International Journal of Scientific Research in _____ Research Paper
Computer Science and Engineering
Vol.6, Issue.6, pp.53-59, December (2018) E-ISSN: 2320-7639

The role of Cyber Security and Human-Technology Centric for Digital Transformation

Yakubu Ajiji Makeri

School of Computing and Information Technology, Kampala International University, Kansanga, Kampala

**Corresponding Author: yakubu.makeri@kiu.ac.ug,+256705843834*

Available online at: www.isroset.org

Received: 07/Dec/2018, Accepted: 22/Dec/2018, Online: 31/Dec/2018

Abstract- Force point's human-centric cyber security systems protect your most valuable assets at the human point; the development of the digital transformation in the organizations has become more expanding in these present and future years. This is because of the active demand to use the ICT services among all the organizations whether in the government agencies or private sectors. While digital transformation has led manufacturers to incorporate sensors and software analytics into their offerings, the same innovation has also brought pressure to offer clients more accommodating appliance deployment options. So, their needs a well plan to implement the cyber infrastructures and equipment. The cyber security play important role to ensure that the ICT components or infrastructures execute well along the organization's business successful. This paper will present a study of security management models to guideline the security maintenance on existing cyber infrastructures. In order to perform security model for the currently existing cyber infrastructures, "Mobile devices and applications involves ensuring mobile devices and the applications used on these devices are secure and meet specified standards," he continues. "Enable features such as conditional access to ensure applications and data are kept secure and separate from personal information on user owned devices. combination of the some security workforces and security process of extracting the security maintenance in cyber infrastructures. In the assessment, the focused on the cyber security maintenance within security models in cyber infrastructures and presented a way for the theoretical and practical analysis based on the selected security management models. Then, the proposed model does evaluation for the analysis which can be used to obtain insights into the configuration and to specify desired and undesired configurations. The implemented cyber security maintenance within security management model in a prototype and evaluated it for practical and theoretical scenarios. Furthermore, a framework model is presented which allows the evaluation of configuration changes in the agile and dynamic cyber infrastructure environments with regard to properties like vulnerabilities or expected availability. In case of a security perspective, this evaluation can be used to monitor the security levels of the configuration over its lifetime and to indicate degradations.

Keywords- Cyber Security, Human technology, digital transformation

I. INTRODUCTION

The development of Information Communication Technology (ICT) infrastructure had growth which is very fast in producing a wide range of computer products cause some medium sized organizations are confused and ambiguous as to what should be done to the ICT infrastructure. This resulted in tragedy 'white elephant' where infrastructure is purchased by the organization were not fully utilized or not used at all especially for ICT security infrastructure. This ambiguity is likely due to the lack of control or it does not give the impression and clear benefits to business activities and organizational management.

Thus, the ICT infrastructure needs of a medium-sized organizations will be discussed to overcome this problem is not clear. Plans are made to the infrastructure of ICT is not simply to facilitate commerce and organization but it must be in line with the mission and objectives of the organization. Such planning should be in terms of ICT needs of an organization. Next, it seeks to be implemented and operated well for the success of an organization, whether it is for profit or social based service. ICT security maintenance is very important aspect in ICT infrastructure to identify any weaknesses which involved security breach in the some organizations at early time. At the same time, some key concerns have also emerged about security maintenance in IT services and infrastructure, which currently are viewed as significant barriers to its fast and wide-spread adoption. According to an IDC survey of CIOs consecutively in 2008 and 2009, security, integration and reliable performance ranked among the top concerns expressed. An ENISA (European Network and Security

Administration) survey of Small and Medium Business (SMBs) also confirms that major concerns for SMBs migrating to the ICT service or infrastructure include the confidentiality of their information and liability for incidents involving the infrastructure. This is understandable, because each of these factors have a major influence on the enterprises bottom-line. Similarly, availability of the ICT services platform with good performance and depends heavily on the quality of network characteristics, especially the round trip delay or latency. Security is a key concern, because confidentiality, integrity, authenticity and auditability of business data, tools and transactions are critical requirements for businesses to stay functional, legal and competitive. This need is especially critical for all users especially for overall security maintenance in IT service and infrastructure.

