AN EFFECTIVE METHOD FOR INFORMATION SECURITY AWARENESS RAISING INITIATIVES

AliMaqousi[1], TatianaBalikhina[1], Michael Mackay[2]

[1]Petra University, Faculty of Information Technology, Jordan
amaqousi@uop.edu.jo, tbalikhina@uop.edu.jo
[2] Liverpool John Moores University, UK
M.I.Mackay@ljmu.ac.uk

ABSTRACT

Increasingly, all kinds of organizations and institutions are adopting the E-business model to conduct their activities and provide E-Services for their customers. In the process, whether they know it or not, those organizations are also opening themselves up to the risk of information security breaches. Therefore protecting an organization's ICT infrastructure, IT systems, and Data is a vital issue that is often underestimated. Research has shown that one of the most significant threats to information security comes not from external attack but rather from the system's users, because they are familiar with the infrastructure and have access to its resources, but may be unaware of the risks. Moreover, using only technological solutions to protect an organization's assets is not enough; there is a need to consider the human factor by raising users' security awareness. Our contribution to this problem is to propose an Information Security Awareness Program that aims at raising and maintaining the level of users' security awareness. This paper puts forward a general model for an information security awareness program and describes how it could be incorporated into an organization's website through the process of development life cycle.

KEYWORDS

Information security awareness program, E-business, Security Policy, Security Culture

1. INTRODUCTION

Increasingly, a wide range of profit or nonprofit, public or private, organizations rely on Information and Communications Technology (ICT) to conduct their businesses, in particular organizations that offer their services online. In doing so, those organizations expose themselves to the risk of information security breaches especially in the case of smaller businesses who lack extensive ICT support services. Therefore, developing appropriate and affordable mechanisms to protect an organization's ICT infrastructure, systems, and data is a vital issue. One of the most significant threats to information security comes from the system's users, because they are familiar with its infrastructure and services but they may not be aware of the security policies in place to protect them and their significance. This reaffirms the finding that it is not always dissatisfied workers and corporate spies (so called insider attacks) that cause problems but often, it is the non-malicious, uninformed employees (users) that pose the greater threat [1].

E-Business refers to the use of ICT by organizations that gives them the capacity to offer online services, transform relations with customers, businesses, and other organization's departments. Any organization can deploy E-Business as a means to improve the internal workings of its operations, the relationship with its customers who consume its services, and manage its

DOI : 10.5121/ijcsit.2013.5206

relationships with other businesses. Researchers usually split IT users into categories such as home user, business user, and academic user [2,3,4] to differentiate levels of competence but this can often be misleading. In this paper we focus on the novice(business) users of an organization's intranet who may be unskilled in ICT but will nevertheless have access to the organization's IT resources.

Often huge amounts of money and time are invested by organizations into technical solutions to security issues while the human factor receives less attention. Technical solutions are of course necessary to address vulnerabilities such as viruses, denial of service attacks, and prevent unauthorized access. However, the involvement of humans in information security is of equal if not greater importance and many examples of security issues such as "Phishing" and Social Engineering exist where any technical solutions can be subverted by misleading the user [5]. Therefore, user information security awareness is a major component within industry good practice for security. In short, we argue that, rather than focusing purely on developing increasingly restrictive technologies and policies that often restrict usability, organizations should focus on making users intrinsic to the security process through education, training, and awareness.

We propose that, in addition to any technological security solutions deployed, an organization has to have an information security awareness program for its users. In this paper we present our approach to build a user-oriented security awareness program to increase and maintain a certain level of user awareness to the risks of ICT and reinforce good security practice. The Information Security Forum (ISF) one of the world's leading independent authorities on information security defines information security awareness as: "An ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioral change" [6]. This could be implemented alongside the organization's website and/or within specific organizational administration tools. This is fundamental to ensure that all staff acts in an appropriate manner to keep sensitive information secure given the broad increase in reliance on IT systems and information stored electronically. This is made all the more pressing due to the extraordinary increase in the use of Internet services to support internal business processes and the advent of Cloud Computing [7, 8, and 23]. This risk is further increased through the availability of personal electronic equipment such as tablet PCs and smart-phones, which are able to communicate wirelessly with many other devices and have massive internal storage capacities [9, 24].

