insider threats, one of the most critical challenges in addressing Information Security. This calls for a lot more than just technology alone, but an integration of people, processes and technologies. An insider threat is considered to be the most difficult threat to detect, prevent and mitigate due to the fact that an insider has access to systems and is a trusted agent with knowledge that can be leveraged to exploit a system, privileges that an outsider does not have.

A statement by Dr Eric Cole in the SANS survey report of 2015 states that [11]: "Preventing insider attacks is important and a key part of security; however, organizations often fool themselves into believing that they can stop all such attacks. Repeat the following sentence three times: "Your organization is and will be compromised by insiders." Insiders, whether malicious or merely negligent, are a continuous and constant problem for IT security; thinking otherwise is naïve."

Looking at the number of researchers who have labored so much in the past in search of the solutions to mitigate insider threats from various countries confirms that insider threat is a global problem that requires considered efforts to mitigate [12][13][14][15][16]. Needless to say, Zambia is not an exception and hence the reason to address this common problem.

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 both in real time and historically, such monitoring becomes an overwhelming challenge in an absence of effective ICT security controls that requires coordinated efforts to implement.

Insider Threat Mitigation has not been fully catered for in most organisations, leaving ICT assets vulnerable which could lead to organization's loss of revenue, organisational reputation, embarrassments, Compromise of organizational networks, forced strategic goal shift, loss of information, legal fines and loss of competitive advantage. The issue can continue and be costly to the organization if not attended to, because compliance to the inadequate security controls in place particularly to do with Insider threats is not easy to achieve due to the absence of the required policies. This is because most of the organisational implementations of Information Security Management Systems (ISMS), such as International Standard Organisations (ISO) 27001, are conventionally focused on preventing external attackers by protecting the digital perimeter, access management, policy compliance and managing vulnerabilities [16].

Recent surveys showed that internal fraud risks, being an area that has long been managed using forensic data analytics,

had been ranked as the top use case at 77%. While Cyber breach and sabotage is ranked the second-highest risk area use case at 70% [17, 18]. It is therefore, common knowledge that internal attackers, generally accounts for approximately more than half of the risks that an organisation is exposed to whist the external threats accounts for approximately above a third of the risks despite the gravity of the external consequences to an organisation [19].

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 be of high priority for all organisations.

All employees have a degree of trust invested in them by their employers and have been granted physical and logical access to the organisation's Information and Communications Technology (ICT)s, in order to fulfil their duties. Most of these employees are gratefully honest, however, there also exist the risk that some will abuse their inside position to commit crimes against their organisations [20][21]. These threats can take the form of a malicious employee downloading sensitive or confidential information and divulge to the public domain, or an unhappy employee destroying data before quitting. In April 2008, an insider at the Sumitomo Mitsui Banking Corporation in London, gained access to the bank's computer network in an attempt to pull off what would have been the biggest bank theft in the UK [22].

Insider Crimes and Motivation behind insiders to attacks

One would wonder what exactly motivates an employee to attack their own employers. The probable impact of an insider crime arrays from trivial irritant to the disastrous in ratio, which can feasibly have an outcome of bankruptcy, death, regulatory contempt, environmental adversity, countered weapons systems, damage of reputation, loss of customer confidence, incurred legal costs, collapsed stock market among others [23].

The five known main categories of insider crimes being, Facilitation of 3rd party access to sites/information, Unauthorised disclosure of information (either to a third party or the media), financial and process corruption (defined as illegitimately altering an internal process or system to achieve a specific, non-authorised objective), Sabotage (electronic or physical) and theft of materials or information. These are re-organized in three main categories which summarize the five categories above including: IT sabotage, Fraud and Theft of Intellectual Property (IP) [11]

A. IT sabotage

These are incidents with which an insider uses ICT to direct specific harm at an individual or organisation. Some of the recorded means for misuse of organisational information by potential insiders includes but not limited to printing, emails, copiers, web posts, blogs, and social media chats [12].

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 disaffected with their company, boss, or co-workers, including dissatisfaction with compensation, arguments with co-workers, reprimands, or job termination [7] [23]. Additionally hostility can arise when employees feel underappreciated, stressed, overworked, unfairly treated and or isolated such that they exert their anger or revenge by performing an inside attack[9]. Sabotage is usually executed by employees with high technical skills and access to critical assets, like ICT technologist, engineers and System Administrators who have the ability to cause implausible damage. Mitigation is the process of reducing the threat and or risk to an acceptable level considering an organisations risk appetite [23].

B. Fraud

These are incidents with which an insider uses ICT for the unauthorised modification, of an organisation's data for personal gain, or information theft that leads to an identity crime. Fraud motivated by financial gain is 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 [13].

