Business Education Journal
Email: jeditor@cbe.ac.tz
Published Online November, 2015 in http://www.cbe.ac.tz/bej

DETERMINING APPROPRIATE SECURITY PROTECTION FOR ENTERPRISE INFORMATION RESOURCES

Respickius Casmir, Senior Lecturer, Department of Mathematics and ICT, College of Business Education, Bibi Titi Mohammed Road, P. O. Box 1968, Dar es Salaam, Tanzania,
Tel: +255-22-2150177, Mobile: +255 784 613198, Fax: +255-22-2150122,
E-mail: rescasmir@gmail.com

ABSTRACT

Information and Communication Technology (ICT) is increasingly becoming an integral part of our work, social, political, business, and private lives. Terminology such as mobile banking, mobile money, e-learning, e-procurement, e-commerce, e-ticketing, social media, Internet, blogs, intranet, extranet, e-books, telemedicine, web portal, management information systems, decision support systems, and the like are quite common in our daily lives. The fundamental element behind all these is ICT. The benefits of ICT are enormous and, indeed, ICT is continually affecting our day-to-day lives in a positive manner. Enhanced efficiency, effectiveness, transparency and operational costs reduction are some of the benefits of ICT. Despite the innumerable benefits of using ICT based tools and systems to support our business operations, there are numerous, yet ubiquitous security risks, threats and vulnerabilities associated with the adoption and deployment of ICT. As a result, private users, enterprises, business entities, educational institutions, government and non-governmental institutions are always in dilemma upon deciding which security mechanisms to go for, why and how to do it. This paper provides insight on how to overcome this challenge by presenting fundamental principles on how to properly determine your information security requirements and decide on suitable and cost effective security mechanisms in a given context.

Keywords: Information Resources, Security Risks, Threats, Vulnerabilities and Mechanisms

INTRODUCTION

Benefits of using Information and Communication Technology (ICT) based systems, tools and infrastructure to enhance efficiency, effectiveness and transparency in public and private business operations are inarguably enormous. Traditional manual business processes are increasingly superseded by computerized systems. Online business transactions (Ghosh, 2001; Prashar, Vijay, & Parsad, 2015) are becoming a de facto standard across all sectors of the economy worldwide. Terminology such as mobile banking, mobile money, mobile applications, e-learning, e-procurement, e-commerce, e-ticketing, social media, blogs, intranet, extranet, e-books, telemedicine, web portal (Prashar, Vijay & Parsad, 2015), management information systems, decision support systems, and the like are quite common in our daily lives (Garfinkel & Spafford, 1997; Swobodzinski & Jankowski, 2015). The Internet that literally means a global network is the cornerstone for the majority, if not all, of online business transactions. Looking at it from one perspective, the Internet facility is educative, informative, recreational, fun and most importantly a handy tool for sharing networked information resources, irrespective of distance, time differences and geographical boundaries between entities involved in a particular communication or business transaction.

On the other hand, security risks, threats and vulnerabilities to information resources (Viega & McGraw, 2002) are ubiquitous and continually evolving with the advancement of Information and Communication Technology. Meanwhile cybercrime is currently commonplace and new ways of exploiting unsuspecting victims in the cyber environment are discovered nearly on daily basis (Vakhitova & Reynald, 2014). The pace with which ICT advances by far outweighs the efforts made by information security professionals and experts in developing appropriate security mechanisms to overcome the emerging security threats and vulnerabilities (Gollmann, 1999). In addition, practitioners' demands and market forces usually necessitates a release and deployment of ill security tested ICT-based solutions and products. This increases security risks and creates ample avenue and potential for security attacks against information resources. The overall objective of this study was to identify challenges facing IT practitioners with regard to the protection of their information assets thereafter to outline guidelines on how to overcome such challenges.

This paper used Meta-analysis research methodology coupled with face to face interview to discuss and highlight the best ways in which an enterprise (public or private) can carry out a self-assessment

on its potential for security attacks and eventually protect its information resources adequately and in a cost effective manner (Layton & Watters, 2014). An enterprise in the context of this paper is an umbrella term including but not limited to the company, firm, organisation, corporation, establishment, office, bureau, agency, school, college, institution, or a department.

