ISSN 2278-8808 SJIF 2014 = 4.889
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

A STUDY ON ISSUES ON PRIVACY, AVAILABILITY & INTEGRITY OF DEVELOPING CYBER SAFETY CHALLENGES SMES IN DEVELOPING ECONOMICS

Kadam Sandeep Uddhavrao[1] & Piyush Pandey[2], Ph. D.

Abstract

SMEs today continue to use networks and the Internet as vital business tools. SMEs are utilizing the opportunities offered by advances in ICTs to adopt innovative business operations, to offer user-friendly and competitive products and services, and to develop customer-centric strategies. While connectivity is indispensable for achieving business success, being connected also implies being exposed to a myriad of cyber-security challenges, such as vulnerabilities which when exploited can violate confidentiality, integrity and availability (CIA) security properties. As vulnerabilities are exploited by the numerous threats, SMEs are adversely impacted which in some cases may lead to business closure. The extent of cyber-attacks have increased in recent times and experts believe that if nothing is done about it, the severity of future attacks could be greater than what has been observed to date. The pace with which these vulnerabilities are introduced and dealt with is uncertain. This situation has necessitated the need for SMEs to have frequent vulnerability assessment. SMEs were surveyed and strategically interviewed on various cyber-security and business metrics.

Keywords: *Cyber Security, Challenges, SMES, Developing Economics, Issues, Confidentiality, Integrity & Availability, etc.*

Introduction:

Globally, SMEs have been defined in a number of different ways. Some definitions involve revenues, capital and staff strength. Interestingly, SMEs in developing countries are characterized by uncertain revenues. Coupled with that, most developing economies have fluctuating currencies. These challenges create uncertainties with any definitions involving monetary value; that is, the set of target SMEs population would vary with exchange rates. Cognizant of the above, the only common denominator is the number of employees [1]. So this study defined SMEs based solely on staff strength, which is also consistent with the norms applied in the case study countries. At least, this approach enhances the generalization of findings to some reasonable extent. Having so defined the SMEs in developing economies, the study focused on those who have embraced the information and communications technology (ICT) and the surge in doing business in the cyber-space.

This study discussed the perceived uncertainties in cyber-security vulnerabilities and threats, and used fuzzy linguistic variables to represent the real-life business environment decision-making approach to model assessment techniques. To address the increasing risk to SMEs in developing economies, the traditional risk equation is decontextualized into a fuzzy risk relational function, with fuzzy arguments of vulnerabilities, threats and asset value, to assist SMEs make better informed decisions. The elicited experts' opinions were used to model the risk function, using neuro-fuzzy techniques, that combines the human inference style and linguistic expressions of fuzzy systems with the learning and parallel processing capabilities of neural networks to analyze the cyber-security vulnerability assessment (CSVA) model.

Review of literature:

This study focuses on the perceived uncertainties in cyber-security vulnerabilities and threats, and uses fuzzy linguistic variables that represent the real world business situational multifaceted decision-making to model mitigation techniques. Usually, the CIA attributes are used as the benchmark for evaluating most information systems security or information assurance systems. Though, the ITU-T Recommendation stipulates eight cyber-securities attributes, there have been other attempts at presenting alternatives. Nevertheless, the convention has been the application or utilization of the confidentiality, integrity and availability (CIA) attributes as the fundamentals of any viable cyber-security endeavor [5]. This study thus concentrates on these three as well.

In this study, cyber-risk is seen as the possibility for loss of confidentiality, integrity and availability due to a specific threat on a given asset. By definition, cyber-risk is a fuzzy measure of the adverse effects that can result if cyber-security vulnerability is exploited. In other words, any time any cyber-security property is violated, there is the possibility of risk. Typically, cyber-security objective is to deter, prevent, detect, recover from, and respond to threats in cyberspace [2-4]. Cyber-security is to safeguard the information assets, the information systems and networks that deliver the information, from damage or compromise resulting from failures of confidentiality, integrity and availability.

Availability: implies that stakeholders expect to be able to access or send emails and to place orders when convenient for them, and the Internet connection is expected to be functional without disruption. These are examples of availability. Thus, Availability is the property that the system has always honored any legitimate requests by authorized principals or entities. Availability ensures that information assets are accessible whenever needed. It is an important property since any disruption of service may adversely affect business operations of SMEs.

The cyber-security infrastructure is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organizations.

Integrity: implies that stakeholders expect that content of the emails are not altered and stock counts received are accurate and any attachments downloaded are authentic and complete. These are examples of integrity. Thus, Integrity is the property that data has not been altered in an unauthorized manner during transmission or storage.

Confidentiality: implies that stakeholders expect that the privacy of their correspondences, their passwords, phone numbers, and any other information shared during email interactions will be secured. These are examples of confidentiality. Thus, Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, either in storage or in transmission.