C. Theft of Intellectual Property (IP)

These are incidents with which an insider uses ICT to steal proprietary information of an organisation. Theft of intellectual property is usually motivated by business 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 only was predictable to be costing $250 billion per year, despite the fact that it wasn't specified to what extent insider action contributed to the figures. The correct figure might not be known because most of the organisations do not realize when they have been compromised, and majority of the few that are aware do not report the attacks for fear of losing customer confidence and competitive advantage [13].

A vital note from the CERT research states that it's prudent to look at these three crimes unconventionally and conspicuously because their nature, as well as the mechanism for detection and prevention, can be diverse. For instance, about 24% of IT sabotage incidents are usually committed by system administrators and engineers mostly after termination of contracts, whereas 16% of IP theft incidents are usually committed by those whose job, once had something to do with that IP then 44% of Frauds are normally committed by lower management employees such as service desk, frontline and or customer services personnel [8].

III. LITERATURE REVIEW

This study addresses only insider threats and any aspect of outsider threats is out of scope. The insider threat problem necessitates an understanding of Actor ANT so as to know the connection between human and circumstantial factors being the technological, sociological and social-technical domains, in which they operate, considering the fact that technology alone can potentially intensify the problem than otherwise. This predicament has headed many researchers to study TPB and individual behavior, in an endeavor to manage insider threats. Despite the scholar efforts and the findings at an international level, no much efforts has been employed to address the Insider threat in Zambia to ensure that while the indispensable privileges are provided insider threats are also mitigated.

Some of the recorded means for misuse of organizational information by potential insiders includes but not limited to printing, emails, copiers, web posts, blogs, and social media chats etc. [18]. The Defense Personnel Security Research Center (DPSRC), has a record of numerous incidences by insider attackers among others including:

- *WikiLeaks:* The case for US Army soldier Bradley Manning who in his role as intelligence analyst, leaked through WikiLeaks organisation, the largest set of classified documents and videos to the public ever in the history of US military Army [18][21][24].
- *SCADA:* 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 programme on one of the organization's critical systems, after his contract termination, and damaged the SCADA system.
- *Cell Phone Clones:* 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.
- *POS System:* In a case of a secretary who worked at a youth organization for over 20 years used a point-of-sale system to issue at least 500 fraudulent refunds totaling over $300,000 to the insider's own bank account over a 5-year period.
- *Banking:* In case of a manager for a branch of a banking institution who stole over $225,000 from business accounts after running into family health problems, gambling and unforeseen expenses.

IV. METHODOLOGY

The researchers used questionnaires and interviews for data collection and assessments of the selected Company.

A. *Interviews:*

The interviewees were given the liberty of countenance on what they knew and felt about the current security controls in place in the organisation, in relation to the security of their Personally Identified Information (PPI) as well as that of the organisation

B. Questionnaires:

Extensive Questionnaires were generated in line with the required research information. The questionnaires design consisted of the ISO 27001:ISMS Annexure A domains that includes: Security Policy, Organization of information security, Asset Management, Human resources security, Physical and environmental security, Operations Security, Access Control, Information systems acquisition, development and maintenance, Information security incident management, Business continuity management and Compliance[25].

The obtained results were analyzed using Microsoft Excel for statistical values. An insider mitigation model concentrated on User awareness and access control was developed to address the negative impact of Actor Network Theory (ANT) and the Theory Planned Behavior (TPB) that leads to Insider Crime.

V. SUMMARY OF FINDINGS

This section describes a case study of a utility company in Zambia. The organisation serves an approximate of 1 million customers and seven thousand internal clients, including both commercial and residential. Financial and private information of the clients are processed, as well as the medical and personally identified information (PII) for the employees. This results in bulky financial, customer, medical and PII transactions where several billions of kwachas are involved. This organisation strives to focus especially on the confidentiality, integrity and availability of information.

As part of the high level assessment of the current state the following activities were performed. Then ISO 27001:2013 Annex A yielded the results in figure 4.

Fig. 1. Assessment activities

The assessment Clauses 4 to 10 of ISO 27001 as in figure 3.

