An Analysis of Information Security Awareness within Home and Work Environments

Shuhaili Talib[1,2], Nathan L. Clarke[1,3], and Steven M. Furnell[1,3]
[1]Centre for Security, Communications and Network Research (CSCAN), University of Plymouth, Plymouth, PL4 8AA, United Kingdom
{shuhaili.talib, n.clarke, s.furnell}@plymouth.ac.uk

[2]International Islamic University Malaysia, Kulliyyah of ICT, Department of IS, P.O. Box 10, 50728, Kuala Lumpur, Malaysia

[3]School of Computer and Information Science, Edith Cowan University, Perth, Western Australia

Abstract - As technology such as the Internet, computers and mobile devices become ubiquitous throughout society, the need to ensure our information remains secure is imperative. Unfortunately, it has long been understood that good security cannot be achieved through technical means alone and a solid understanding of the issues and how to protect yourself is required from users. Whilst many initiatives, programs and strategies have been proposed to improve the level of information security awareness, most have been directed at organizations, with a few national programs focused upon home users. Given people's use of technology is primarily focused upon those two areas: the workplace and home, this paper seeks to understand the knowledge and practice relationship between these environments. Through the survey that was developed, it was 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.

Keywords-information security; information security awareness; security culture; security management

I. INTRODUCTION

The volume and nature of information security threats has evolved, moving away from technical savvy hackers demonstrating their skill, to organized and well established crackers that aim to receive substantial financial rewards for their efforts [1]. This has resulted in an increase in cybercrime activities and subsequent threats end-users find themselves the target of. For examples, [2] stated that 52% of organizations had encountered threats in 2007. Another survey [3] found that 64% of respondents had encountered a Phishing email – a threat rarely encountered 5 years ago. To safeguard users a range of security countermeasures exist. These tools continually evolve in sophistication and increase in number to counter the changing nature of the threats. 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 [4].

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 with [5] indicating 82% of Enterprise organizations having training programs. Unfortunately, however, this is not necessarily the case for all, with [6], which largely comprises of small-to-medium sized companies (SMEs), indicating only 40% of their respondents conduct training. Whilst many organizations arguably have the resources to provide such training, should they deem it important to do so, they only represent a (95%) proportion of people who use the Internet. The remaining users are typically home-users or the general public. Worryingly, evidence demonstrates that it is this group of users that are most at risk, with 95% of all attacks being focused upon them [7]. Home users have a variety of resources at their disposal in order to improve their awareness of online threats. All the major Anti-Virus providers, Operating System vendors and government initiatives such as [8-10] all provide supporting information to the home user.

Whilst training programs and initiatives exist within both the workplace and home, little research has been conducted to understand what is being taught and where, the effectiveness of such strategies and to what degree learning styles play a role in achieving good information security practice. Information security awareness can be tackled from a variety of different directions, such as within school, government-sponsored initiatives and security providers; however, this paper will specifically focus upon and investigate the behavior, practices and interactions within and between organizations and home environments. The paper is organized as follows: Section II discusses the current state-of-art in information security awareness and the development of security culture. Section III describes the

methodology of the study, with section IV presenting the results. Section V discusses the main findings of the study with the conclusion and future work being presented in Section VI.

II. PRIOR WORK IN INFORMATION SECURITY AWARENESS TRAINING

Information security awareness has been given an increasingly important focus within both academic and commercial communities. Organizations are gradually understanding the importance of their information assets and developing strategies to improve awareness throughout the company. Good corporate governance, regulation and legislation have also helped in raising the importance and relevance of good information security policies and practices [11]. Within academia, focus by researchers has partially moved away from the technical issues towards understanding the end user and developing models and programs that organizations can utilize in developing better awareness [12].

Interestingly, within academia, current research is suggesting that simple awareness strategies that educate employees about particular security topics through traditional mechanisms such as class-room based teaching, online education and poster/email campaigns are not sufficient in maintaining long-term information security practice [13-14]. Rather an increasing volume of research is proposing the need to develop an information security culture within the organization – moving away from surface learning and embedding or indoctrinating good practice within employees [14, 15-17]. The authors of these studies believe through establishing an information security culture in the organization, long-term security practice can be maintained and moreover, the drive towards awareness and education of security issues becomes self-fulfilling, as employees are engaged and proactive about their practice.