II. ISO NETWORK MANAGEMENT MODEL

Management of operational security maintenance in ICT infrastructure must adopt a management model such as ISO network management model. ISO network management model is a five functional area of network management that developed by The International Organization for Standardization (ISO). It provides a design guideline for future implementation of network management tools and technologies. Five functional area of network management consist of Performance Management, Configuration Management, Accounting Management, Fault management and Security Management. Performance management functions in ISO network management model is to monitor, assessment and review of the available bandwidth and network usage of resources in a network to make more efficient to run. Performance management is a very important part of the ISO network management model, especially for ICT infrastructure that wants to streamline network performance in the organizations.

The goal of Configuration Management functions in ISO network management model is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed. It will centrally monitor configuration aspects of network devices such as configuration file management, inventory management and software management.

Accounting management functions in ISO network management model is the process to use in measuring network utilization parameters so that individual or group users on the network can be regulated appropriately for the purposes of accounting or chargeback. Same as the performance management, the first step toward appropriate accounting management is to measure the utilization of all important network resources. This aspect of network management usually focusing on Internet service providers to bill customers for the resources they use. Fault management in ISO network management model is similar on what most people think that the administration thinks to manage the network. The goal of this network management functional is to identify, detect and alert system administrators of problems that may affect the system operations. Then, it needs to fix network problems primely in automatically to keep the network running effectively. Any faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management.

The goal of security management ISO network management model is to control access to network resources according to local guidelines so that the network cannot be sabotaged whether in intentionally or unintentionally. Implementation of security management subsystem it seems like can monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes. Security management deals with controlling access to resources. Then, notify the competent authorities if some resources are available. Similarly like a network operator or e-mail outsourcing, if a resource fails, management systems can be used to access the network to send messages when certain files or routers, servers.

It security management

The definition of Information Security based on ISO/IEC 17799:2005 is “preservation of confidentiality, integrity and availability of information, in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved”. Information has many definitions as follows:

(i) Information is about someone or something consists of facts about them.
(ii) Important or useful facts can be obtained as output from a computer by means of processing input data with a program.
iii) Information is an asset which is like other important business assets which is has value to an organization and consequently needs to be suitably protected.
(iv). Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films or spoken in conversation.

The core elements of information security management are to ensure the information assets, namely the following aspects.

(i) Confidentiality
(ii) Integrity
(iii) Availability

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities,

or processes. Some examples of breach of confidentiality are "Unauthorized personnel can read the classified documents", "Remote access to the system without approval", and "Shared folders without consent of the owners".

Integrity separates into data integrity and system integrity. Data integrity means the property that data has not been altered or destroyed in an unauthorized manner [6]. System integrity means the property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system.

The definition of Availability is the property of being accessible and usable upon demand is obtainable from an authorized entity.

Security of Information Technology Infrastructure Maintenance

Upon the successful implementation and testing of a new and improved security profile, an organization might feel more confident of the level of protection it is providing for its information assets. By the time the organization has completed implementing the changes mandated by an upgraded security program, a good deal of time has passed.
In that time, everything that is dynamic in the organization's environment has changed. Some of the factors that are likely to shift in the information security environment are:

• New assets are acquired.
• New vulnerabilities associated with the new or existing assets emerge.
• Business priorities shift.
• New partnerships are formed.
• Old partnerships dissolve.
• Organizational divestiture and acquisition occur.
• Employees who are trained, educated, and made aware of the new policies, procedures, and technologies leave.
• New personnel are hired possibly creating new vulnerabilities.

If the program is not adjusting adequately to change, it may be necessary to begin the cycle again. That decision depends on how much change has occurred and how well the organization and its program for information security maintenance can accommodate change. If an organization deals successfully with change and has created procedures and systems that can flex with the environment, the security program can probably continue to adapt successfully.

The CISO determines whether the information security group can adapt adequately and maintain the information security profile of the organization or whether the macroscopic process of the SecSDLC (Security System Development Life Cycle) must start a new to redevelop a fundamentally new information security profile. It is less expensive and more effective when an information security program is designed and implemented to deal with change. It is more expensive to reengineer the information security profile again and again.