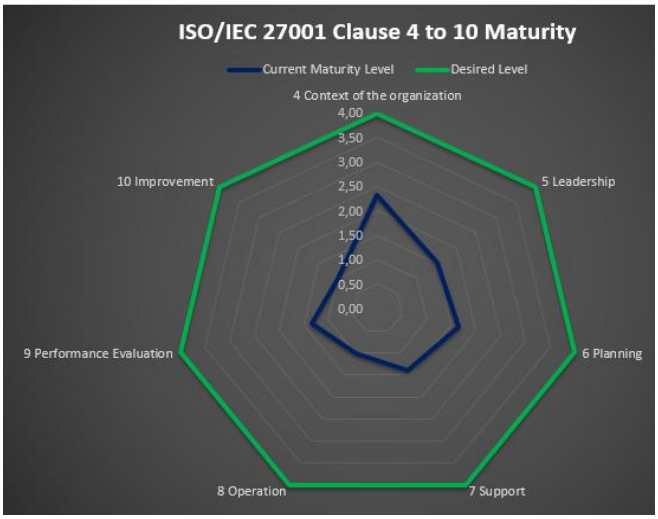

Fig. 2. ISO 27001 Assessment of clauses 4 to 10

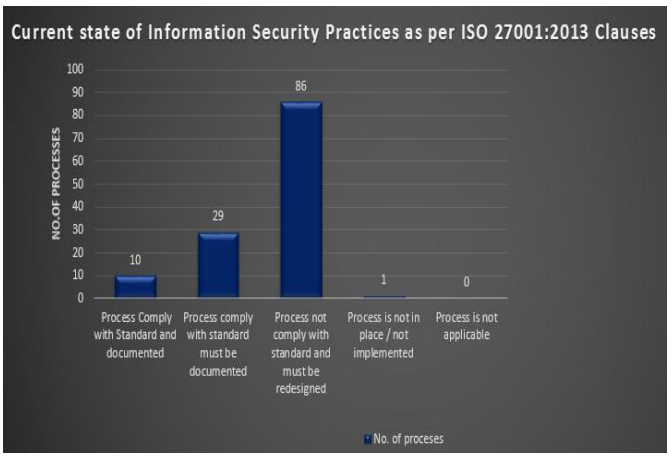

Fig. 3. Results: ISO 27001:2013 Clause 4 to 10 assessment

The organisation is precisely aware of the importance of information security and concedes the possible threat that are likely to be caused by insiders. The responsibility of the information security process lies with the Head of Cyber Security. There is a Cyber/ICT Security Policy that describes security norms and measures. The organisation needs improvements on the traditional requirements of the security departments' documents that would address the negative impact of ANT and TPB as it relates to Insider Crimes propagation. These documents includes: ICT Security strategy that aligns to the corporate objective, ICT Security procedures, Information classification procedure, information assets classification, incidence handling procedure, employee

screening policy, exit/leavers policy, Comprehensive Non-disclosure agreements and accompanying handling procedures.

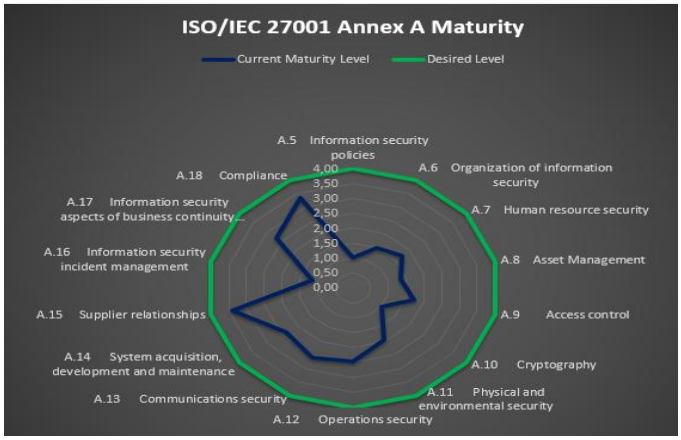

Fig. 4. ISO 27001 Assessment of Annex A Controls for maturity level.

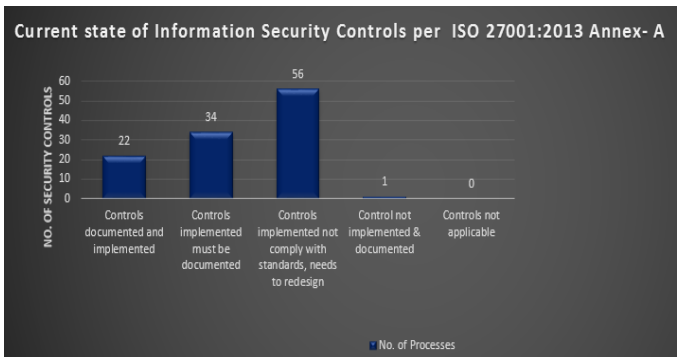

Fig. 5. Results of the current state of the ISO 27001:2013 Annex A

The organisation is implementing several measures and standard including ISO 2700, ISO 9001 and Control Objective for Information and Related Technologies (COBIT) 5.0. These standards needs compliance and minor improvements coupled with the need to be applied more consistently to decrease the number of insider threats. The standards also require that certain procedures, guidelines, policies and process flows be in developed, documented, approved and communicated to users continuously for awareness purposes, but was not the case in the utility company.

