ISSN 22773061

Information Security Awareness Behavior : A Conceptual Model for Cloud

[1] Sasan Karamizadeh, [2] Jafar Shayan, [3] Mojtaba Alizadeh, [4] Atabak Kheirkhah

[1,2,4] Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, 54100, Malaysia

Ksasan2@live.utm.my, sjafar3@live.utm.my, katabak2@live.utm.my

[3] Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur, 54100, Malaysia

amojtaba2@live.utm.my

ABSTRACT

Cloud computing has changed the whole picture that distributed computing used to present such as Grid computing, server client computing. Despite Cloud offers great benefits, it also introduces a myriad of security threats to the information and data which is now being ported from on-premises to off-premises. These security threats must be overcome in order to get full benefit from this new computing exemplar. This paper identifies the importance of awareness behavior in context of information security for cloud. We investigate four important factors of security awareness behavior that should be considered when organisations intend to improve their security toward cloud computing environment based on awareness-focused programs. Finally we conclude that a well-structured awareness program that positively affect the level of self-efficacy, security practice care behavior, security awareness technology behavior and intention will improve the level of total information security in cloud computing environment.

Indexing terms/Keywords

Cloud computing; Security; Security awareness; awareness behavior.

1. INTRODUCTION

The emergence of the phenomenon commonly known as cloud computing represents a fundamental change in the way information technology (IT) services are invented, developed, deployed, scaled, updated, maintained and paid for. Computing becomes more pervasive within the organization, the increasing complexity of managing the whole infrastructure of disparate information architectures and distributed data and software has made computing more expensive than ever before to an organization [1, 2]. The promise of cloud computing is to deliver all the functionality of existing information technology services (and in fact enable new functionalities that are hitherto infeasible) even as it dramatically reduces the upfront costs of computing that deter many organizations from deploying many cutting-edge IT services [3]. All such promise has led to lofty expectations — Gartner Research expects cloud computing to be a $150 billion business by 2014.

The impetus for change right now is seen predominantly from a costs perspective, as organizations increasingly discover that their substantial capital investments in information technology are often grossly underutilized. One recent survey of six corporate data centres found that most of the servers were using just 10–30% of their available computing power, while desktop computers have an average capacity utilization of less than 5%[4]. Equally pertinent are the maintenance and service costs that have proved to be a drain on scarce corporate resources.

Cloud computing technologies can be implemented in a wide variety of architectures [5-7], under different service and deployment models, and can coexist with other technologies and software design approaches. The security challenges in cloud computing presents, however, are formidable, especially for public clouds whose infrastructure and computational resources are owned by an outside party that provide those services to the general public. The (advancements, progress!) emerge of cloud computing promises far-reaching effects on the systems and networks of state agencies and other organizations. Many of the features [8] that make cloud computing attractive, however, can also be at odds with traditional security models and controls.

Cloud security issues and the risks of cloud computing are not well understood today and are one of the biggest barriers to adopt cloud/grid services. This section helps CIOs and IT managers assess the security risks of cloud computing with the latest information on cloud security standards; how to manage data security, data privacy, regulatory and compliance implications in a cloud model [9].

Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions are critical for its success. Although clouds allow customers to avoid start-up costs, reduce operating costs, and increase their agility by immediately acquiring services and infrastructural resources when needed, their unique architectural features also raises various security and privacy concerns.

2. INFORMATION SECURITY AND HUMAN ERRORS

An The National Research Council Computer Science and Telecommunications Board has distinguished between accidental and deliberate causes of poor computer and information security (CIS): ‘‘Accidental causes are natural (e.g., a lightening surge that destroys a power supply in a network that causes part of the network to fail) or human but non-deliberate (e.g., an accidental programming error that causes a computer to crash under certain circumstances, or the unintended cutting of a communications cable during excavation) [10].

In the fall of 2000, Western Union was victim to an attack that was attributed to human error rather than a design flaw. A hacker electronically entered one of Western Union’s computer servers without permission and stole about 15,700 customer credit card numbers. The incident occurred after the system was taken down for regular maintenance, and a file containing the credit card information had inadvertently been left unprotected when the system was returned to operation. In addition, Whitman’s [11] study found that the IS directors, managers, and supervisors ranked technical software failures or errors and acts of human error failure higher than deliberate software attacks. Whitman’s [11] findings support recognition of human error and failure as a significant area for consideration in the field of CIS. In addition, examining accidental causes may allow an organization to identify weaknesses in its systems or processes that may be deliberately exploited.

