International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

SECURITY IMPLICATIONS OF INFORMATION AND COMMUNICATION TECHNOLOGY ADOPTION

Mohd Shahid Dar

Research Scholar: Department of Computer Science,

Shri JJT University,Jhunjhunu, Rajasthan, 333001, India.

ABSTRACT

Remembering the double-edged nature of information and communication technology (ICT), it is conceded that towards one side, ICT offers great payoffs and opportunities and at the opposite side it unavoidably prompts different vulnerabilities and insecurities [1]. It is within this setting that this paper attempts to investigate the security implications of ICT adoption in business in SMEs. The research adopts a qualitative method directed to collect primary data from case studies and secondary data from online sources. A total of ten SMEs were chosen as cases from Kashmir India. The primary data which has been resulted in is analyzed by thematic analysis. The paper concludes that the adoption of ICT in these SMEs is disquieted with various security implications, which from multiple points of view would challenge users' intentions to adopt the technology.

Keywords: Security, Implications, ICT, SMEs

I INTRODUCTION

Information security is an indispensable segment to the era in which information with respect to a multiplicity of individuals and organizations is stored in a variety of computer systems, frequently not under our immediate control. Information security can be thought of as a risk to information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction [2]. The perception of risk engaged with embracing ICT is a noteworthy issue to managers and owners of SMEs. It has been recognized by the various researchers that the role of the individual view of security is conceivably the most significant influential issue with respect to the selection of ICT into SMEs. Trust in the technology in connection with handling transactions, securing systems and maintaining relationships is an impressive issue influencing decision makers of SMEs [3]. Taking a look at the growth and capability of the internet in connection to security issues, presently a lack of security is seen as a noteworthy barrier to doing business online. Risks of system corruption, fraud, theft, and viruses direct organizations toward the requirement for improved security [4]. Security related threats have turned out to be not only more numerous and diverse but additionally having more detrimental and disruptive effect. In the past, a computer security incident was thought of as a security-related adverse event in which there was a loss of data confidentiality, disruption of data or system integrity or disruption or denial of

availability. New types of security-related incidents rise frequently since then [5]. In like manner, this paper attempts to explore and discuss the viewpoints on the security implications raised by ICT in the SMEs in India. This paper concludes with the preliminary findings of the research study.

II. RESEARCH OBJECTIVE

This study is driven to explore the security implications of technology adoption, consequently, the objective of this research study is:

To examine the security implications of ICT in business processes of SMEs in India.

Keeping in mind the research objective and/or problem in hand, this research study arises the following research question:

What security implications does the current adoption of ICT have on business processes of SMEs in India?

III. RESEARCH METHODOLOGY

This research adopts a qualitative, cross-sectional research methodology. The collection of the primary data involves face-to-face semi-structured interviews which were conducted with owners, managers and IT professionals of SMEs, who are directly involved in ICT related decision making in their respective enterprises. The face-to-face interviews are most reasonable for exploratory investigation. Sekaran [6]; Zikmund [7] have suggested that the interview method in qualitative research study fill in as a technique which helps with narrowing down the perspective of the research topic and carry out a systematic inquiry about diverse issues; Based on the researcher's convenience and willingness on the part of the participant SMEs to share their views concerning the research area ten SMEs were finally selected as cases which comprised of diverse business sectors. The interviews enquired into the perception of the respondents on various security implications (security risks) of technology adoption in their business. Thematic analysis was put into use for interpreting and analyzing the data obtained from the interviews. According to Morse and Field [8], thematic analysis assists the researchers to place great importance on the central thought of the data which is accomplished by identifying certain themes and analyzing them.

IV. RESULTS AND DISCUSSION

This section is aimed to present the findings brought about through analysis of qualitative data gathered through in-depth interviews with the aim to find the answers to research question mentioned in section II. The semi-structured questionnaire is encouraged to provide enough opportunities for respondents to provide a detailed account of the issue under consideration. The respondents were asked to comment on the security implications of information and communication technology adoption. The participants highlight number of security implications that led them not to adopt or delay their decisions to adopt ICT in their business. All of the participants shared a similar view with regard to their perception of security implications of technology to be

employed in their business operations. The various emergent themes in the light of research objective provide findings to answer research question which is:

What security implications does the current adoption of ICT have on business processes of SMEs in India?

The number of themes that emerged from the interviews with ten SMEs is as follows.

