International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 1 [ISSN : 2250-3757]
Publication Date : 30 April, 2015

A Comparative Study on the Information Security Culture Related to Workplace and Home Practices

[Hamida Omer Issa Asker & Mohd Zalisham Jali]

Abstract*— Security awareness can be practiced from various angle like within school, government-sponsored initiatives and security providers. The aim of present paper is however confined to investigating the behavior, practices and interactions at the organization level and within home environments. Therefore, the survey was conducted to assess the information security culture among workers in terms of their workplace and home practices; and to determine if a relationship exists between information security culture practices at the workplace and at home. The result demonstrated that the awareness at home and within the workplace appears to be of the same level, with negative practices are still practices insecure behavior.

***Keywords*— Security awareness, workplace practice, home practice.**

I. Introduction

Information security threats have experienced significant evolution in terms of volume and nature, shifting from technical savvy hackers with unerring skills to organized and meticulous crackers aiming to gain financial benefits for their work [1]. Consequently, cybercrime activities have increased and end-users find themselves the recipient of threats. According to [2], more than half (52%) of firms have been threatened in 2007 alone while [3]reported that 64% of the study respondents admitted to encountering Phishing email, a threat that was not widespread 5 years ago. In this regard, user's protection has been proposed in a range of security countermeasures. These safeguarding tools constantly involve in terms of sophistication and in number to counter the evolving threats. Nevertheless, the successful operation of such tools depends upon their effective deployment, configuration and operation by end-users. More importantly, it is a well-known fact that the strength of security is only as effective as its weakest link, and the latter is, more often than not, the end user [4]. In an attempt to counter the threat experienced by end-users, increasing concentration has been directed towards information security awareness, education and information dissemination.

Hamida Omer Issa Asker
Universiti Sains Islam Malaysia (USIM)
Malaysia

Mohd Zalisham Jali
Universiti Sains Islam Malaysia (USIM)
Malaysia

In the context of the organization, efforts have been expended towards enhancing awareness among workers [2] as evidenced by the fact that 82% of enterprise firms provide training. This scenario is however not common for all companies [5] as in majority of small-to-medium companies only 40% reported to provide training. Several organizations possess the training resources if they intend to provide training but they only constitute 95% of Internet users. The remaining 5% are home-users or the general public. The concern lies on the fact that 95% of users are prone to threats and attacks [6]. On the other hand, home users have various resources to enhance their online threats awareness and they are provided with supporting information by anti-virus providers, operating system vendors, and government initiatives [1].

Moreover, despite the available training programs and initiatives at the workplace and at home respectively, research dedicated to understanding what is being relayed and where, the strategies effectiveness and the level of learning styles' role in realizing good information security practice is still few and far between. In this regard, security awareness can be viewed from various directions like within school, government-sponsored initiatives and security providers. The present paper is however confined to investigating the behavior, practices and interactions at the organization level and within home environments. The organization of this paper follows the following sequence; the current information security awareness and the security culture development are discussed in Section II, followed by the study methodology in Section III, and the presentation of study findings in Section IV. Section V provides a discussion of the main findings, while Section VI presents the conclusion and sets the direction for future studies.

II. Related Works

Both academic and commercial communities have given due attention to information security awareness in the past few years. Organizations are increasingly acknowledging the significance of their information assets and the development of effective strategies to enhance awareness within the company. This has been further supported by effective corporate governance regulation and legislation [7]. In addition, a considerable amount of studies have called for the need to develop an information security culture in the organization and to shift from surface learning to embedding good practice among workers [8, 9]. Researchers are convinced that establishing such culture in the organization, can lead to the maintenance of long-term security practice and promote awareness and education of security issues as it facilitates employee engagement of the practice.