The field of human factors has developed models and concepts for understanding and characterizing varying types and levels of human error, which have been used successfully in various industries to analyze causes of accidents [12]. These taxonomies not only explore the cognitive mechanisms involved in human error [13], but also emphasize the role of organizational and management factors in the creation of error-prone conditions [12]. We propose that taxonomies and models of human error can be used to identify and characterize vulnerabilities of computer and information systems.

Research indicates that insiders perpetrate 70% of fraud rather than external criminals but that focus 90% of security controls and monitoring on external threats [14]. Even where technical controls for insiders are available, they must not be considered in isolation [15].

Information security violations continually evolve in sophistication and increase in number to counter the changing nature of the threats [16].

However, in order for these to operate successfully they inherently rely upon the end-user to be able to deploy, configure and operate them. Unfortunately, it is also a well-recognized fact that security is only as strong as the weakest link; and the weakest link is frequently the end-user [17].

To counter the threat caused by end-users an increased focus has been given towards information security awareness and the need to educate and inform end-users. Within an organizational context, efforts towards improving awareness amongst employees have increased.

One of the largest problems in computer and information security (CIS) is the effective remediation of vulnerabilities and damages from attacks; however, organizations emphasize a technological approach to protect their assets [18]. Computer and information security has focused mainly on technological solutions to prevent vulnerabilities and attacks and have not yet fully adopted a Socio-technical approach that addresses human and organizational aspects of CIS [19]. Human and organizational aspects have been found to be important in the effectiveness of other critical systems, such as safety and accident mitigation [12, 13].

People are the weakest link for security. Knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry. Social engineering attacks, lower reporting of and slower responses to potential security incidents, and inadvertent customer data leaks are all possible and probable risks that may be triggered by lack of an effective security awareness program [20].

3. SECURITY AWERENESS AND COMPRISED FACTORS

Nowadays awareness about security behavior in pervasive systems and environments is very important. Cloud customers are not aware of the risks they could face when migrating into the cloud, particularly those risks that are generated from cloud specific threats, i.e., loss of control, vendor lock-in, exhausted CP resources, etc. This lack of awareness could also affect the cloud provider who may not be aware of the actions that should be taken to mitigate these risks.

A lot of variable is that has effect in security behavior to enhance awareness but according to observation self-efficacy, Security Practice Care Behavior, Security Awareness Technology Behavior, Intention are very important to enhance awareness.

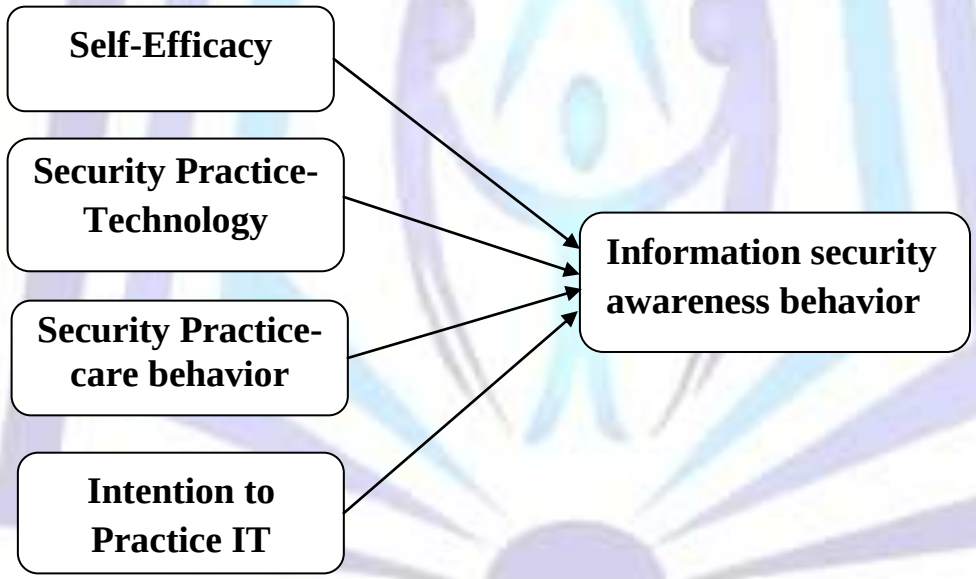

Figure1: Model of information security awareness behaviour utilized in cloud

4. INFORMATION SECURITY AWARENESS BEHAVIOR

claimed that awareness instructions and guidelines are vital parts of defending stability. In addition, every client must be educated by means of stability awareness, with their effective role in protecting details that are possessed [19]. It employs a continuous protection awareness training program as a possible compound in the enterprise property defence system. The specific program's intention is to increase users' attention of the risk and the necessity regarding resource security techniques, particular tool safety along with the consequences associated with illegal measures [16].