Within the context of home users, awareness raising initiatives have been created. Reference [8] is a UK Government sponsored initiative that provides a blanket based approach; providing general information about the risks and how to get protected. The site provides a variety of information from beginnings guides to specific information about relevant threats in a timely fashion. The site is predominately text based information with the addition of occasional video files. Other countries such as the USA have similar national based websites [9]. A number of companies that provide security software and operating systems also provide web-based access to resources – largely reading based – to assist in educating and informing home users [18-19].

Arguably, motivating home users into undertaking security training is challenging as security is always a requirement but never actually the primary task the user is trying to achieve. People often do not have the understanding they need to do it and moreover for those that do, they frequently do not have the time or inclination in any case. Worryingly, evidence demonstrates even when users do think they know about security and how to protect themselves, this is often found not to be the case. A joint study by [20] found that while 75% of home users thought they had spam protection, in fact only 42% actually did. This disparity between what they think they have and actually do have illustrates a significant gap in their understanding.

In order to achieve good security awareness considerable research has been undertaken into developing various learning mechanisms, such as: face-to-face training sessions, email messages, online training, video game, intranet-based access and poster campaigns [21-25]. Whilst focus has been given to what and how to educate within organizations, research has identified the importance of measuring the effectiveness of such programs in order to ensure education leads to practice [26-27]. The Computer Security Institute (CSI) survey reported that 68% of the organizations measure the effectiveness of their awareness training [5]. Unfortunately, no figures were given as to the actual levels of effectiveness of the training. Various approaches have been identified to assist in creating an effective security program, such as, having more user engagement in the process through workshops and providing the training on a continuous basis. [12, 28-29].

However, whilst such strategies might be possible for organizations to utilize, home users would find it arguably difficult to engage for a multitude of reasons: desire, time, resources and the knowledge they need to, to name but a few. Unfortunately, there is little evidence demonstrating whether home users are in fact knowledgeable about information security and indeed practicing it.

III. A SURVEY OF END-USER AWARENESS AND PRACTICES

Given the prior literature in the area, it was concluded that it was difficult to determine the effectiveness of training and moreover where and how they received that training. In addition, whilst it could be hypothesized that the majority of training came from organizations, it is not clear exactly to what extent learning from work and home played a role in information security practice in general. A survey was therefore created to assess these factors. A quantitative method of collecting data was chosen for the study in order to maximize the number of respondents across a broad spectrum of industries and roles. The aims of the survey are:

- To understand respondents general levels of security awareness and practice.
- To understand whether they received training from work and if so, what type and how effective it was.
- To understand the relationship between knowledge gained and practice between work and home
- To understand how people learn and what preferences they have towards various learning styles.

The survey consists of four sections: Demographics; Information Security Awareness; Practice at Workplace and Practices at Home. The Practices at Workplace, sought to investigate the current practice of respondents at their workplace. The section also enquired about the type of training that they have attended and what the learning methods that they have experienced had been and what they preferred. Respondents were also asked about the sources of

information security knowledge in the workplace. This section provided information about the degree of transferability of information security knowledge between home and the workplace. At the end of the section is a list of common security practices that have been created to understand what their practices at their workplace actually are. The final section on Practices at Home sought to mirror much of the composition of the previous section but with a view to practices and education at home.

The survey was distributed to a wide range of people regardless of location but with the condition that they were in employment and regularly use a computer at home and their workplace. The study was undertaken from 20th August – 7th October 2008 (49 days). The survey collection has been stopped when it reached more than the survey target (300) respondents. The survey was promoted via email, based on the authors' academic contacts, personal contacts, from the word-of-mouth and two mailing lists such as Google and Yahoo groups. A total of 333 responses were obtained and the results are analyzed in the sections that follow.

IV. RESULTS

An analysis of the demographics identified that a fairly even split in responses were received from both genders (55% male; 45% female). It was found that the majority of the respondents (55%) were from the age group 25 to 34 and 81% had at least an undergraduate level of education. This could be due to the personal contacts of the author and those who are in the age group are more likely to be IT literate and have at least an email account. Whilst this proportion of users are clearly not representative of the general population, it is not felt this would bias the results of the survey except to provide perhaps a more informed and educated response to the questions. The results therefore probably indicate a more positive perspective on the use and knowledge of information security than what exists within the general population.

A. Information Security Awareness

In order to assess the level of security awareness, respondents were asked to rate their perceived level against a five point scale. Almost half of them (49%) rated themselves at high or very high (as illustrated in Fig. 1). When tied to the question asking respondents what their level of competency is with Information Technology (IT), where 64% stated that they had at least an advanced level of knowledge, it can be surmised that this group of respondents are well educate and informed about IT and Information Security in general.