RESEARCH METHODOLOGY

This study employed both interview and meta-analysis research methodology which is an integral part of a systematic reviews procedure (Glass, McGaw, & Smith, 1981). In the former, unstructured interview method was used whereby 28 randomly selected Information Technology (IT) Managers from 28 public and private organisations were interviewed. The meta-analysis was used in this study to aggregate relevant information from multiple quantitative and qualitative research findings on information security implementation. Implementation of a meta-analysis method went through a series of steps.

First, a list of related research studies was identified. Secondly, scholarly publications and relevant studies whose content can significantly contribute to achieving the objective of this study were carefully chosen. At this stage, the eligibility of the studies was determined by identifying which studies to include and which ones to exclude.

The third step was to abstract data from the studies; and lastly, to analyze the data with respect to the objective of the study. The meta-analysis methodology was chosen on grounds that it would help the researcher achieve a higher degree for the measure of interest, as opposed to a less precise measure derived from a single study. The advantage of meta-analysis methodology is its objectivity, and yet like any research, ultimately its value depends on making some qualitative-type of contextualization and understanding of the objective data.

INFORMATION RESOURCES

One of the challenges that clearly emerged from the interviews with IT managers was an apparent ambiguity in identifying what constitutes information resources in an organisation. Nearly 70 per cent of the interviewees thought information resources were limited to data and application software. However, at higher levels of abstraction, information resources include people, processes and technology. On drilling down, information resources include hardware, software, network infrastructure, data, information, time and people that are involved in performing computing tasks (Gollmann, 1999). Information resources can also be likened to information assets. Therefore, the two terminologies shall be applied interchangeably throughout this paper. Data refer to known facts with implicit meaning and that when the meaning is explicitly assigned to these facts, and then data become information. From the security perspective, individuals, business entities, public and private institutions are more concerned with the security with which data and information are processed, stored and transmitted within and between computer systems than any other type of information asset. This is not only because data and information are highly valuable to the owners but also because if compromised it might be difficult, costly and sometimes impracticable to fully recover the data and information to its original or normal status (Brenton, 1999). Furthermore, technical security mechanisms which are required to protect information assets are quite sophisticated and its implementation requires highly skilled security personnel.

SECURITY ATTACKS

Another challenge facing IT practitioners was how to identify various types of security attacks and to determine appropriate security mechanisms against a given attack. About 78 per cent of the interviewees thought that a security attack always meant an intrusion into a computing system by an individual with malicious intention. Nevertheless, security attack is more than intrusion in to the computing system. Bishop (2003) defines security attack as any action that attempts to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an information asset. An attack is usually perpetrated by someone with malicious intentions and, if successful, results into compromising an information asset. Much as the majority of security attacks are technical oriented, some are non-technical such as social engineering attacks (Baase, 2002). Krombholz *et al* (2015) describe social engineering attacks as non-technical methods of intrusion attackers use to circumvent security mechanisms. It relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Technical oriented sorts of security attacks emerge in various forms including fabrication, interception, interruption and modification of data or information. When an attack involves some modification of the data stream or the creation of a false data stream it is referred to as an active attack otherwise it is a passive attack.

Agents of attacks or simply attacking entities are referred to as security threats that exploit vulnerabilities in a computing system resulting into security breach (Jackson, 2010). As has always been the case, security attacks emanate from outside as well as from within the target network. Unfortunately, 64 per cent of the interviewees thought attacks just originate from outside their network perimeters, something which is not the case. There are various motives and reasons for a given network to get attacked; therefore, when planning for an organisation network security one has to take into account many factors that make a network under consideration appealing for attackers.

Attacks from within

Experience has shown that majority of attacks originate from within an organisation or from someone with inside information such as an ex-employee (Jackson, 2010). Much as different security mechanisms such as firewalls and intrusion detection systems protect information assets from external attacks, it is the employees who know the internal workings including the network vulnerabilities.

These might be the ones responsible for compromising an organisation's network (Gollmann, 1999). One of the best ways to overcome attacks that emanates from within is to develop and implement a comprehensive and enforceable information security policy and procedures. Additionally, there is need for sensitizing and educating employees through security awareness programme at workplace on a continuous basis.

Attacks from outside the network

Attacks from outside the network may emanate from many diverse sources including disgruntled employees. In any case, someone gains in monetary terms or otherwise by staging an attack. In addition, external attacks may originate from the following sources (McNab, 2007; Brenton, 1999):

- Competitors, if you are in a highly competitive business;
- Individuals with a different point of view to your business, if your business is considered controversial (i.e. militant viewpoint);
- Random sources, if your business has higher visibility for notoriety gains (high profile);
- Internet service providers or email users, if your domain's mail system is used as a spam relay;
- Individuals with personal vendetta with one or more of the employees; and many more.