With regards to home users, awareness raising initiatives have been proposed; for instance, [10] is a U.K. Government sponsored initiative that offers general information concerning risks and protection from threats. Such initiative offers information from guidelines to particular information concerning threats and is primarily text based information coupled with a few video files. The U.S. and other countries also have a similar national-based websites catering to awareness [11]. Several companies providing security software and operating systems also offers web-based access reading-based resources to educate and inform home users [12, 13]

Evidently, it is a challenging feat to motivate home users to employ security measures as security, although a requirement is not always the user's primary task. People often fail to understand that they need to follow security measures and those that do understand, have limited time to so. According to evidence, even when users think they are well-informed about security and self-protection, they often fall off the mark. According to a study conducted by [14], 75% of home users think they are protected from spam, but in actuality only 42% did. This gap between what they know and the actual reality demonstrates a significant gap in understanding. Good security awareness has been investigated by various studies in the hopes of creating learning mechanisms like face-to-face training sessions, email messages, online training, video game, intranet-based access and poster campaigns [15]. Studies primarily concentrated on what and how to educate workers in the organization and highlighted the significance of measuring security programs effectiveness to guarantee that education results in practice [16].

[1] identified that the majority of the learning about information security occurred in the workplace, where clear motivations, such as legislation and regulation, existed. It was also found that user's were more than willing to engage with such awareness raising initiatives. From a comparison of practice between work and home environments, it was found that this knowledge and practice obtained at the workplace was transferred to the home environment. Given this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organizational awareness programs and to move towards awareness raising strategies that, whilst deployed in the organization, will develop an all-round individual security culture for users independent of the environment within which they are operating.

[17] identified the ambiguous aspects of current security awareness approaches and the proposed classification provides a guide to identify the range of options available to researchers and practitioners when they design their research and practice on information security awareness.

III. Survey of End Users' Awareness and Practices

Due to the lack of literature focused on end-user awareness and practice, determining the awareness and assessing information security culture in both organization and home place is quite challenging. Additionally, it is possible to assume that most employees perceive information security culture from within the workplace and at home, but the issue lies in determining the level of the relationship between home and workplace practices that encourage a security culture. For this reason, a survey was developed for the assessment of such factors where data were collected and a quantitative method was followed. The survey's primary objectives is to conduct an assessment of the information security culture among workers in terms of workplace and home practices.

The survey is divided into three namely demographics, background of information security awareness, workplace practices and home practices. The workplace practices are geared towards examining the present practice of the workers within their place of work. The survey was distribution to random people who are employed and are regular computer uses at work and at home.

IV. Results & Findings

• *Reliability Test*

The reliability of the survey were measured by analyzing the questionnaire' results to obtain coefficient Cronbach alpha. The most popular test of inter item consistency reliability is the Cronbach's Coefficient Alpha, In general, reliabilities less than 0.60 are considered to be poor, those with above 0.60 ranges are acceptable, and those over 0.80 are good. The Cronbach's Alpha value of this survey is 0.759 that considered an acceptable value.

TABLEI.I. Reliability Statistics

Cronbach's Alpha	*N of Items*
.759	92

After analyzing the demographics, it was revealed that the majority of respondents were male workers with 76.5%, while the remaining 23.5% were female workers. Also, 41.2% of the respondents were from the age range 30-34 years and 35% of the total respondents had at least a degree level of education. This may be attributed to the author's personal contacts who were in the same age group and who have a tendency to be more IT literate or have at least an email account. Most respondents (40%) perceived themselves to be moderate in their awareness level of security culture as presented in Figure 1. It is believed that this proportion of users do not represent the general population and that this would not bias the survey results but it would provide a more informed and accurate response to the survey questions. Therefore, the results showed a positive perspective of the use and knowledge of information security existing within the population at large.