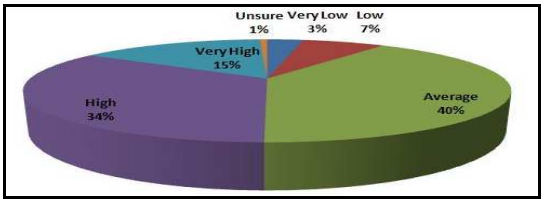

Figure 1. Perceived level of information security awareness.

In order to better understand what aspects of information security respondents understood, they were asked a couple of questions surrounding their knowledge of security threats and their use of social networking sites. Table I presents the results of respondent's awareness of a variety of security threats. Un-surprisingly, the long-standing threats such as Virus and Spam were amongst the highest selected as being understood and newer threats such as zero-day attacks, Botnets and Zombies less understood. Interestingly, whilst 70% understood Phishing, a relatively smaller 44% understood Social Engineering, of which Phishing is an example of. The list of terms also included a couple of fake terms – Phlopping and Whooping – so that it was possible to identify respondents who might be exaggerating their knowledge or providing arbitrary responses. On the whole, relatively small numbers (7-10%) of respondents thought they had heard and understood the terms. That said it is a little concerning that these terms received any acknowledgement at all.

TABLE I. PERCEIVED UNDERSTANDING OF SECURITY THREATS

Information Security Terms	You Understand It (%)	You Never Heard Of It (%)
Virus/Worm	92	0
Trojan horse	80	3
Spam	90	0
Social engineering	44	24
Phishing	70	10
Pharming	24	42
Identity theft	81	8
Key loggers	57	22
Phlopping[a]	7	68
Botnets	33	43
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
Whooping[a]	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24

a. Fake security term

Social networking is a popular Internet activity, which literature has suggested is a common threat vector when looking to obtain information about people for subsequent use in identity fraud [30-32]. Amongst the respondents, 63% indicated they belong to one or more sites. When asked what information they release onto the social network, the respondent group overall appear to be informed and careful about releasing too much information. Table II illustrates

that whilst 59% and 62% are releasing information regarding their real name and email address; only 7% reveal their full postal address. The most worrying statistic is the 45% releasing their date of birth but along with their name this amount of information is unlikely to result in identity theft.

TABLE II. PERSONAL INFORMATION REVEALED BY SOCIAL NETWORKING

Personal Information	You understand it (%)
Real name	59
Email	62
Real date of birth	45
Full address	8
Phone number	14
Personal blog	22
Special occasions	22
Photographs of yourself	67
Photographs of your family members	37
Photographs of your friends	42
Photographs of your office	7
Photographs of your house	8
None of the above	5
Other	1

B. Information Security Practices at Workplace

Analysing the participant's responses with reference to their practices within work, 36% stated their organization provided some sort of training with regards to information security. When comparing this to the size of the organization the respondent works for, it was found that 36% came from SMEs and coincidently 36% also came from Enterprises (an Enterprise being defined as those organizations with 250 or greater employees). Whilst this figure is in line with the 40% stated by [6], which largely canvases SMEs, it falls somewhat short of [5] survey results; 80% (whose respondents are largely but not exclusively Enterprises). A further analysis of those responding on behalf of Enterprises shows that relatively few (3%) come from US-based companies – where regulation and legislation have arguably been prime motivators in ensuring staff are appropriately trained. Of the 36% of respondents who stated their organization provided training, 95% also stated they attended the training sessions.

In order to understand more about security practices in the workplace, respondents were asked about the sources of their information security knowledge. The top three information security sources at work are presented in Table 3; with websites and search engines the most popular. Arguably this could be due to many organizations now providing open access to the Internet. This freedom permits the employee to search and locate information of value at the time required. In addition to asking what their top three sources of information security knowledge were, they were also asked what they prefer. Interestingly, the results from these two questions came out identically, illustrating user's already have the freedom of choice when it comes to learning about information security and organizations are not burdening them with approaches they would not prefer.

From Table III, it is evident that much of the knowledge for Information Security within a workplace comes from fairly informal means – web searches and informal discussions with colleagues. Interestingly, these results do illustrate the importance and relevant of the organizational policy in informing employees and moreover practice.