a) It was also noted during the baseline assessment that the access control policy is not fully implemented and complied with. This leaves the other source of the information being protected vulnerable, thereby making the whole infrastructure vulnerable to insider threats through ANT and TPB.
b) The utility Company has an approved information security policy, but the procedures are not in place. ICT Security objective has been developed but no Key performance indicator (KPI's).
c) There is a lack of alignment between information security and strategic ICT risk management. ICT Risk planning for assessments and treatment options are not clearly defined and documented. While many standards exist, the policies procedures and processes have not been completely documented and approved, leaving gaps for insider threat mitigation.
d) There is a lack of enforcing and incorporating information security controls as required by ISO 27001:2013 in various processes which includes architecture, incident management, change management, operations, access management, business continuity, human resource, physical security, asset management and project management.
e) The evaluation of information security performance and the effectiveness of the information security management system is not clearly documented or being performed. The utility Company's current ICT security product portfolio covers the minimal ISO 27001:2013 requirements and need to be reviewed
f) The above are the identified gaps in the existing policies, procedures and processes in the management of ICT security in the organisation leaving it vulnerable to the negative impact of Actor Network Theory (ANT) and the Theory Planned Behavior (TPB) that leads to Insider Crimes.

VI. DISCUSSIONS

Based on the findings above, it is clear that processed organisational information is not secure from insiders due to the lack of critical processes. Despite the fact that the organisation puts in efforts to prevent misuse of the critical data, there are spills that ends up in the hands of the unauthorised, because users are not aware of these controls.
The results of fraud, sabotage and espionage would not just result in direct loss or disclosure of information, but would also be devastating for the image of the organisation.

A. Mitigating and countermeasures

Although the ICT security department provides advice and implementation of measures to avert vulnerability exploitation by insider threat agents, below are the proposed steps of measures that must be considered in order to avert the insider threat with the top being User awareness.

1) *Pre-employment screening*: Necessities on integrity and confidentiality of insiders, both employees and externally hired personnel, must be applied. The insiders must sign a secrecy agreement and need a certificate of good conduct.
2) *Legally binding documents*: Currently, employee contracts should contain paragraphs that cover non-disclosure-requirements, non- compete-requirements or other statements on the confidentiality and integrity of the information that the organisation processes and users must be made aware on a continuous basis.
3) *Security education / awareness:* Employees must be informed about the rules of ICT security and integrity at entry into the their roles and on a continuous basis through trainings and broadcasted security tips
4) *Punitive Actions:* The consequences of being found to be an insider must be well spelt out and should be very grave so as to deter users from engaging in insider crimes and users must be made aware on a continuous basis.
5) *Access Control:* All access to both the systems and premises must be well structured and monitored with automated rules, and for system access, users well trained and aware, access should be Role Based and strictly monitored
6) *Revocation of authorizations*: There must be a checklist for functional changes and retirement of

personnel. Logical and physical authorizations are withdrawn at the latest on the last working day.

7) *Registration of information security incidents*: ICT security incidents must be registered, analyzed, watched over and reported to the persons in charge as stated the security guideline and users must be made aware on a continuous basis.
8) *Third party contracts:* In case outsourcing the services or activities, there is need for the supplier to be made aware of the policies so as to comply with the stated procedure for information security.
9) *Guidelines for Information Security:* There is need for one central document that describes the rules for Information Security and users must be made aware on a continuous basis.

B. Reccommendations

We further recommend that senior management demonstrate leadership and commitment with respect to the information security management system by ensuring the ICT security strategy and objectives are established, enforced and monitored. All the missing ICT related policies, standards, processes and procedures need to be developed, implemented, enforced, complied to, updated regularly and communicated to the users.

There is need to define, approve and apply an ICT security risk assessment process that establishes and maintains information security risk criteria. Management need to ensure that information security is an integral part of all processes throughout the organisation when it comes to the management and protection of company information, for to achieve its information security objectives.

A comprehensive user security awareness program for employees, customers and business associates need to be implemented to raise awareness of information security, social engineering and Cyber/ICT-crime. There is also need to implement a comprehensive, robust, effective and continual information security program and be able to evaluate the information security performance and the effectiveness of the information security management system.