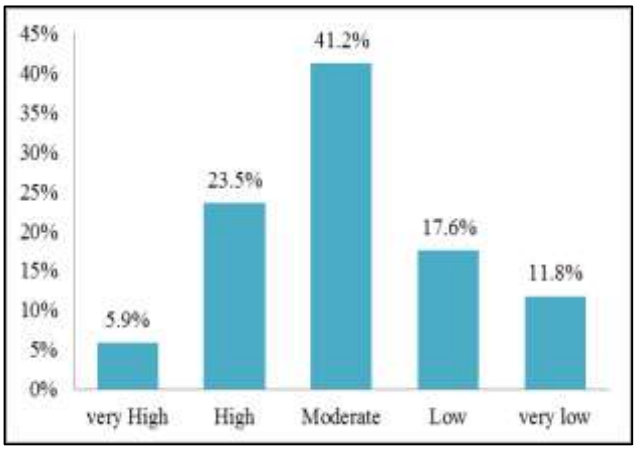

Figure 1. Level of information security awareness culture

• Information Security Awareness Background

The understanding of the information security culture of the workers entailed questions provided to them concerning the information security threats, particularly in question number 2 that is dedicated to Trojan, spam, social engineering (phishing), denial of service, identity theft and hackers. The entire respondents are aware of the virus and Trojan threat as evidenced in Figure 2.

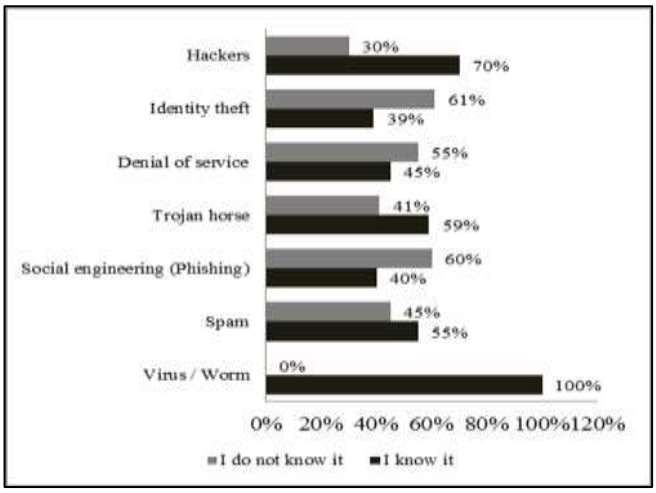

Figure 2. Security threats awareness

- Installing Antivirus

All the respondents (100%) have antivirus in their home computers, indicating that they are all aware of the virus/worm threats and they employ the required safeguard (installing antivirus).

TABLEII. USING ANTIVIRUS AT HOME

	Percent	*Valid Percent*	*Cumulative Percent*
Valid yes	100.0	100.0	100.0

• Information Security Practices at Workplace

With regards to the workplace, the respondents were requested to respond to several questions dedicated towards understanding common security practices. Questions pertaining to these practices are divided into general security practices, practices related to password and security practices related to antivirus and firewall the chosen for these practices it is the common simple practices that could be understood from the respondents.

- General Security Practices

This covers the practice of logging off computers whenever they are using a computer system where 71% of the respondents claim to do so, and steering clear of executable files received in their emails, a practice done by 77% of the respondents (see Figure 3).