TABLE III. TOP THREE SOURCES OF INFORMATION SECURITY & LEARNING AT WORK

Top Three For Information Security In The Workplace		Top Three Most Preferred Sources For Information Security In The Workplace	
1	Websites and search engines	1	Websites and search engines
2	Informal discussions with colleagues and professional contacts	2	Information discussions with colleagues and professional contacts
3	Organization's policy	3	Organization's policy

This freedom of choice of how to learn comes through again when the respondents were asked about where or how they received their training. 28% of respondents responded that it was through self-study. As illustrated in Fig. 2, the remaining options received a fairly even split, indicating that if organizations are willing to invest in training their staff, the methods utilized will vary with no single option being a considered standard. Interestingly, further analysis of these responds when taking into account the size of the organization found that the preferred training type was independent of the organizational size, with SMEs willing to invest in outside experts as much as Enterprises – countering the standard assumption that SMEs do not have the resources to pay for training and would rely upon less expensive options such as self-study or online training.

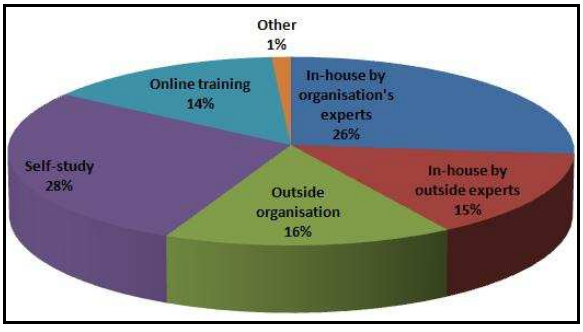

Figure 2. Preferred training type.

Respondents were also asked how frequent they would like to have security training. As Fig. 3 illustrates, the largest proportion of users preferred to have an on-demand service, with the majority of the remaining respondents split between monthly, quarterly, half-yearly and yearly. Overall 95% of respondents felt they needed some level of training.

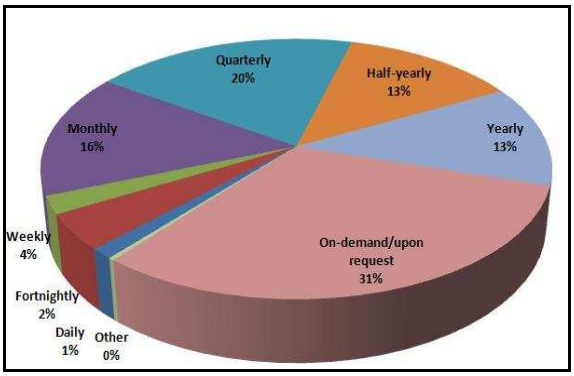

Figure 3. Respondent preference to having information security training.

C. *Information Security Practices at Home*

In order to compare practice from the workplace and home, respondents were asked a series of questions with respect to their practice at home. When analysing the top three sources of acquiring information security knowledge and what sources they preferred to learn from, it can be seen that the lists were identical, with web searches coming out first, what they had learnt from the workplace second, and reading newspapers and magazines third (as illustrated in Table IV). Upon reflection, this correlation should be expected as within the home environment you have complete freedom over what and how you learn. The user is not forced through employment to attend training courses or learn in a specific manner depending upon how the organization has decided to implement training. This freedom provides the user with the opportunity of using learning approaches that are preferred and most convenient to the individual. Arguably, without the formal training approaches that organizations utilize it is difficult to understand the depth of learning that goes on at home – with much of the learning likely being a result of news articles and press coverage of a particular event. A further research that focused on the level of understanding of information security knowledge acquired at home would be required to further explore on this aspect.

TABLE IV. TOP THREE SOURCES OF INFORMATION SECURITY & LEARNING AT HOME

Top Three For Information Security At Home		**Top Three Most Preferred Sources For Information Security At Home**	
1	Websites and search engines	1	Websites and search engines
2	From what I learnt at my workplace	2	From what I learnt at my workplace
3	Daily newspaper and Magazines	3	Daily newspaper

That said, the results from Table IV do illustrate the users are willing and do learn at home. Interestingly, the second most preferred source of information is what they learn from the workplace. Acquiring knowledge about information security within the workplace has an impact upon the level of awareness and learning at home.