According to Pfleeger (2006), security attacks have always adverse effects on the computing resources regardless of the intention. That is, in the words of Panza as cited in Man of La Mancha (Pfleeger & Pfleeger, 2012), "it doesn't matter whether the stone hits the pitcher or the pitcher hits the stone, it's going to be bad for the pitcher." Adding that, an inadvertent error can cause just as much harm to the users and their data as can intentionally induced flaw. This means that an organisation needs to consider and protect itself against all possible sources of attacks to its computing resources.

INFORMATION SECURITY IN A BIGGER PICTURE

Information security, which is commonly referred to as 'IT Security' is all about controlling access to information resources using security mechanisms that provide various security services. Security services include authentication, authorisation, confidentiality, availability, integrity and non-repudiation. Any security mechanism offers one or more of the above mentioned security services. Security mechanisms protect information assets which are valuable to business operations against security threats and vulnerabilities that increase security risks. Security risks indicate security requirements that are met by security controls as illustrated in Figure 1 (adopted from Casmir, 2005). It is this security complexity that makes it harder for security professionals to successfully protect their respective networks and information systems; and somewhat easier for attackers to compromise those networks and systems. While security professionals strive to implement security controls on all potential security holes; attackers explore to find at least one window of vulnerability to compromise a network. This means that attackers rarely attempt to penetrate through tight security mechanisms such as firewalls and cryptographic systems instead they look for weaker parts in a security chain.

Experience has shown that people are the weakest part of all (Bishop, 2003; Gollmann, 1999). Social engineering tactics and its variant threat known as phishing (Shashidhar & Chen, 2015) are the most widely used techniques by attackers, especially, in places where technical security mechanisms are tightly secured. Social engineering tactics, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information (Gollmann, 1999). It is, literally, a type of confidence trick for the purpose of information gathering, fraud, or gaining unauthorised access to a computing system. From the technological perspective, software vulnerabilities (Viega & McGraw, 2002) are predominant compared to hardware faults. From the processes point of view, misconfiguration of security parameters and non-adherence to non-technical security controls are the most outstanding security challenges.

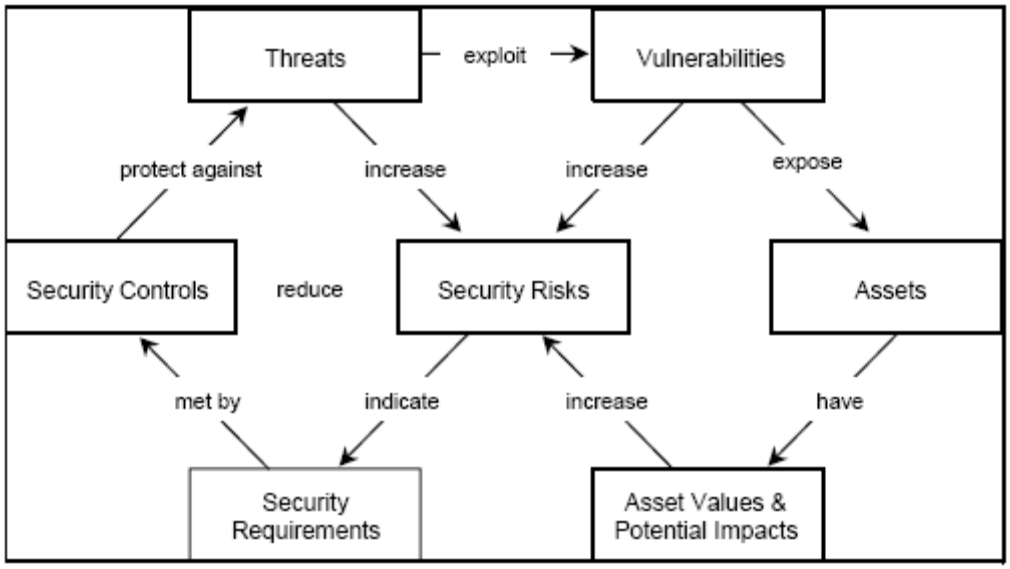

Figure 1: ***Security Complexity at Higher Abstraction*** adopted from Casmir (2005)

Effective security controls consists of both technical and non-technical aspects (Yngström, 1996; McNab, 2007). The technical aspects include all sorts of hardware and software security mechanisms such as antivirus software, intrusion detection systems, firewalls, demilitarised zone, access control list, mobile agents, cryptographic tools, and reference monitor. The non-technical aspects refers to the concept in operating systems architecture (Viega & McGraw, 2002) whereby a reference monitor defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g. processes and users) ability to perform operations (e.g. read and write) on objects (e.g. files and sockets) on a system (Gollmann, 1999). Security controls are, therefore, meant to deter, detect and recover from a security attack.