Believe that companies should focus on protection awareness and make their own plans elaborately clear in order to ensure that there is no security issue in the organization. It proposes a chaos of consumers in protection problems which casually take the potential risks by their certain natural actions [20].

4.1 Text Self Efficacy

Self-efficacy is a Self-efficacy is a key element in the formation of social cognitive theory. It's a form of self-evaluation that is a proximal determinant of individual's behavior [21]. People with a high level of self-efficacy have got stronger form of conviction regarding their capability to mobilise motivation, cognitive resources and course of action needed to efficiently implement a task. Self-efficacy affects just how much of work, self-regulations, and the initiation and endurance of managing challenge [21]. The particular medical quality of this specific argument may be mentioned in a range of research contexts for critiques, discover [22] warns against utilizing of circumstances with significantly less steps of SE. In keeping with this specific domain-specific discussion, [23] explicate the particular concept of computer self-efficacy by considering widespread tasks as well as certain amounts. Task specific self-efficacy is related to the particular effectiveness viewpoint in starting specific computer-related tasks from the region of standard computing. Typical computer self-efficacy is related to the actual effectiveness belief close to many computer program regions.

4.2 Security Practice Care Behavior

According to social psychological theory on information security platform, when individuals start to believe in protection of their own information and systems information, they tend to help in the process of improving security methods and they show positive intentions to the organization to continue its efforts on the current system. In change, self-Efficacy was positioned in order to influence current information security application and intention of increasing this sort of project. Every single of the actual constructs and it is discussion is explained below [17]. Security exercise may be significant as individuals' information security risk management behaviors are the two factors of the utilization of security technology as well as security knowledgeable care behavior, associated with computer and Internet use. The previous relates to making use of security software and characteristics such as anti-virus software, anti-spyware, and a pop-up obstructing perform. For instance, when a criminal recognizes security syndication behavior in utilizing a computer and Internet, he or she can employ a robust code and generate a backup replicate. Moreover, various dimensions of security exercise behavior are necessary for a better effective risk management. Training security awareness care- behavior together with entitlement of security software decreases some weakness of information security and increases the use of security software on its own.

4.3 Security Practice Technology

The particular growing class of information security dangers and the actual ever-growing body of rules has made information security an essential function within many areas of businesses. However, many companies find it difficult to access sources that protect hazards imposed on their information security. Securing networks can be done through implementing a mix of anti-virus/anti-spyware software, firewalls, intrusion prognosis and reduction systems, and articles filtering software. Nevertheless, this specialized layer of defence to an organization's security may falter to human disappointment. A mobile computer remains thoughtlessly behind in a public location including a good internet cafe. Organizations are actually facing problems in their securities with all the introduction of electronic commerce and open up network architectures [24]. Much better computer reading and writing, improved computer literate personnel, and accessibility to superior software methods might also contribute to the increase in security violations in future. Therefore, management must pay more attention to potential security problems.

4.4 Intention to Practice It Security

Nowadays highly interconnected world, cyber security is a serious issue that requires attention. With 888 million Internet users (Internet Usage Statistics 2005), it is imperative to study the security of home computers connected to the Internet, as it has a direct impact not just on individual computers, but the security of the cyberspace, including critical infrastructures and services (such as telecommunication and banking) that are heavily dependent on the secure functioning of the cyberspace. Undefended home computers can become part of networks of remotely controlled machines that are then used to attack critical infrastructures. Thus, we consider the practice of home computer security as a socially and personally positive behavior as it protects one's home computer and contributes to the security of the cyberspace.

Information systems (IS) cannot be effective unless they are used. However, people sometimes do not use systems that could potentially increase their performance. Behavioral intention measures individuals' willingness to continue their efforts in order to strengthen their security measures.

One of the biggest threats to home computer security is virus infection, which has the potential to threaten the confidentiality and integrity of information on computers as well as the availability of computers and networks. The damage is not limited to just home users, as the security of the cyberspace is affected.

5. CONCLUSION

Emerging of cloud computing was forced by economic crisis and trends show it will be hot topic for following years. Benefits offered by cloud computing and the need for cost saving in nowadays competitive environment, made it inevitable transition to cloud.

Although enterprises are satisfied with these advantages but in other hand, this phenomenon brought us some concerns in terms of Information security risks and vulnerabilities.

So far, most of focus in order to form, more secure computing environment was on Technical aspects and solutions but several studies revealed that role of human errors or accidental faults should be considered because they can play important role in success or failure of security programs.

Especially in cloud computing environment that we outsourced most of technical issues and concerns to cloud providers, it is vital point to address human security behaviors that can affect whole information security.

As cloud, computing is still a new model; it needs more investigation and research to satisfy users concerns. We need to declare models of evaluating security awareness behavior in cloud environment and survey its implications to whole information security program.