In addition to understanding how they learn, respondents were also asked how frequent that learning takes place. Fig. 4 presents the breakdown of responses. 71% of respondents undertake some level of training at home with 39% performing this on average on a monthly basis and 25% weekly. Whilst the regularity of the training is somewhat infrequent, given the lack of motivation within the home environment to undertake training, it is encouraging to note that over two thirds are willing to undertake some level of training at home.

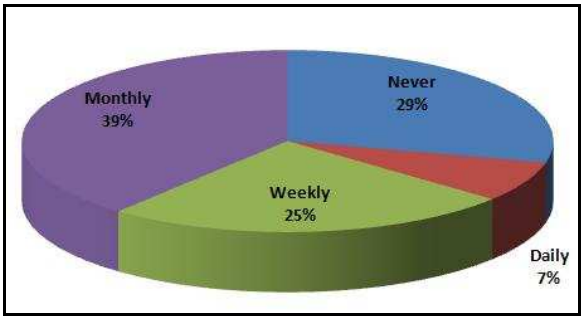

Figure 4. How frequent learning takes place at home.

Given that the proportion of users not willing to learn at home and the proportion that learn on a monthly basis make up 68% of the respondents, the need to acquire the knowledge necessary to ensure they remain secure at home is imperative. Arguably therefore, the knowledge users obtain within the workplace and subsequently transfer into the home environment is key to establishing a level of information security awareness for many respondents. Without such transference, a good proportion of home users will have little or no security awareness.

D. *Effectiveness of Information Security Training*

Having established training practices at home and the workplace, the survey proceeded to understand the extent to which this training and practice was effective. A total of 115 of the total respondents received training, 115 did not and the remaining claimed that they are not sure they have attended the training. Whilst training, awareness and practice are arguably associated with each other, simply undertaking training or having an awareness of an issue does not necessarily imply practice.

To this end, Fig. 5 provides a comparison between those respondents who undertook training and what they considered their level of security awareness is. A total of 67% of respondents who undertook training felt they had a high or very high level of awareness. This compares to just 43% who had not received training. This demonstrates

respondents at least perceive they have a better understanding of the information security threats and countermeasures over those that have not received training.

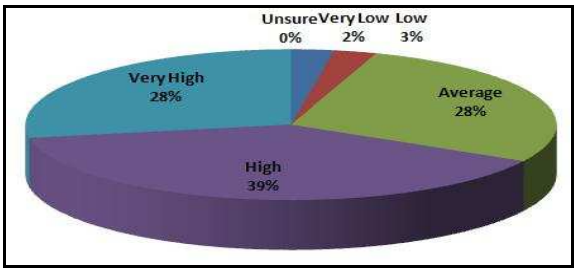

Figure 5. Respondents who attended training and their awareness level.

TABLE V. PERCEIVED UNDERSTANDING OF SECURITY THREATS BASED UPON WHETHER TRAINING HAD BEEN PROVIDED

Information Security Terms	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Virus/Worm	97	93
Trojan horse	94	77
Spam	94	88
Social engineering	58	40
Phishing	81	67
Pharming	34	20
Identity theft	85	81
Key loggers	72	55
Phlopping[a]	10	5
Botnets	50	28
Zombies	50	30
Denial of service	75	56
Packet sniffer	65	48
Whooping[a]	17	8
Hacker	97	95
Zero day attacks	45	23
Cracker	73	55

a. Fake security term

A further analysis of respondents' understanding of various security threats based upon whether they had undertaken training or not also reveals those with training on the whole have a better understanding of terms. As illustrated in Table V, all security threats were better understood by those with training than those without – unfortunately, this also included the fake terms. Whilst the difference between those that had training and those that did not are not large (from 3%) for many of the terms, it is worth noting the large proportion of respondents in this survey who regard themselves as advanced users. It is therefore anticipated that this difference would be larger under normal circumstances. It is also noticeable that while the difference is small on well established threats such as virus, worms and spam; less established threats such as Botnets and Zero-day attacks have a significantly larger difference between those with and without training.