Non technical aspects of security controls include policies, procedures, guidelines, ethics, best practices, laws and regulations. Both technical and non-technical security controls are not only equally important but also must co-exist in an organisation for they complement each other. Implementing one at the expense of the other might lead to fatal security flaws.

Furthermore, Solyom and Bertram (2015) highlight on the five mistakes that organisations cannot afford to make as cited below:

1. *Failing to build cyber defences around a granular understanding of threat. Any cyber defence programme should be intelligence-led. That includes collecting operational and strategic*

information that helps the organisation understand the specific nature of the threat. It may be necessary to look up and down the supply chain, as vulnerabilities in subcontractors or suppliers often affect the organisation and vice-versa – attackers will target the weakest link.

2. *Over-focusing on prevention and not paying enough attention to detection and response. Organisations need to accept that breaches are inevitable and develop and test response plans, differentiating between different types of attacks to highlight the important ones.*
3. *Treating cyber security as an IT issue rather than a business risk. Many organisations accept that cyber security is a business risk, rather than an IT-specific issue – but not many act on this by integrating cyber security risk management with wider business risk management processes.*
4. *Failing to identify and protect the organisation's most important assets. Organisations need to focus budgets on prioritising protection. Many focus excessively on ensuring organisation-wide compliance to standards, without effectively protecting their most important assets.*
5. *Lacking the technical defences to deal with advanced persistent threats. Through 2015, an increasingly broad group of highly capable actors will target those critical assets across a wide range of organisations.*

[Source: *http://www.computerweekly.com/opinion/The-cyber-security-outlook-for-2015*]

From the above mentioned items, it is evident that proper planning is required if an organisation is to adequately protect its information resources as discussed in the subsequent section.

PLANNING FOR INFORMATION SECURITY REQUIREMENTS

Primarily, when planning for information security requirements one has to think like an attacker. This is achieved by performing a comprehensive security risk analysis (RA) and vulnerability assessment (VA) (Jackson 2010). Security Risk analysis (Xin & Xiaofang, 2014) in this context refers to the process of identifying various security threats and their potential of compromising information resources, whereas Vulnerability Assessment refers to the evaluation of a system susceptibility to threat scenarios. It is, therefore, imperative that a thorough security risk analysis and vulnerability assessment are successfully accomplished by accurately attempting and providing appropriate answers to the following key questions (Brenton, 1999).

- What information resources do I need to protect and why?
- From what threats am I attempting to protect these resources?
- Who may need to compromise my network and for what gain?
- How likely will a given threat compromise my information resources?
- What are the immediate costs should the information resources be compromised?
- What are the costs of recovering from an attack or system failure?
- How may information resources be protected in a cost effective way?
- Am I governed by a regulatory body that dictates the required level of security for my business environment?
- Who will be in charge of the security protection?
- Who else will be involved in the implementation of security apart from IT security provider?

Primarily, security risk consists of three elements namely an event, consequence and uncertainty (Caralli, Stevens, Young & Wilson, 2007) taken together; the three elements form a risk equation as illustrated hereunder.

Threat (condition) + **Impact** (consequence) = **Risk**

Much as there are several methods for performing Risk Analysis (RA and Vulnerability Assessment (VA) this paper recommends the use of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework (Alberts, Behrens, Pethia & Wilson, 1999). Security risks and

vulnerabilities are inherent in all the three principal components of information assets namely people, processes, and technology. The latter includes software, hardware and network infrastructure. According to Alberts *et al.* (1999), the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) are a framework for identifying and managing information security risks. It defines a comprehensive evaluation method that allows an organisation to identify the information assets which are important to the mission of the organisation, threats to these assets, and vulnerabilities that may expose these assets to threats. By putting together the information assets, threats, and vulnerabilities, the organisation can begin to understand what information is at risk. With this understanding, the organisation can design and implement a protection strategy to reduce the overall risk exposure of its information resources. As Alberts *et al.* (1999) explicate, OCTAVE examines organisational issues and technology issues to assemble a comprehensive picture of the information security needs of an enterprise; and that OCTAVE consists of the following phases:

- Phase 1: Build Enterprise-Wide Security Requirements
- Phase 2: Identify Infrastructure Vulnerabilities
- Phase 3: Determine Security Risk Management Strategy

The authors explain further that each phase of OCTAVE is designed to produce meaningful results for the organisation. This methodology works very well with nearly all types of organisations.