Theme 1: Availability Risks

Theme 2: Privacy Risks

Theme 3: Confidentiality Risks

Theme 4: Integrity Risks

Theme 5: Repudiation Risks

Theme 6: Authentication Risks

1. Availability Risks

One of major concerns when discussing about the data protection is to ensure that the data is available to the users when needed to access it [2]. Availability of information refers to ensuring that authorized users are able to access the information when it's requested or needed. In an ICT enabled business environment loss of availability is deciphered as loss of data or sometimes loss of access to information temporary or permanently, which has become a very serious concern nowadays. Andress [2] defines loss of availability as loss of the data in its physical medium unavailable for our use, on a temporary or permanent basis. Evans et al. [9] ascertain that a loss of availability is the disruption of access to or use of information or an information system; Threats to availability include hardware failure or system malfunctions, software corruption, computer virus and malware, external hackers, distributed denial of service (DDoS) attacks, programming errors, human error, staff negligence, theft, or natural disasters. Besides, the data loss by breaches from external hackers, fraudsters or other incidental events, this is of concern that it is the internal threat of theft by staff that is considered to be the greater risk to information availability by many organizations. It is internal staff, with malicious or financial motivations, that will always be in a better position to copy, remove or even destroy vital business information, often undetected until it is too late. This loss can be costly and detrimental to business. The loss of financial reports, client information or other information that is crucial to business would let you down for days. Once this information is lost, data reconstruction becomes hard. In many cases, organizational operations can be so adversely affected.

2. Privacy Risks

Information privacy is an important aspect of information technology (IT) security which ensures that data either shared with trading parties or entrusted to organizational IT professionals who have authorizedly given access to data cannot be divulged to third parties without the express consent of the organization; From the viewpoint of Suh and Han [10] privacy protection ensures that personal information about customers collected from their electronic transactions is protected from disclosure without permission [10]. However, in its broader

perspective, the risks of data privacy could result from both within the organization and from trading parties since data privacy is suitably defined as the appropriate use of data. Data privacy is about authorized access and is a legal issue. In one hand, when enterprises and stakeholders use data or information that is provided or entrusted to them whether personal or financial, it should be ensured that data might not be sell or disclosed to any third party without explicit consent and the data should be used according to the agreed purposes. Uncertainty, the trading parties could reveal or sell volumes of the information to other parties that were entrusted to them without getting prior approval. On the other hand, there is also the threat of violation of data privacy from authorized users of data within the organization. An authorized IT professional could also sell the organizational important and sensitive data and thereby breaches security by violating data privacy.

3. Confidentiality Risks

Confidentiality is a concept similar to, but not the same as, privacy. Confidentiality refers to the ability to protect data from those who are not authorized to view it [2]. Privacy ensures that information shared between trading parties who have authorizedly given access to data should be protected from disclosure [10]. According to Chaeikar et al. [11] confidentiality is keeping sensitive data secret against unauthorized users; An attack against confidentiality refers to access to data, applications or environments by unauthorized users [2]. Similarly, Suh and Han [10] infer that confidentiality warrants that all communications between trading parties are restricted to the parties involved in the transaction; Confidentiality is about securing and protecting information against unauthorized access or disclosure. In other words, confidentiality means preserving authorized restrictions on access and disclosure of information and ensuring the protection of information from those who are unauthorized to view the data or information. The loss of confidentiality is essentially a technical issue where an unauthorized person unauthorizedly access, stole and divulge or sell organizational critical business data. The tort of breach of confidentiality applies to both organizational professionals who maintain relationships of trust and the violators from outside the organization. One of the biggest threats to violation of data confidentiality from external environment is hacking, a technique to breach the security of information systems with the use of computers, networks and malwares like Trojan, Spyware etc. to unauthorizedly access and stole the data ranging from organizational records to trade secrets and in some cases, security questions and passwords. At the same time, your business data accessed by unauthorized users within the organization could be possibly sold to third parties, which may result in further loss and overheads.

4. Integrity Risks

Data integrity is a fundamental component of information security; Integrity refers to the ability to prevent data from being changed in an unauthorized or undesirable manner. This could mean the unauthorized change or deletion of data or it could mean an authorized, but undesirable change or deletion of data [2]. Integrity is assurance of originality of data and realizing any data alteration or tampering [11]. According to Suh and Han [10], data integrity means that data in transmissions are not created, intercepted, modified or deleted illicitly.

From the perspective of data transmission, Smedinghoff and Bro [12] ascertain that integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage [12]? A loss of integrity is the unauthorized modification or destruction of information [9]. As for information security, integrity is the protection of information from intentional/deliberate or unintentional/accidental unauthorized modification. The data source must not be changed in transit or at rest and should be accessible and preserved in its original form. In other words, integrity is a requirement that information is changed only in a specified and authorized manner to maintain its accuracy and consistency over its entire life-cycle to ensure that the information is same as it was intended to be. That is to say that it is maintaining and assuring the accuracy and consistency of data stored and processed by IT professionals. Data integrity risk in an unintentional or accidental circumstance is the risk of unexpected modification of data by IT professionals or IT systems (human errors, software, hardware malfunctioning) results in incomplete, inaccurate or inconsistent data across different IT systems. In an intentional or deliberate attempt, data integrity risks could be led either by organizational professionals for their personal benefits or by hackers and fraudsters using a computer to alter data especially in business dealings for illegal benefits.

