Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Evaluation model for knowledge sharing in information security professional virtual community

Alireza Tamjidyamcholo[a,b,*], Mohd Sapiyan Bin Baba[a], Nor Liyana Mohd Shuib[a], Vala Ali Rohani[a]

[a] Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia
[b] Computer Science and Information Technology Department, Islamic Azad University, Parand Branch, Tehran, Iran

ARTICLE INFO

Article history:
Received 21 September 2013
Received in revised form
19 February 2014
Accepted 23 February 2014

Keywords:
Knowledge sharing
Information security
Risk
Professional virtual community

ABSTRACT

Knowledge sharing has been proven to have affirmative effects on both the education and business sectors. Nevertheless, many professional virtual communities (PVC) have failed due to reasons, such as the low willingness of members to share knowledge with other members. In addition, it is not explicitly evident whether knowledge sharing in information security is able to reduce risk. To date, there have been relatively few empirical studies concerning the effects of knowledge sharing and its capability to reduce risk in information security communities. This paper proposes a model that is composed of two main parts. The first part is the Triandis theory, which is adapted to understand and foster the determinants of knowledge sharing behavior in PVCs. The second part explores the quantitative relationship between knowledge sharing and security risk reduction expectation. One hundred and forty-two members from the LinkedIn information security groups participated in this study. PLS analysis shows that perceived consequences, affect, and facilitating conditions have significant effects on knowledge sharing behavior. In contrast, social factors have shown insignificant effects on knowledge sharing behavior in information security communities. The results of the study demonstrate that there is a positive and strong relationship between knowledge sharing behavior and information security risk reduction expectation.

Introduction

As knowledge management (KM) is gaining more strategic significance in organizations and institutions, these organizations have turned to applying different KM initiatives (Chen et al., 2012). Lin et al. (2012) discerned a number of fundamental factors in KM activities, which include recognition, collection, selection, organization, implementation, sharing, and construction of knowledge. Knowledge sharing is considered as a critical step for successful knowledge management (Lee and Ahn, 2007). In knowledge management, a critical problem is how to encourage people to engage in knowledge sharing with others (Hung et al., 2011). Hung and Cheng (2012) contended

[*] *Corresponding author*. Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia. Tel.: +60 3 79676343; fax: +60 3 79579249.
E-mail address: itm.tamjid@gmail.com (A. Tamjidyamcholo).

http://dx.doi.org/10.1016/j.cose.2014.02.010
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

that knowledge sharing should be considered as a process, an action or a behavior. Ryu et al. (2003) put forward another definition for knowledge sharing. They defined knowledge sharing as a connecting behavior in which people try to gain knowledge from others. Meanwhile, Lee (2001) defines knowledge sharing as the willingness of individuals, groups or institutions to convey or spread knowledge to others. Holtshouse (1998) maintained that knowledge is a flow concept and that knowledge holders share their knowledge with knowledge receivers. Furthermore, Bock et al. (2005) defined knowledge sharing as the attitude of individuals to construct and transfer knowledge whereas Wijnhoven (1998) maintained that knowledge conveyance occurs via information media in which recipients are able to add new knowledge to their existent knowledge. The emergence of the Internet has popularized interaction and information sharing among users via virtual space or cyberspace. Yang and Maxwell (2011) identified different factors influencing knowledge sharing from three perspectives: interpersonal, intra-organizational, and inter-organizational. Knowledge sharing in virtual space is mostly related to the interpersonal perspective. Users from all walks of life join virtual communities in order to share their knowledge relevant to common interests and topics. Virtual communities can be described as a social community that originated through the Internet. These communities take shape when the number of people who want to participate in public discussions increase and reach an acceptable number and when participants possess strong and sufficient emotion to build networks of personal relationship through the Internet (Vijayasarathy, 2004). These communities are built upon the interconnections and relationships of participants. They can generate particular scopes of information in which participants are able to perform ordinary tasks, and learn from each other and make a contribution to community knowledge, and, ultimately, they can extend the knowledge collectively (Lee et al., 2002). Professional virtual communities (PVCs) are somehow different from general virtual communities. We can define a professional virtual community as an expanded community with a shared activity (Wenger, 1998). In fact, cyberspace communities work as a warehouse of knowledge that provides people with an opportunity to receive or share information.