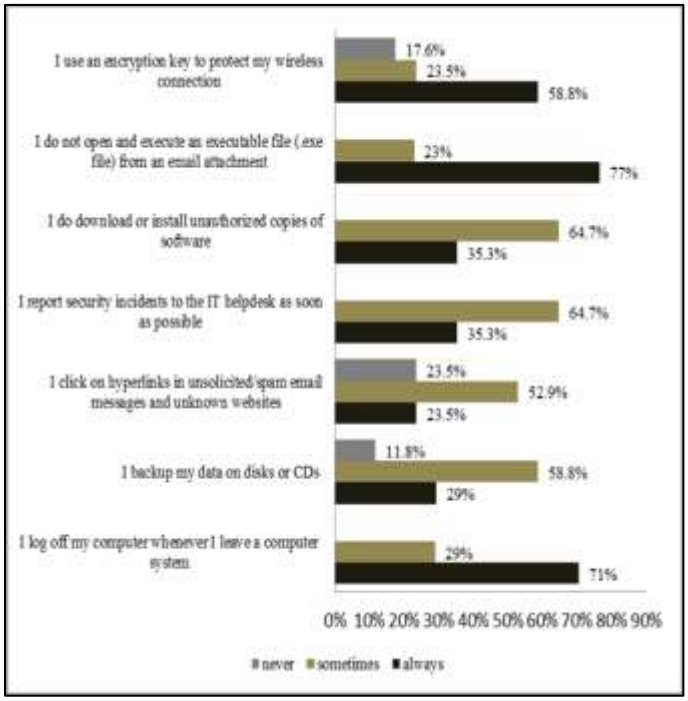

Figure 3. General security practices

- Practices Related To Password

These practices include the use of passwords comprising of at least 8 characters and the use of combined letter (a-z) symbols (!@#$%), where 64.7% of the respondents claim to do so, and keeping passwords confidential - a practice followed by 64.7% of the respondents (see Figure 4).

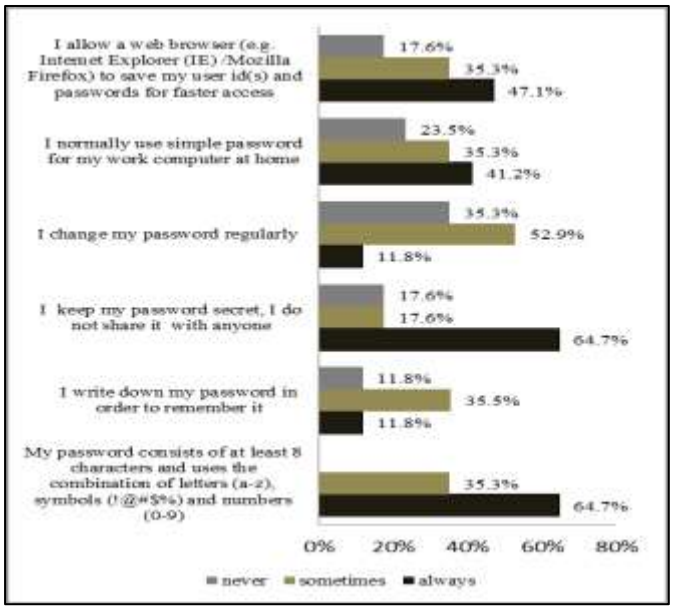

Figure 4. Practices related to password

- Security Practices Related to Antivirus and Firewall

This covers practices such as scanning external disk/thumb drive/USB driver with antivirus prior to reviewing the files within. As evident from Figure 5, 70.6% of the respondents claim to follow such practice (see Figure 5).

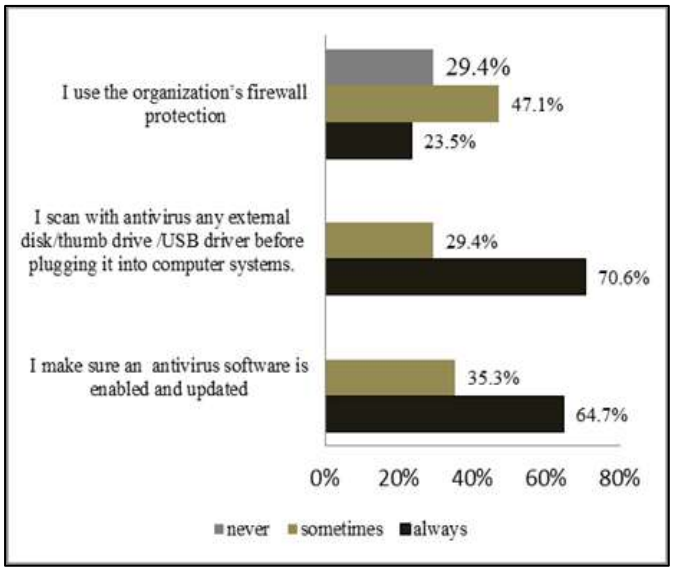

Figure 5. Security practices related to antivirus and firewall

- ***Information Security Practices at Home***

With regards, to their awareness at home, the respondents were asked questions pertaining to common security practices in three different categories, general security practices, practices related to password and security practices related to antivirus and firewall.