6. REFERENCES

[1] P. Roehrig, "New Market Pressures Will Drive Next-Generation IT Services Outsourcing," *Forrester Research, Inc,* 2009.

[2] Mojtaba Alizadeh, Wan Haslina Hassan, Navid Behboodian, and Sasan Karamizadeh, "A Brief Review of Mobile Cloud Computing Opportunities," *Research Notes in Information Science (RNIS),* vol. 12, pp. 155-160, 2013.

[3] J. Staten, "Hollow Out The MOOSE: Reducing Cost With Strategic Rightsourcing," *Forrester Research, Inc,* 2009.

[4] VMWare, "Addressing Desktop Challenges," *VMWare,* 2008.

[5] Zhang Liang-Jie and Zhou Qun, "CCOA: Cloud Computing Open Architecture," in *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pp. 607-616, 2009.

[6] Ahmad Azarnik, Jafar Shayan, Mojtaba Alizadeh, and Sasan Karamizadeh, "Associated Risks of Cloud Computing for SMEs," *Open International Journal of Informatics,* vol. 1, pp. 37-45, 2012.

[7] Jafar Shayan, Ahmad Azarnik, Suriayati Chuprat, Sasan Karamizadeh, and Mojtaba Alizadeh, "Identifying Benefits and risks associated with utilizing cloud computing," in *Identifying Benefits and risks associated with utilizing cloud computing*, San Francisco, USA, 2013.

[8] Sandra Upson, "Cloud Computing: It's Always Sunny in the Cloud," *IEEE Spectrum's Special report,* Jan 2011 2011.

[9] Mojtaba Alizadeh and Haslina Hassan Wan, "Challenges and Opportunities of Mobile Cloud Computing," in *Challenges and Opportunities of Mobile Cloud Computing*, 2013.

[10] Sara Kraemer and Pascale Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Applied Ergonomics,* vol. 38, pp. 143-154, 2007.

[11] Michael E. Whitman, "Enemy at the gate: threats to information security," *Commun. ACM,* vol. 46, pp. 91-95, 2003.

[12] J.T. Reason, *Managing the risks of organizational accidents*: Ashgate, 1997.

[13] J. Rasmussen, A.M. Pejtersen, and L.P. Goodstein, *Cognitive systems engineering*: Wiley, 1994.

[14] A McCue, "Beware the insider security threat," *CIO Jury,* 17/4/2008 2008.

[15] Andy Jones and Carl Colwill, "Dealing with the malicious insider," presented at the 9th Australian information and Warfare security Conference, 2008.

[16] S. Talib, N. L. Clarke, and S. M. Furnell, "An Analysis of Information Security Awareness within Home and Work Environments," in *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pp. 196-203, 2010.

[17] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*: John Wiley & Sons, 2011.

[18] Denis Besnard and Budi Arief, "Computer security impaired by legitimate users," *Computers & Security,* vol. 23, pp. 253-264, 2004.

[19] Gurpreet Dhillon and James Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal,* vol. 11, pp. 127-153, 2001.

[20] Kresimir Popovic and Zeljko Hocenski, "Cloud computing security issues and challenges," in *MIPRO, 2010 Proceedings of the 33rd International Convention*, pp. 344-349, 2010.

[21] A. Bandura, "Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy," 1986.

[22] A. Bandura, "Self-efficacy: toward a unifying theory of behavioral change," *Psychological review,* vol. 84, p. 191, 1977.

[23] G. Marakas, R. Johnson, and P.F. Clay, "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time," *Journal of the Association for Information Systems,* vol. 8, p. 2, 2007.

[24] K. Bussey and A. Bandura, "Social cognitive theory of gender development and differentiation," *Psychological review,* vol. 106, p. 676, 1999.

Author' biography with Photo

Sasan Karamizadeh received his MSc in Computer Science (Information Security) from Universiti Teknologi Malaysia in 2012 and is doing his PhD in Computer Science (face recognition). His research interest is in Biometirc, Cryptography, and Cloud Computing.

Jafar Shayan received his MSc in Computer Science (Information Technology) from Universiti Teknologi Malaysia in 2012. His research interest is in IT Management, Software, and Cloud Computing.

Mojtaba Alizadeh received his MSc in Computer Science (Information Security) from Universiti Teknologi Malaysia in 2012 and is doing his PhD (Communication Systems and Networks Security) studies in Computer science. His research interest is in Cryptography, Network Security, and Mobile Cloud Computing.

Atabak Kherikhah received his MSc in Software Engineering from Universiti Teknologi Malaysia in 2012 and is doing his PhD in Computer Science (Genetic Algorithm). His research interest is in genetic algorithm, cloud Computing.