Essential Elements of Cyber-security: As indicated in the preamble, the ITU-T Recommendation X.805 [10] stipulates eight (8) cybersecurity dimensions. In spite of attempts by some authorities to propose alternatives, universally literature accepts the classical cyber-security triad of confidentiality, integrity and availability (CIA) as the basic building blocks of any good cyber-security initiative. This study thus focuses on these three (3) and defines cyber-security as the ability to safeguard computers and network systems and the confidentiality, integrity and availability of the data they contain. The objective of this study is to highlight the challenges confronting SMEs and the need to mitigate the associated risks in order to build a secure business that would ensure business continuity. It is essential to devise cyber-security solutions or mechanisms that would address the needs of SMEs. For instance, encryption and message authentication mechanisms usually work on the assumption of pre-existing relationships between senders and receivers. But in practice, end-users communicate with people they never met, or buy products online from merchants they have never met. In essence, to encrypt or authenticate all messages would have rendered communications impossible. "An open, unauthenticated, risky channel" is however used in establishing communication channels or sessions; cryptography could, at best ensure confidentiality, integrity and non-repudiation between entities which have pre-existing relationships [9]. The communicating entities involved are able to instantiate a session by exercising a relationship to effect communication. This session establishment synchronizes the entities to ensure that appropriate entity credential are exchanged to provide mutual assurance of non-repudiation and confidentiality. As new technologies and services become available, the original uses of local area networks (LANs) and Intranets have also changed [10]. Today's Intranet is said to be a combined web portal and public dashboard. Numerous

challenges beg for resolution as well as a balance needed for end-users, utilization of resources, and the policies facilitating their interactions. Mansoor (2009) posits that the weakest link in security is the user training and awareness. He advocates that new recruits must be given all security policies and be made to sign off before being given access to the network.

Small & Medium sized Enterprises (SMEs): SMEs have been touted as the engine of growth for developing economies. Generally, SMEs are estimated to employ about 22% of the population in developing economies. The SME sector in Ghana (as of 2010) accounts for about 92% of all businesses and contributes about 70% of GDP. Similarly, the Federal Office of Statistics (as captured in) indicated that 97% of all businesses in Nigeria employ less than 100 employees, and the SME is defined under the umbrella term of less than 250 employees. Whereas cyber-security vulnerabilities pose serious concerns to all businesses, SMEs are usually hardest hit victims and find it very difficult to recover after a cyber-attack [6]. The issues of cyber-security metrics and dimensions are explored in details in subsequent sections. Small and medium-sized enterprises (SMEs) consist of varied businesses usually operating in the service, trade, agri-business, and micro-finance and manufacturing sectors. SMEs may be innovative and entrepreneurial, and usually aspire to grow; though, some stagnate and remain family owned [7]. The subject of an investigation under this study is the small-and-medium-sized enterprises (SMEs). Who or what are SMEs? It may seem very simple and easy question, but most literatures reviewed have divergent views. There is no consensus on its definition; no single, uniformly accepted definition of small-and-medium sized enterprises (SMEs) [8].

Conclusion:

Cyber-risk based on intuitive, subjective and holistic assessment of each of the key constructs of cyber-security can be applied by SMEs due to its simplicity and low cost. The taxonomies could also fill the gap created by the lack of standardized lists of vulnerabilities and threats in developing economies for SMEs. At least, SMEs can have some empirical basis of cyber-security challenges to benchmark their business and security performance metrics, rather than relying upon the usual "TV news effect" of most publicized compromises with disproportionate mitigation measures. In essence, all these techniques have been modeled with the SMEs in developing economies in mind. For example, the CSVA model does not require any specialized software or tools; just basic analytical reasoning with technical knowledge in cyber-security and network operations could suffice. Similarly, the application

of fuzzy cognitive map approach to assess vulnerable policies requires only algebraic matrices and the requisite technical knowledge in cybersecurity.

References:

Wiles, Jack & Russ Rogers, Techno Security's Guide to Managing Risks - For IT Managers, Auditors & Investigators, Elsevier, Inc., 2007.

S. K. Katsikas, "Risk Management," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 605-625.

I. Perfilieva, "Fuzzy Function: Theoretical and Practical Point of View," in EUSFLAT, Aix-les-Bains, France, 2011.

J. Walker, "Internet Security," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 93-117.

Cashell, Brian, William D. Jackson, Mark Jickling& Baird Webel, "The Economic Impact of CyberAttacks," US Congressional Reserach Service, 2004.

B. Mansoor, "Intranet Security," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 133-148.

Kapurubandara, Mahesha& Robyn Lawson, "Barriers to adopting ICT & e-Commerce with SMEs in Developing Countries: An Exploratory Study on Sri Lanka," in CollECTeR '06, Adelaide, Australia, 2006.

Meyers, Carol, Alan Lamont & Alan Sickerman, "Use of Multi-attribute Utility Functions in Evaluating Security Systems," Lawrence Livermore National Security Laboratory, USA, 2008.

Better Business Bureau Wise Giving Alliance, "Small Business Giving Survey," 2001. [Online]. Available: www.give.org/news/SBSurvey.pdf. [Accessed January 2012].

Ellefsen, I.D. & S.H. von Solms, Framework for Cyber Security Structure in Developing Countries, University of Johannesburg, 2012.