TABLE VI. INFORMATION SECURITY PRACTICE OF RESPONDENTS

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I log off my computer whenever I leave a computer system	50	37
I backup my data on disks or CDs regularly	35	22
I check that antivirus software is enabled and updated	69	60
I use the organization's firewall protection	72	56
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#$%) and numbers (0-9)	72	45
I keep my password a secret and only I know it	84	61
I change my password regularly	23	9
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	43	27
I report to security incidents to the appropriate parties	33	14
I look for "https://" or the "little gold padlock" before I make financial transaction online	60	54
I protect confidential files with passwords	36	23
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	34	17
I ensure nobody is looking at my keyboard each time I key in my password	57	37

In terms of understanding how training effects actual practice, respondents were asked several questions about common security practices. Table VI illustrates the findings from these questions based upon whether they had undertaken training or not. More significantly from these results it is identifiable that a bigger difference exists in practice between those that had training and than those that did not. A good example here is the use of strong passwords for user authentication, with 72% of those trained using them but only 45% of those un-trained doing so. Training

therefore is arguably having a positive effect not only upon awareness but also on actual practice. Unfortunately however, it is also evident that the level of practice amongst the trained respondents is not necessarily as high as would be liked with certain practices such as changing passwords and reporting incidents as low as 23 and 33% respectively.

In order to understand the effectiveness of users practice at home based upon whether they had received training, participants were asked a series of questions. Table VII illustrates that practice at home for those respondents with training is significantly better than those without – with practice differing from 7 to 17%. Similarly with the previous question, the level to which trained user's are actually following good practice is worryingly low, highlighting some potential concerns over the nature and type of training been undertaken.

TABLE VII. INFORMATION SECURITY PRACTICE AT HOME

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I shred confidential documents before throwing them into the bin	50	38
I change the default password for my router	53	36
I use encryption key to protect my wireless connection	58	51

Security controls are one of the first defense layers that protect users from security threats. The survey finally tried to understand what kind of security controls were used by respondents while at home. The results are shown in Table VIII. Even though respondents do not receive training, 97% of them are using Antivirus at home. This could be related with the results discussed in the previous section where 92% of them are aware of the virus/worm threats and take necessary action such as installing Antivirus. Overall, there is no significant difference between those who received training and those who did not. However, the results do demonstrate that those trained respondents are still marginally ahead of those who are not in using security controls at home.

TABLE VIII. RESPONDENTS' USE OF SECURITY CONTROLS

Security Controls	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Antivirus	98	97
Firewall	78	72
Anti-phishing	45	38
Anti-spyware	75	75
Intrusion Detection Systems (IDS)	20	18
Spam filter	67	66

V. DISCUSSION

On the whole, the participants represented a well-informed group of individuals on the topic of Information Security, with respondents generally having a good level of awareness and practice. Care should therefore be given in generalizing these results to a wider population as it is anticipated that the levels of IT and security awareness would be generally lower. Whilst this does not affect the key results of the survey, it is important to realize that the problem of achieving information security awareness and practice still remains. Indeed, even within this well educated demographic, 50% of them felt they had an average or lower level of awareness.

Whilst establishing the effectiveness of awareness training is not a simple task, the results have demonstrated that respondents whom have undertaken training are more aware of a greater variety of security issues – particularly threats. With the ever-changing security landscape and people's increasing adoption of technology, the need to maintain up-to-date levels of awareness is imperative if users are to remain secure. Indeed, the last few years alone has seen a significant increase in security threats that focus upon the human-factor, such as Phishing, that countermeasures were unable to protect against. Only through relevant and timely training can security be maintained.

Encouragingly, when looking at the motivations of participants in undertaking some form of education on information security, respondents appear very willing to engage to some degree both in home and workplace environments. Unfortunately, however, the volume and depth of such education is lacking in places – with only 36% of organizations willing to invest in security education and home users arguably lacking in credible, structured learning, given their focus upon web searches and news reports. What is evident from the findings is the participant's freedom of choice when looking to learn about security – both in terms of what they learn and how. Flexibility therefore appears to be an important consideration, so that users are able to learn what topics they want, in a manner or learning style they prefer, at a time and location they feel most comfortable in.

As motivation of home users will inevitable be problematic due to the various constraints of every-day life, focus therefore arguably has to be placed upon what can be achieved in the workplace. With 95% of participants who have training provided; attending, and home users stating that what they learn in the workplace is key to what they practice at home, leveraging workplace learning could potentially be very useful in establishing good security practice independent of the environment. The workplace environment is also better placed to ensure a credible and structured security awareness program is in place to ensure important aspects of knowledge are not missed. Industry therefore has an important role to play in educating employees on the subject of information security awareness; however, it is important to ensure such training is not too specifically focused upon any particular company's processes and is easily generalizable so that employees are able to apply such knowledge within the home environment.