In addition, Caralli, Stevens, Young and Wilson (2007) introduce OCTAVE Allegro which is a variant of OCTAVE for improving Information Security Risk Assessment Process. In OCTAVE Allegro methodology, there are four distinct areas of activity which are carried out through eight steps as follows:

- Establish drivers, where an organisation develops risk measurement criteria that are consistent with organisational drivers.
- Profile assets, where the assets which are the focus of risk assessment are identified and profiled and the assets' containers are identified.
- Identify threats, where threats to the assets—in the context of their containers—are identified and documented through a structured process.
- Identify and mitigate risks, where risks are identified and analyzed based on threat information, and mitigation strategies are developed to address those risks.

The OCTAVE Allegro process is illustrated in Figure 2.

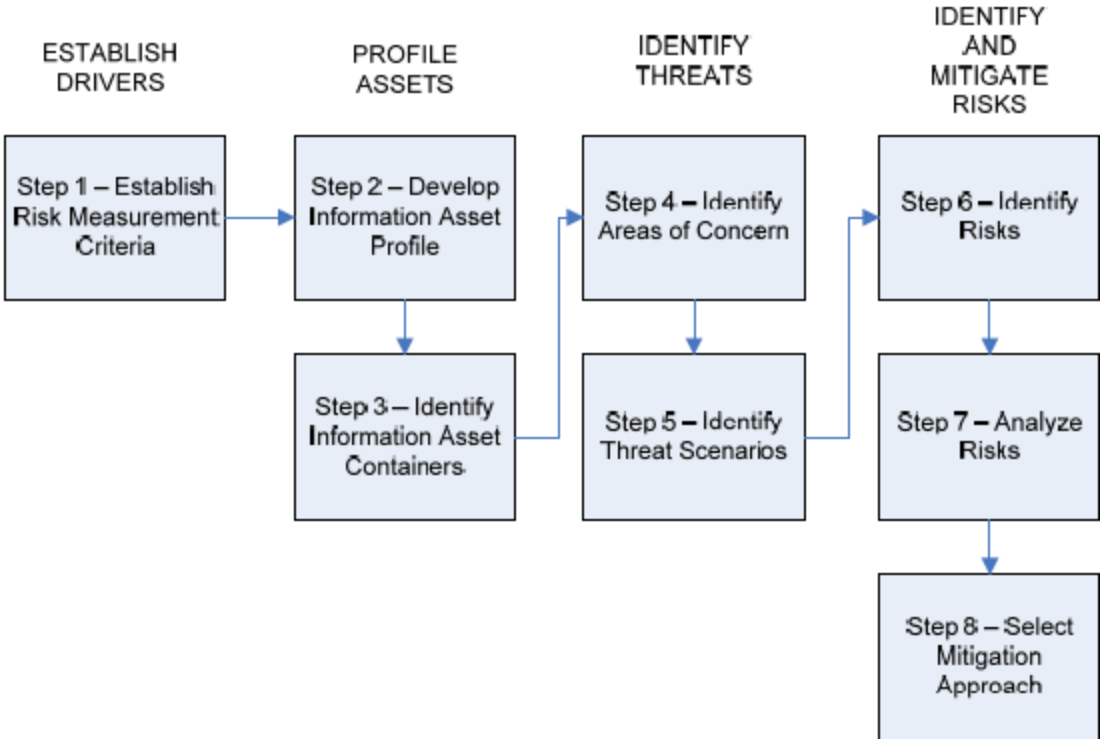

Figure 2: OCTAVE Allegro Roadmap [adopted from Caralli, Stevens, Young and Wilson (2007)]

Both OCTAVE and its variant OCTAVE Allegro are handy tools for security Risk Analysis and Vulnerability Assessment in an organization. However, OCTAVE Allegro methodology is mostly used in large or multilevel organizations. Most organisations around the world have found success in applying, tailoring and institutionalising the OCTAVE methodology.