Management model must be adopted to manage and operate ongoing security program. Models are frameworks that structure tasks of managing particular set of activities or business functions. With that, by assist the information security community to manage and operate the ongoing security program, a management model must be adopted. In general, management models are frameworks that structure the tasks of managing a particular set of activities or business functions.

A maintenance model is intended to complement the chosen management model and focus organizational effort on maintenance. This figure 1 diagrams a full maintenance program and forms a framework for the discussion of maintenance that follows.

• External monitoring
• Internal monitoring
• Planning and risk assessment
• Vulnerability assessment and remediation
• Readiness and review

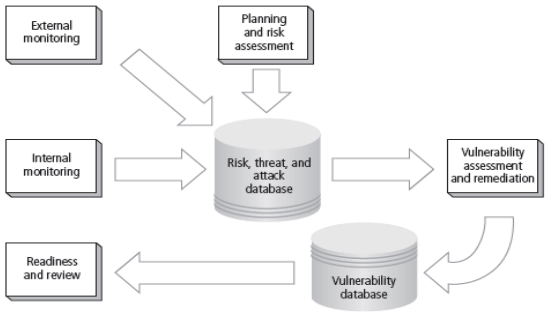

Fig.1. The maintenance model

III. TYPES OF SECURITY THREATS AND RISKS

Generally, ther
e are three types of risks that threaten the security of data in the form of digital environment or IT infrastructure which are vulnerability, threat and attack. In the beginning, all the vulnerability and threats are occurring passively in information technology infrastructure. However, it is necessary to solve and overcome this passively weaknesses and threats before it becomes as an active mode. The attack is represents as a risk that is occur in actively. Further following discussion is about each type of risk that is capable of threatening the security of the information technology infrastructure. All the risks can go beyond the

data security which is very valuable to an organization or company such as in Figure 2.

1. Vulnerability is anything that is weaknesses occur in used of information technology infrastructure and services. This vulnerability can be existing in many situations such as in design, configuration, implementation or management of information technology infrastructure that makes it vulnerable to the threats. The downside is what makes information technology infrastructure vulnerable to the information loss and downtime issues or down time.
2. Threat in the cyber world is anything that can be interferes with the operation, function, integrity, availability of all types of IT infrastructure and services. Threats can be occur in any type of form. Threats can be happen as an evil action by those who are not responsible or by accident due to natural events or human errors.
3. Attack is the particular technique used to exploit the existing weaknesses that occur in information technology infrastructure. For an example is a type of threat as a denial of service or DoS. Actually, this weakness exists in the design of operating systems and a type of attack that can be done due to the weaknesses is an attack called Ping of Death attacks. There are two main categories of attack which is passive attack or active attack.

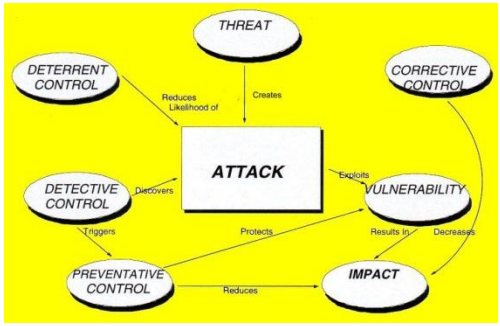

Fig. 2. IT Security Risks

Information security management model review

ICT infrastructure security is a state which protects a system or object from risk. It consists of systems, operations and internal controls in order to ensure the confidentiality, availability and integrity of data, knowledge and ICT infrastructure of an organization. User's roles in ICT systems have evolved from IT specialists for accessing information facilities, non-IT personnel for daily operation, unspecified individuals which is interested parties from outside organization.

Establishment of organization information security policy (ISP) is the first step to protect organizations from security threats. Figure 3 summarized procedures for building a set of ISP through the comparison of six standards in information security management standard.