5. Repudiation Risks

A repudiation is an event where someone denies of having performed a specific action or transaction. This is usually seen in electronic communications where one party cannot be established as the recipient or either of the party deny to any communication established or having existed. In former case a receiver may block email inbox or internet ports for communication and later denying for performing that action. In later case a sender may deny to any communication that he/she originated or a receiver denies of having been take delivery of something sent or communicated. As technology advances and improves, an ever-increasing number of methods of communication and business dealings are being directed digitally, rather than the times of old when all business was engaged by close and personal communication between trading parties. Since there is no physical interaction (face-to-face) between stakeholders, therefore, there is dependably a need to guarantee the authenticity and legitimacy of the transaction taking place over electronic channels. That's where non-repudiation comes into play. In information security settings nonrepudiation refers to a situation in which sufficient evidence exists as to prevent an individual from successfully denying that he or she has made a statement or taken an action. Nonrepudiation prevents someone from taking an action, such as sending an e-mail and then later denying that he or she has done so [2]. According to Suh and Han [10] nonrepudiation means that neither of the trading parties should be able to deny having participated in a transaction after the fact; Non-repudiation therefore means putting measures in place to ensure that in any digital transaction someone cannot deny or contest that thing.

6. Authentication Risks

The authentication risk has turned into a difficult issue in the course of recent years and therefore is a central focal point of many enterprises. Authentication is the way of guaranteeing that systems are accessed in the strict sense only by the genuine or valid users. In security systems, authentication is recognizably different in nature from authorization, which is the process of granting individuals access and privileges to information based on their identity. Authentication just guarantees that the individual is, in fact, who he or she is asserted to be, but says nothing in regards to the access rights of the individual. As stated by Grance [5] authentication means every user-initiated activity within the computer system should be attributable to a system user. Suh and Han [10] state that authentication ensures that the trading parties in an electronic transaction or communication are who they claim to be. The IT systems could prompt authentication risks in the event user's identity (usually based on a username and password) is lost to someone, for example, spyware Keylogger, something that keeps a record of every keystroke you made on your keyboard. Keylogger has turned out to be a dangerous threat to steal login credential of people such as their username and password. Another thing is Phishing, a fake website which is designed in a way that it almost looks like the actual website to trick the user into entering their login credential into the fake login form which serves the purpose of stealing the identity of the user. The information submitted to the phishing site will go to the server controlled by attacker rather than the actual one.

V. CONCLUSION

In light of the discussion above, the adoption of the ICT in SMEs has certainly raised many security implications. All these implications would in turn have profound consequences not only on the ICT adoption decision in SMEs' yet in addition the way business would be led by these organizations.

REFERENCES

[1] A. M. Mohamad, Z. Hamin, and M. B. Othman (2012), Security Implications of ICT Adoption in the High Courts of Malaysia, International Journal of Future Computer and Communication,1(3), 2012, 256-259.

[2] J. Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress Publishing, Inc. Rockland, MA, United States 2014.

[3] C. Allan, and J. Annear, A Framework for The Adoption of ICT and Security Technologies by SME's, *16th Annual Conference of Small Enterprise Association of Australia and New Zealand, 28 September to 1 October 2003.*

[4] A. Aldridge, M. White, and K. Forcht, Security Considerations of Doing Business via the Internet: Cautions to be Considered, Internet Research, 7(1), 1997, 9-15.

[5] T. Grance, J. Hash, and M Stevens, Security Considerations in the Information System Development Life Cycle, Washington: National Institute of Standards and Technology, 2004.

[6] U. Sekaran, Research Methods for Business: A Skill Building Approach (3rd Ed.). John Wiley & Sons, Inc 2000.

[7] W. G. Zikmund, Business Research Methods (6th Ed.). Dryden Press, Orlando, Florida, U.S.A, 2003.

[8] J. M. Morse, and P. A. Field, Qualitative Research Methods for Health Professionals. California: Sage Publications 1995.

[9] D. L. Evans, P. J. Bond, and A. L. Bement, Standards for Security Categorization of Federal Information and Information Systems. Computer Security Division, Information Technology Laboratory, NIST. 2004. Available at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[10] B. Suh and I. Han, The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, International Journal of Electronic Commerce, 7 (3), 2003, 135- 161.

[11] S. S. Chaeikar, M. Jafari, H. Taherdoost, and N. S. Chaei kar, Definitions and Criteria of CIA Security Triangle in Electronic Voting System, International Journal of Advanced Computer Science and Information Technology (IJACSIT), 1(1), 2012, 14-24.

[12] T. J. Smedinghoff, and R. H. Bro, Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce, J. Marshall J. Computer and Info. L, 17(1), 1999, 723-768.