VII. CONCLUSION

Considering the criticality of the utility service provisioning to the nation, and the required privacy of Customers and PII that the organisation processes, the identified gaps confirms that the organisation is vulnerable to Insider threats. The current implemented information security solutions and controls are not effective and well alignment to the ISO 27001:2013 required technical solutions. Senior management needs to assure total support in the implementation of the ISMS and compliance to the requirements of the adopted international standards and frameworks. All aspects of ICT security reporting, needs to be significantly enhanced to raise focus and inculcate a culture of high awareness of information security.

VIII. REFERENCES

[1] J. I. Agbinya, N. Mastali, R. Islam and J. Phiri, "Design and implementation of multimodal digital identity management system using fingerprint matching and face recognition," 7th International Conference on Broadband Communications and Biomedical Applications, Melbourne, VIC, 2011, pp. 272-278. doi: 10.1109/IB2Com.2011.6217932

[2] Memorie Mwanza and Jackson Phiri, Fraud Detection on Bulk Tax Data Using Business Intelligence Data Mining Tool: A Case of Zambia Revenue Authority, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016, ISSN (Online) 2278-1021 ISSN (Print) 2319 5940.

[3] Insiders and Insider Threats - An Overview of Definitions and Mitigation Techniques by Jeffrey Hunker Jeffrey Hunker Associates LLC & Christian W. Probst Technical University of Denmark

[4] D. Cappelli, A. Moore, and R. Trzeciak, the CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). NJ, Addison-Wesley, 2012.

[5] Common Sense Guide to Mitigating Insider Threats 4th Edition / December 2012 Technical Report/CMU/SEI-2012-TR-012 / (CERT Division of the Software Engineering Institute at Carnegie Mellon University

[6] Jacinda L. Wunderlich - Fall 2011 thesis -The Insider Threat

[7] Centre for the Protection of National Infrastructure (CPNI), managing the insider threat. CPNI. London, Security Industry Authority (SIA), 2013. EY 2016 Global Forensic Data Analytics Survey

[8] CERT, Unintentional Insider Threats: A Foundational Study. CERT Co-ordination Centre/SEI, Pittsburgh, 2013. http://www.sei.cmu.edu/reports/13tn022.pdf Accessed on 11/07/2017

[9] https://hbr.org/2014/09/the-danger-from-within Accessed on 10/11/2017

[10] https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#2013767ee795 Accessed on 11/11/2017

[11] https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-37447 Accessed on 11/11/2017

[12] Detecting Malicious Insider Threat in Cloud Computing Environments by Nikolaos Pitropakis of University of Piraeus - Ph.D. Thesis Piraeus, 2015

[13] Managing Cybersecurity As A Business Risk For Small And Medium Enterprises by Stephanie K. Chak of John Hopkins University Baltimore, Maryland May, 2015

[14] C. Kabuya, J. Phiri, T. Zhao, Y. Zhang, "Metric Based Technique in Multi-factor Authentication System with Artificial Intelligence Technologies" in Future Wireless Networks and Information Systems, Springer Berlin Heidelberg, vol. 143, pp. 89-97, 2012

[15] An analysis of insider dysfunctional behaviours in an accounting information system environment by Mohd Saiyidi Mat Roni of Edith Cowan University - Doctorates Thesis 2015 October 2012

[16] Jackson Phiri, Tie-Jun Zhao, Johnson I. Agbinya, "Biometrics device metrics and pseudo metrics in a multifactor authentication with artificial intelligence", Broadband and Biomedical Communications (IB2Com) 2011 6th International Conference on, pp. 157-162, 2011.

[17] Mitigating the cyber threat from malicious insiders -A practical 10-step program to detect and tackle potential insider attacks by Jason Anthony Smith MSc (Royal Holloway, 2014) and William Rothwell, Abatis (UK)

[18] PWC & Info Security Europe - 2015 Information Security Breaches Survey results

[19] Forrester's Global Business Technographics Security Survey, 2015.

[20] 2015 InsiderThreat. (2015, March 19). Accessed on 22/09/2017, from http://www.vormetric.com/campaigns/insiderthreat/2015/

[21] https://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence Accessed on 22/09/2017

[22] IS Now - autumn 2009 –Insider Threats - BCS Magazine

[23] Christopher J. Callahan September 2013 Thesis - Security Information And Event Management Tools And Insider Threat Detection

[24] Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threats 3rd edition – version 3.1. CMU SEI,

[25] R. Trzeciak, Insider Threat Blog, The CERT Insider Threat Database, CERT Coordination Center/SEI, 2011. http://www.cert.org/blogs/insider_threat/2011/08/the_cert_insider_threat_database.html