It is unthinkable for one to commit funds for and invest considerably in acquiring various security mechanisms prior to performing a comprehensive security risk analysis and vulnerability assessment for this might result into uncalled for overprotection or ill-protection of the information assets as the case may be (Zhang, Yang, Li & Xiang, 2014). In either case, the cost of protecting an information asset should not exceed the value of the said asset (Gollmann, 1999).

Documenting findings

Findings from the security risk analysis (RA) and vulnerability assessment (VA) need to be properly analysed and documented (McNab, 2007). It is important to note that these findings, if properly analysed and documented, then they not only serve as input for developing a crosscutting information

security policy but they also serve as a basis for budgeting for one's security precautions. As a rule of thumb, the costs of security protection should commensurate with the value of the asset to be protected based on the results of the Risk Analysis and Vulnerability Assessment.

Developing information security policy and procedures

A security policy serves many functions. First, it is a central document that describes in detail acceptable use of information resources and the corresponding penalties for non compliance. It also provides a forum for identifying and clarifying security goals and objectives to the organisation as a whole. A good security policy shows the responsibilities for each and every employee and other stakeholders in an attempt to maintain a secure computing environment (Yngström, 1996). In addition, a good security policy must be:

- Consistent with other corporate policies;
- Accepted by network support staff, users, and all levels of management;
- Enforceable using existing infrastructure, systems and technical tools;
- Compliant with local, national and international laws.

In addition, according to the Organisation for Economic Co-Operation and Development – OECD (2003), the full potential of ICT remains unknown, and that it requires appropriate policies and continued monitoring of its impacts to seize its benefits. Furthermore, OECD (2003) proposes a number of key policy recommendations that are imperative if organisations are to reap the full benefits of ICT. A synopsis of the policy recommendations made is as follows:

1) Strengthening competition, by ensuring network infrastructure competition across and within different platforms, placing more emphasis on regulatory frameworks that are neutral with respect to alternative technologies.
2) Fostering appropriate business environment for effective use of ICT, whereby measures should aim at reducing obstacles to organisational change within enterprise; and strengthening education and training systems across all sectors of the economy.
3) Spreading the benefits of ICT across the economy, by removing sector-specific Regulations that affect the uptake of ICT, helping small firms assess the opportunities of e-business.

4) Boosting security and trust to enhance usage of ICT by business and consumers, by implementing information security guidelines, by developing a culture of security, and by strengthening cross-border co-operation and enforcement in privacy and consumer protection.
5) Supporting of the developing countries in seizing the benefits of ICT, by using development co-operation policies to integrate ICT into national development strategies and help create the right economic, legal and institutional environment for ICT investment and use.

If the abovementioned attributes are taken into consideration systemically and holistically chances are quite high that the computing environment will not only be fairly secure but also it will make enterprises reap the most from their investments in ICT and spend less on securing the computing systems.

CONCLUSION AND RECOMMENDATIONS

Information security is a process not a product; therefore, it is a context dependent phenomenon. In addition, security is usually meant for hedging shareholders' value. Given the complexity and multidisciplinary nature of security, each and every stakeholder has a role to play individually as well as collectively. In this case, if security controls are to succeed in an organisation, implementation of information security awareness and training programmes to all relevant stakeholders is inevitable. Since security threats and vulnerabilities are ubiquitous, training and re-training of all personnel that are involved in performing computing tasks should be given a priority it deserves.

It is only through security awareness and training programmes that organisations shall be able to effectively deal with all sorts of security threats and vulnerabilities including social engineering tactics. In terms of governance aspects, information security should be considered as one of the responsibilities of a governing body in a given organisation. It is, therefore, recommended that during the planning and budgeting sessions, intangible information assets have to be treated as one of the enterprise's strategic resources, that is, at par with financial and human resources. In addition, information security requirements for a given organisation must emanate from a comprehensive Risk Assessment (RA) and Vulnerability Analysis (VA) to see to it that the investment in the protection of information assets is commensurate with the value of the assets to be protected. It is only from the results of the RA and VA that an organisation can appropriately and adequately define protection profile for its information resources. Thus, value for money should always be the guiding principle when it comes to budgeting for and investing in information security.

REFERENCES

Alberts, C. J., Behrens, S. G., Pethia, R. D., Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework*, Version 1.0, TECHNICAL REPORT CMU/SEI-99-TR-017 ESC-TR-99-017

Baase, S (2002). A Gift of Fire: Social, Legal and Ethical Issues for Computers and the Internet. Prentice Hall, ISBN: 0130082155.