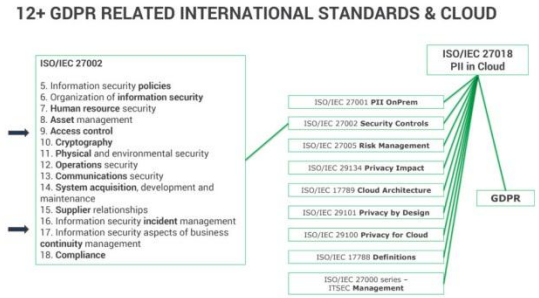

Fig.3. International standard for Information Security Management Model

As a pioneer, UK Department of Trade & Industry (DTI) firstly developed Code of Practice (CoP) PD0003 on information security in September 1993, with the assistance of a group of leading UK organizations. This Code of Practice was later retitled and published as BS 7799 Part 1 "Code of Practice for Information Security Management" in February 1995 by British Standards Institution (BSI). BS 7799 provides a common basis for developing organizational security standards and effective information security management practices. It enhances confidence in inter-organizational dealings.

Then, a new standard BS 7799 Part 2 "Information Security Management System –Specification with guidance for use" was released in 1998. The structure of this standard was the same as Part 1, in addition to defining a Code of Practice based on a set of key controls. As BS7799 was a theoretical control standard and not a technical standard of practice, it might not solve ISMS problems effectively. Therefore, ISO further developed ISO/TR 13335 (Information Technology – Guideline for the Management of IT Security) and ISO/IEC 18044 (Information Security Incident Management) standards (ISO/IEC FDIS 17799:2005; ISO/IEC 27001:2005 [15]. Both standards are helping ICT industry to implement information security management.

A scheme for accreditation of BS 7799 entitled "c:cure" was launched at InfoSecurity 1998 by UK Accreditation Certification Service (UKAS) and the British Standards Institution (BSI).

The accreditation procedure for ISO 9001 was adopted such as independent accredited certification body required for the purpose. This scheme initiated the further adaptation from national standard (BS) to international standard (ISO). Following the revisions of BS 7799 part 1 in 1999, the standard was transferred to ISO/IEC 17799:2000 (Part 1) – Code of Practice for Information Security Management. Finally, ISO/IEC 27001 Part 1 and Part 2 were issued in

2005, making them official and recognized standards both locally and internationally [16]. ISO/IEC 27001:2005 is directly related to the original BS 7799.

ISO/IEC 27002:2005 is a generic and advisory document, not a formal specification standard.

It provides a well-structured and comprehensive set of controls to address information security risks, covering confidentiality, integrity and availability aspects. Organizations that adopt ISO/IEC 27002 must assess their own information security risks and apply suitable controls, by following the standard for guidance.

ISO 27001

ISO 27001 is an International Standard which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) of an organization's overall business risks. ISMS is designed to ensure the selection of security controls is adequate and proportionate so as to protect information assets of the organization and give confidence to their customers.

ISO/IEC 27001:2005 (Information Security Management System Requirements)

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. This standard is generally applicable to all types of organizations, including business, enterprises, government agencies, institution, healthcare and so on. The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has four phases:

1. Plan – Establishment of the ISMS. The first step is to define risk assessment, in which risks shall be identified, analyzed and evaluated. Identification and evaluation of the risk treatment options are then followed. After the control objectives and controls are selected, management needs to approve residual risks and authorize implementation of ISMS.
2. Do – Implementation and operating the ISMS. Management actions, resources ,priorities, roles and responsibilities shall be defined in this step. It needs to determine the risk treatment plan to the respective risks, and to implement controls accordingly.
3. Check – Monitoring and reviewing the ISMS. Monitoring and reviewing procedures should be developed and executed. The effectiveness of ISMS and controls, as well as the risk assessment methodology and residual risks, should be included and reviewed.
4. Act – Maintaining and improving the ISMS. Implementing both preventive and corrective actions in this step could further improve the ISMS. It also enforces document and record control, and reviews information security incidents for lessons learning, so as to improve the ISMS. Often, ISO/IEC 27001:2005 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 and ISO/IEC 27002 assist in defining the requirements and outlining the most suitable information security controls for the ISMS respectively. However, no guidelines of risk assessment mechanism and ISMS implementation are included; those standards are only stated what is needed to do but it does not mention how to do.

ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

ISO/IEC 27002:2005 (replacing ISO/IEC 17799:2005 in April 2007) is an international standard that originated from the BS7799-1 standard originally laid down by the British Standards Institute (BSI) [18]. ISO/IEC 27002:2005 refers to a code of practice for information security management, and is intended to be a common basis and practical guideline for developing organizational security standards to facilitate the effectiveness of management practices.

By adopting the standard, an organization can address information security risks comprehensively. This standard consists of several guidelines and the best practices in 11 security domains shown as follows:

1. Security policy.
2. Organization of information security.
3. Asset management.
4. Human resources security.
5. Physical and environmental security.
6. Communications and operations management.
7. Access control.
8. Information systems acquisition, development and maintenance.
9. Information security incident management.
10. Business continuity management.
11. Compliance.

Among these 10 security domains, a total of 39 control objectives and 133 best practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.

ISO/IEC 13335 (IT Security Management)

ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard. It consists of a series of guidelines for technical security control measures:

1. ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.
2. ISO/IEC TR 13335-3:1998 provides the techniques for the management of IT security. It was superseded by ISO/IEC 27005:2008.

3. ISO/IEC TR 13335-4:2000 covers the selection of safeguards (for example technical security controls). It was superseded by ISO/IEC 27005:2008.
4. ISO/IEC TR 13335-5:2001 suggests management guidance on network security. It has been under review, and may merge with ISO/IEC 18028-1 and ISO/IEC 27033.Information security is a multi-dimensional discipline that can be viewed from different perspectives. The conceptual models are presenting security element relationship that shows how assets are potentially subjected to a number of threats. The threats and environment change over time and it may have impacts on the probability of risk occurrence. The model has been developed with the assumption of an environment containing constraints and threats that change constantly and are only partially known, including the assets of an organization, the vulnerabilities associated with those assets, safeguards selected to protect assets and residual risks acceptable to the organization.

IV. METHODOLOGY AND PROPOSED FRAMEWORK

The methodology of the proposed research will be carried out based on the fundamental of the experimental information technology method. This method examines the research work to demonstrate two important concepts: proof-of-concept and proof-of-performance.

To demonstrate the proof-of-concept, some important steps were performed. First, the research area within security maintenance is critically reviewed to provide the overview that leads to the justification of a valid research problem. Then, a novel model of the security maintenance framework is designed and analytically analysed. This includes the creation of the mechanism for managing security model, processes and metrics in relation to use of security maintenance.

Proof-of-performance is demonstrated by integrating the proposed security model, processes and metrics within a novel conceptual framework of the security maintenance in IT infrastructure. Then, it will be assessed using proposed framework. In those proposed framework, various parameters and workloads were used to examine and demonstrate the viability of the proposed solutions compared to other similar baseline solutions. Also, analytical analysis of some proposed security metrics is performed to evaluate the correctness.

Specifically, the main stages involved in the research are divided into three:

a. Data Acquisition Stage
b. Investigation and Modelling Stage
c. Analysis and Evaluation Stage

The proposed conceptual framework for security maintenance in mid-size IT infrastructure represents as an integration of IT security management model and concepts covering several facets of information security aspects and processes. The framework draws from multiple areas including software vulnerability, risk assessment, attack motivation, threat detection, deterrence and security objective. It is based on an earlier model for information security management model. The framework has been enhanced with the inclusion of combination of constructs and refined through the recalibration of IT security management model to ensure that potentially anomalous situations are prevented. The proposed framework is depicted as in Figure 4.

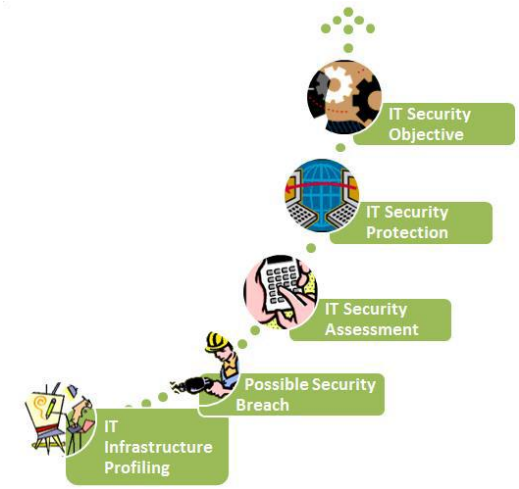

Fig. 4. Proposed IT Security Maintenance Framework

V. CONCLUSION

After review of information security management, this provides foundation knowledge and supporting evidences to develop a security maintenance model for ICT infrastructure. The development on Information Security Management System (ISMS) had a long development history in any organization and low adoption of ISO 27001 was observed. The high costs in money and time of ISMS implementation are definite barriers for smaller size companies to adopt the standard.