VI. CONCLUSIONS

Achieving good information security awareness in the general population of Internet users is imperative if they are to remain secure and electronic business is to thrive. Unfortunately, educating users about the threats and countermeasures in a dynamic environment like security requires time, resources and motivation. Comparing the home and work environments, it is clear the latter provides more opportunity for such education to take place – with companies motivated to provide training due to changes in legislation, regulation and governance. The survey findings have already demonstrated that leveraging this transference of knowledge from the workplace to home is already underway.

Whilst the workplace provides a good opportunity to educate users about information security, it has also become apparent that care needs to be taken when looking into what they are taught, when they are taught it and how they like to learn. Given the mixture of: differing priorities of business; cost; the varying degrees of prior knowledge of security from employees; and the differing pedagogies required, it follows that a highly flexible framework is required that is capable of tailoring information security awareness training to the individual across all environments: work and home. Future research will focus upon the developing such a framework and in particular look to incorporate other factors such as psychological profiling in order to maximize the learning experience but importantly also ensure that learning follows through to practice.

ACKNOWLEDGMENT

The authors would like to thank to Ministry of Higher Education Malaysia and the International Islamic University Malaysia for their funding of the scholarship for this research.

REFERENCES

[1] S. Hinde, "Hacking gains momentum," Computer Fraud & Security, vol. 2004, pp. 13-15, 2004.

[2] R. Richardson, "2007 CSI computer crime and security survey," in The 12th annual computer crime and security survey: Computer Security Institute, 2007.

[3] Harris Interactive, "Online security and privacy study," 2009.

[4] B. Schneier, Secrets and lies. Indiana: Wiley Publishing, Inc., 2000.

[5] R. Richardson, "2008 CSI computer crime & security survey," Computer Security Institute 2008.

[6] BERR, "The 9th information security breaches survey," Department for Business Enterprise and Regulatory Reform & Pricewaterhouse Coopers, United Kingdom 2008.

[7] Symantec, "Symantec Internet security threat report - Trends for January - June 2007," Symantec Corporation 2007.

[8] GetSafeOnline, "Get safe online with free, expert advice." 2009.

[9] StaySafeOnline, "Are your defenses up and your instincts honed?." 2009.

[10] WebWise, "The BBC guide to using the Internet." 2009.

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

[12] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, "Information security: The moving target," Computers & Security, vol. 28, pp. 189-198, 2009.

[13] G. Rotvold, "How to Create a Security Culture in Your Organization," Information Management Journal, vol. 42, pp. 32-38, 11 2008.

[14] 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.

[15] B. von Solms, "Information Security -- The Third Wave?," Computers & Security, vol. 19, pp. 615-620, 2000.

[16] P. A. Chia, S. B. Maynard, and A. B. Ruighaver, "Understanding organizational security culture," in Sixth Pacific Asia Conference on Information Systems Tokyo, Japan, 2002, pp. 731-740.

[17] T. Schlienger and S. Teufel, "Analyzing information security culture: Increased trust and appropriate information security culture," in 14 th International Workshop on Database and Expert Systems Applications, 2003 (DEXA'03) Prague, Czech Republic, 2003.

[18] McAfee, "McAfee security tips - 13 ways to protect your system." 2009.

[19] Microsoft, "Consumer online safety education." 2009.

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

[21] C. C. Wood, "Information security awareness raising methods," Computer Fraud & Security Bulletin, vol. 1995, pp. 13-15, 1995.

[22] P. Spurling, "Promoting security awareness and commitment," Information Management & Computer Security, vol. 3, pp. 20-26, 1995.

[23] S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," Information Management & Computer Security, vol. 8, pp. 131-143, 2000.

[24] 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.

[25] ENISA, "The new users' guide: How to raise information security awareness," European Network and Information Security Agency 2008.

[26] M. E. Thompson and R. von Solms, "Information security awareness: Educating your users effectively," Information Management & Computer Security, vol. 6, pp. 167-173, 1998.

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

[28] E. Albrechtsen, "A qualitative study of users' view on information security," Computers & Security, vol. 26, pp. 276-289, 2007.

[29] M. H. Cooper, "Information security training: lessons learned along the trail," in Proceedings of the 36th annual ACM SIGUCCS conference on User services conference Portland, OR, USA: ACM, 2008.

[30] BBC, "Web networkers 'at risk of fraud'," 2007.

[31] H. Wallop, "Fears over Facebook identity fraud," Telegraph Media Group Limited, 2007.

[32] D. Adlam, "Social networking identity fraud," 2009.