Virtual communities have faced a serious issue in recent years pertaining to cyber-attacks and security breaches. A large and diverse number of institutions have been the targets of such attacks, ranging from high-profile firms to prestigious universities. Richardson (2011, http://gocsi.com/) in the 15th annual computer crime and security survey pointed out that 41% of respondents had confirmed that they had experienced a security incident over the course of the year. According to Richardson (2011), this study had been performed in 351 industrial units with various backgrounds; namely, educational services, financial services, health services and manufacturing. Very few participants were inclined to give out the exact amount of financial losses. However, two respondents revealed their losses, which were sizably large; namely, $20 million in total for one and $25 million for another. Nowadays, financial profits are the key motivation for hackers, while many people may think they look for personal information or for more excitement (Liu et al., 2011). Hence, it is quite reasonable to see that organizations that depend on the Internet for their major business activities take serious precautions for information security (Szymanski and Hise, 2000; Chen et al., 2008). Nonetheless, those institutions that are not directly dependent on the Internet for their business activities still regard information security as a vital issue. This is because such organizations have access to plenty of personal and sensitive information about their customers, product sales, and technical information. More funding in the information security sector is considered a major initiative for institutions to achieve more information security. One of the initiatives that organizations can apply to increase information security is to invest in security technologies; namely, antivirus software, firewalls, sophisticated encryption technology, intrusion detection systems, and other hardware devices (Hamill et al., 2005; Liu et al., 2006). The investment fund must be cautiously balanced with the effects they can create in information security. It is also possible for companies to enhance their information security via cooperating and sharing technical security information with other companies. It has been shown by a number of experimental studies that institutions can save their investment expenditure when they share their security knowledge with each other and that it can help them to decrease their expenses (Liu et al., 2011; Gal-Or and Ghose, 2005; Gordon et al., 2003). The Information Technology Information Sharing and Analysis Centre (IT-ISAC) (https://www.it-isac.org) can be viewed as a good example of security knowledge sharing. The major goal of this center is to assist in sharing information on cyber-security threats and vulnerabilities. An impartial forum is designed for members of this center to communicate with peers from other companies in order to share and identify technical and non-public details of threats and vulnerabilities. In addition, members can have access to a trusted point of contact for knowledge sharing before or during forum sessions. IT security specialists are baffled by similar problems and need to find effective ways to circumvent such problems. However, when specialists have the chance to share their knowledge such situations would not arise as they would be able to provide high quality solutions and enhance previous approaches rather than just reinventing the security wheel. Currently, virtual space is a common and joint environment in which experts are able to find each other and share their knowledge and information (Lin et al., 2008). Researchers have noted that virtual communities often fail in fostering knowledge sharing efforts because they are oblivious of the willingness of individuals to share knowledge and the knowledge that is needed for successful knowledge sharing (Chen and Hung, 2010; Lin et al., 2009). The evaluation of the virtual communities in information security has shown that the most important challenge for knowledge sharing is motivating users to participate in knowledge sharing (Feledi et al., 2013; Fenz et al., 2011). Tamjidyamcholo et al. (2013) studied influencing factors, including attitude, self-efficacy, trust, norm of reciprocity, and shared language with regard to the intention of information security workers to share knowledge in virtual communities. However, other factors, such as perceived consequences, affects, social factors and facilitation conditions, need to be investigated. In this research, we investigated the effects of the remaining factors on knowledge sharing behavior of security experts. In addition, the applicability of knowledge sharing in improving performance (Huang, 2009) and enhancing online learning (Ma and Yuen, 2011; Chan and Chan, 2011) are