Therefore, a security maintenance model for ICT infrastructure based on putting the core and compatible requirements of ISO 27001 ISMS for reducing the redundancy of the existing usage of ICT security safeguards and aimed to reduce domain's barriers. The development of a security maintenance model for ICT infrastructure is proposed as a common framework and overcome the limitations of integrated system theory, as well as adopting the key concepts from IT security model.

Moreover, the PDCA approach was observed in ISO 27001 ISMS model. Combination of all the advantages in each model as example like understanding customer requirements, value-added processes, processes performance and effectiveness, continually improvement and others to develop the security maintenance model for ICT infrastructure.

A review on different approaches of IT security management model was performed such as ISO/IEC 27005:2008 and PDCA framework. This is combined with PDCA and IT security management model to fulfill ISO 27001:2005 standard. Lastly, the different implementation models for ISMS and IT security management model had reviewed. Actually, a novel conceptual framework of the security maintenance had proposed to make any IT infrastructures and services that follow those guidelines will accessible properly and secure by any authorized peoples. However, there are no security aspects had been discuss in details for IT services and infrastructure's maintenance. Then, the documentation had been provided as a manual access which is needs to follow the guidelines.

Now days, security should be concern in any IT services and infrastructures including in any proposed maintenance model and guidelines. Then, its need overall coverage to make the guidelines become more effective and easy to use. Security maintenance is more important in cyber space for any organizations especially for IT services and infrastructure usage in safe and secure manner.

REFERENCES

[1] J. May, Analyzing the socio-organizational constructs for IS security within organizations, in: S. Furnell, P. Dowland (Eds.), in: Proceedings of the 11th IFIP TC11. 1 Working Conference on Information Security Management, Richmond, VA, 2008.

[2] K.H. Guo, Y. Yuan, The effects of multilevel sanctions on information security violations: a mediating model, Inf. Manage.

[4] A. Simmonds, P. Sandilands, L.v. Ekert, An ontology for network security attacks, in: S. Manandhar, J. Austin, U. Desai, Y. Oyanagi, A. Talukder (Eds.), Applied Computing, Springer, Berlin, 2004,

[5] D. Trcek, Security models: refocusing on the human factor, Computer 39, 2006,

[6] M.d. Vivo, G.O.d. Vivo, G. Isern, Internet security attacks at the basic levels, ACM SIGOPS Oper.

[7] ISO/IEC 17799 (2005), Information Technology – Security Techniques – Code of Practice for Information Services, International Organization for Standardization, Geneva.

[8] J. Fonseca, M. Vieira and H. Madeira, "Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection," IEEE Transactions on Dependable and Secure Computing,

[9] C. Melara, J.M. Sarriegui, J.J. Gonzalez, A. Sawicka, D.L. Cooke, A system dynamics model of an insider attack on an information system, in: J.J. Gonzalez (Ed.), From Modeling to Managing Security: a System Dynamics Approach, Norwegian Academic Press, Kristiansand, Norway,

[10] C.E. Landwehr, Formal models for computer security, ACM Computer.

[11] D.L. Nazareth, J. Choi, Information security management: a system dynamics approach, Eighteenth Americas Conference on Information Systems (AMCIS- 2012), Seattle, WA, 2012, Paper 3.

[10] D. Trcek, Using system dynamics for managing risks in information systems, WSEAS Trans. Inf. Sci.

[12] M.E. Whitman, H.J. Mattord, Principles of Information Security, fourth ed., Course Technology, Boston, MA, 2014.

[13] M.A. Alnatheer, A conceptual model to understand information security culture, Int. J. Soc. Sci. Hum.