Bishop, M (2003). *Computer Security: Art and Science*, Addison-Wesley. ISBN 0-201-44099-7.

Brenton, C (1999). Mastering Network Security. SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. ISBN: 0-7821-4142-0

Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Software Engineering Institute, TECHNICAL REPORT: CMU/SEI-2007-TR-012 ESC-TR-2007-012

Casmir, R (2005). A Dynamic and Adaptive Information Security Awareness (DAISA) Approach. Universitetsservice US-AB, Stockholm, Sweden, 2005, ISBN 91-7155-154-9

Garfinkel, S. and Spafford, G (1997). Web Security & Commerce. O'Reilly & Associates, Inc.Sebastopol, CA, USA. ISBN:1-56592-269-7

Ghosh, A. K (2001). Security and Privacy for E-Business, John Wiley & Sons, Inc. New York, NY, USA. ISBN:0471384216

Glass, McGaw, & Smith (1981). Meta-analysis in social research. Beverly Hills, CA: Sage.

Gollmann, D (1999). *Computer security*. Wiley in Chichester, New York. ISBN 0471978442.

Jackson, Chris (2010). *Network Security Auditing*, Cisco Press. ISBN 978-1-58705-352-8

Krombholz, K., Hobel, H., Huber, M., and Weippl, E. (2015), Advanced social engineering attacks; *Journal of Information Security and Applications, 22*, 113-122; Special Issue on Security of Information and Networks; ISSN: 2214-2126

Layton, R and Watters, P. A., (2014); A methodology for estimating the tangible cost of data breaches; Journal of Information Security and Applications, Volume 19, Issue 6, Pages 321-330; ISSN: 2214-2126

McNab, Chris (2007). Network Security Assessment, 2nd Edition, O'Reilly, ISBN 978-0-596-51030-5

Organisation for Economic Co-Operation and Development (OECD) (2003). Seizing the Benefits of ICT in a Digital Economy.

Pfleeger, C. P. and Pfleeger, S. L. (2012). *Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach*, Pearson Education, Inc. ISBN 978-0-13-278946-2

Pfleeger, Charles P. (2006). Security in Computing, Fourth Edition, Prentice Hall ISBN: 0132390779.

Prashar, S., Vijay, T. S., & Parsad, C. (2015). Antecedents to Online Shopping: Factors Influencing the Selection of Web Portal. International Journal of E-Business Research (IJEBR), 11(1), 35-55. doi:10.4018/ijebr.2015010103.

Shashidhar, N. and Chen, L. (2015). An Indistinguishability Model for Evaluating Diverse Classes of Phishing Attacks and Quantifying Attack Efficacy, International Journal of Security (IJS), Volume (9) : Issue (2), Pages - 15 – 23, ISSN - 1985-2320.

Solyom, J and Bertram, S. (2015). The cyber security outlook for 2015, Computerweekly.com, http://www.computerweekly.com/opinion/The-cyber-security-outlook-for-2015 [Last accessed July 2015].

Swobodzinski, M. and Jankowski, P., (2015). Evaluating user interaction with a web-based group decision support system: A comparison between two clustering methods, Decision Support Systems and Electronic Commerce Journal, Volume 77, ISSN: 0167-9236, Pages 148–157

Vakhitova, Z. I. and Reynald, D. M. (2014). Australian Internet Users and Guardianship against Cyber Abuse: An Empirical Analysis, International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891, Vol 8 (2): 156–171

Viega, J. and McGraw, G. (2002). Building Secure Software: How to avoid security problems the right way, Boston: Addison-Wesley. ISBN 020172152X

Xin, T. and Xiaofang, B. (2014). A Hierarchical Information System Risk Evaluation Method Based on Asset Dependence Chain, International Journal of Information and Network Security (IJINS), doi:10.11591/ijins.v3i3.6137

Yngström L (1996). A systemic-Holistic Approach to academic programs in IT Security, Stockholm University/Royal Institute of Technology ISRN SU-KTH/DSV/R-96/21-SE.

Zhang, Z., Yang, L., Li, H., and Xiang, F. (2014). A Quantitative and Qualitative Analysis-based Security Risk Assessment for Multimedia Social Networks. *International Journal of Network Security*, *18*, (1), 43-51.