- General Security Practices

The majority of the respondents (82%) claimed to log off of their computers when they are done using the system (See Figure 6).

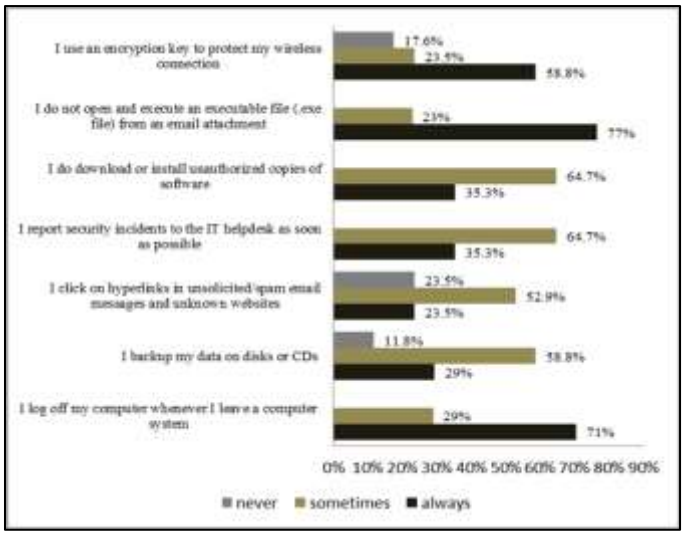

Figure 6. General security practices

- Practices related to password

The majority of the respondents (58.8%) change their passwords regularly as presented in Figure 7.

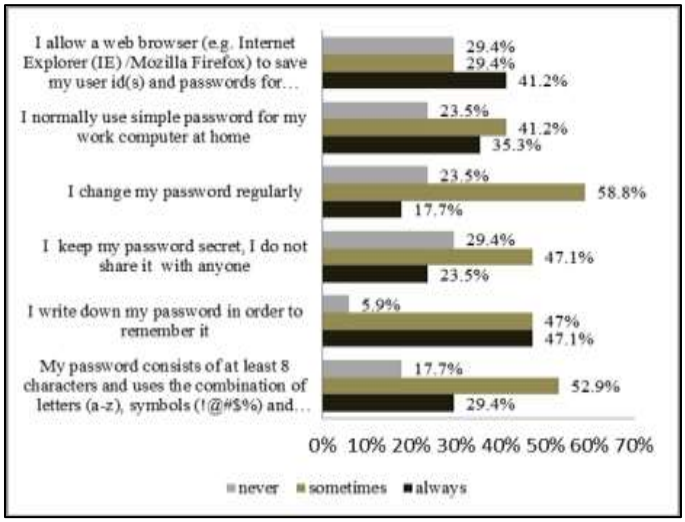

Figure 7. Practices related to password

- Security Practices related to antivirus and firewall

This covers the practice of scanning external disk/thumb drive/USB drivers prior to accessing it in computer systems and 71% of the respondents claimed to follow such practice (Figure 8).

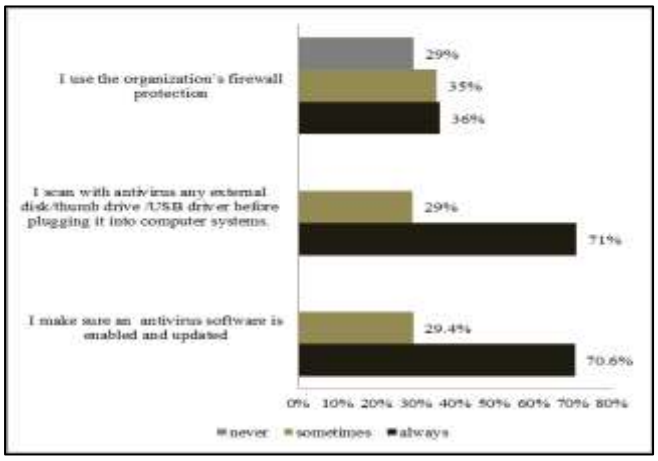

Figure 8. Security practices related to antivirus and firewall

v. Discussions

Overall, the respondents appeared to represent a knowledgeable group of individuals concerning the topic of IS, with majority of them possessing a good level of awareness and practice. However, generalizing the present study's findings to a wider population has to be done with caution as it is anticipated that the levels of IT and security awareness of the larger population is generally lower.

It is identified that practices for both workplace and home could resulted in danger for example downloading/install unauthorized copies of software and click on the hyperlinks in spam email/unknown website still for both practices participants were wrote down their password and use simple password . In addition, allowing browser to save user id and password could expose to insecure behavior if it is broken by hackers.

However, this does not affect the current study's results, although it is crucial to realize that the issue of information security awareness and practice still exists. On a brighter note, the respondents to the survey possess a good level of awareness and practice of IS security both at home and in the workplace.

vi. Conclusions

Good information security awareness should be achieved in the population of Internet users at large if users are to remain security and if e-business is to develop. Awareness at home and within the workplace appears to be of the same level as demonstrated by the survey findings pertaining to the scanning external disk/thumb drive/USB driver prior to accessing their contents, changing passwords on a regular basis and logging off of computers when done using the computer system.

On the other hand, it is identified that practices for both workplace and home could resulted in danger by considering to the survey finding in the following practices such as downloading/install unauthorized copies of software, click on the hyperlinks in spam email/unknown website and writing their password down to remember it.

Future research will focus upon the developing information security awareness framework and in particular look to incorporate other factors such as education background, training, and user behavior, as well as, to identify if there is transferability of the security practices from work place to home or from home to workplace, as well as targeting larger number participants with different backgrounds such as education background, ethnicity and religious.

References

[1] 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*, 2010, pp. 196-203.

[2] R. Richardson and C. Director, "CSI computer crime and security survey," *Computer Security Institute*, vol. 1, pp. 1-30, 2008.

[3] H. Interactive, "Online security and privacy study," 2009, [2, sep,2014].

[4] B. Schneier, *Secrets and lies: digital security in a networked world*: John Wiley & Sons, 2011.

[5] BERR. The 9th information security breaches survey [Online].[4,sep, 2014].

[6] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computers & Security*, vol. 29, pp. 840-847, 2010.

[7] R. von Solms and S. H. von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, pp. 494-497, 2006.

[8] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security*, vol. 2009, pp. 5-10, 2009.

[9] T. Schlienger and S. Teufel, "Analyzing information security culture: increased trust by an appropriate information security culture," in *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, 2003, pp. 405-409.

[10] GetSafeOnline. (2009). *Get safe online with free, expert advice*. [10, sep, 2014].

[11] StaySafeOnline. (2009). *Are your defenses up and your instincts honed?*,[12, sep, 2014].

[12] McAfee. (2009). *McAfee security tips - 13 ways to protect your system,[15,sep,2014]*.

[13] Microsoft. (2009). *Consumer online safety education*.[2, sep, 2014].

[14] NCSA and Symantec, "NCSA-Symantec national cyber security awareness study newsworthy analysis," ed, 2008.

[15] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, pp. 63-72, 2007.

[16] C. C. Chen, B. D. Medlin, and R. Shaw, "A cross-cultural investigation of situational information security awareness programs," *Information Management & Computer Security*, vol. 16, pp. 360-376, 2008.

[17] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating information security awareness: research and practice gaps," *Information Security Journal: A Global Perspective*, vol. 17, pp. 207-227, 2008