The remainder of this paper is organized as follows; section 2 will present an overview of existing approaches to maintaining user security and awareness raising approaches. Section 3 will describe our methods for conducting an awareness raising program and then explain our experimental design. Thereafter, section 4 presents our approach to raising security awareness among users and section 5 abstracts this to define our overall approach. Finally, we conclude in section 6 with some final thoughts and an outline for further work.

2. RESEARCH OVERVIEW

The growth in organizations using ICT for E-Business imposes the need to develop extensive and robust computer and mobile security mechanisms. These mechanisms are largely intended to help organizations protect their assets, such as information, databases, programs/services, and hardware from any inadvertent or malicious harm or damage with the minimal level of user knowledge or input. The level of severity obviously varies from one case to another and depends largely on the users' awareness of possible harm and damage, their knowledge of the source of threats, and whether they are applying security good practice or not [2,3].

The problem of lax security awareness among non-malicious users has long been recognised as a significant vulnerability in any IT system. A 2005 report from Mcaffee [10] highlighted the following statistics:

- "One in five workers (21%) let family and friends use company laptops and PCs to access the Internet".
- "More than half (51%) connect their own devices or gadgets to their work PC... a quarter of who do so every day".
- "One in ten confessed to downloading content at work they should not".
- "Two thirds (62%) admitted they have a very limited knowledge of IT Security".
- "More than half (51%) had no idea how to update the anti-virus protection on their company PC".
- "5% say they have accessed areas of their IT system they should not have".

The impact of these bad practises are reaffirmed in the most recent report for Q1 2012 [11] which demonstrates that many of the common exploits targeted at unwitting users continue to thrive. The development of an effective Information Security Awareness Program is therefore recognised as a cornerstone for the effective protection of IT infrastructures and there has been a significant amount of research work done in order to establish the most effective approaches to this. For example, in the United States, the National Institute of Standards and Technology (NIST) published a report to guide firms in building an Information Technology Security Awareness and Training Program [12]. This is just one example of the broader movement towards security awareness and many organisations now publish such information for their employees [13] or for the general public at large [14, 15].

Fundamentally however, this research is done either from an academic or managerial perspective and less consideration is typically given to tailoring this to a specific user base or company. Whether it is due to educational, regional, cultural, or ethnic reasons, groups of users will respond differently to any programs or policies which aim to govern how they interact with ICT [16]. As such, more recent works focus on how to effectively 'segment' the audience to refine the program and produce a more fine-grained security approach [17]. These efforts propose 5 steps to more effectively identify and engage users into security awareness:

1. Ascertain the current level of computer usage
2. Understand what the audience really wants to learn
3. Test how receptive the audience is to a security program
4. Examine how to gain acceptance
5. Research who might be a possible ally

2.1 Progressive development in an Information Security Awareness Program

Once the target audience has been selected and engaged, the next task is to consider the level of awareness that is necessary and desirable for users to reach. Of course, any organisation must be realistic in defining what is achievable through such a program based on the level of user expertise, the available resources to implement the program, and the overheads involved. Four levels of awareness can be identified here which represent increasing stages of user understanding: All Users, IT aware Users, Trained IT users, and IT specialists. The transition between each level can also be broadly understood in terms of the types of engagement required, a summary of which is presented in figure 1 below:

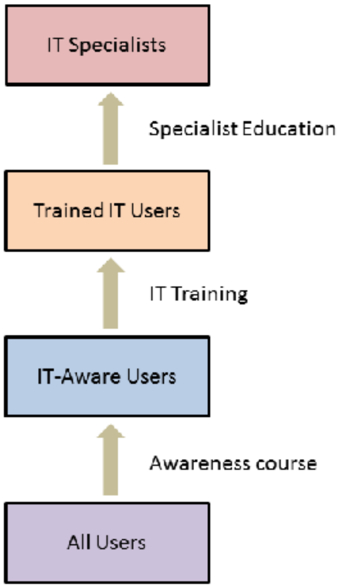

Figure 1- User transitions in Information Security Awareness

This diagram shows that some effort is necessary in order to promote users from the lowest, uninitiated, level to the first stage where they have some basic awareness of IT security issues. This may be intrinsically present in some cases, in a ‘western’ university environment for example, where one can assume that by virtue of being immersed in an IT environment some basic awareness is imbued in to users by default whereas this may require an explicit step in other cases [15, 18]. Beyond this, a degree of formal training is required in order to transition users to the next step up where some assurance is present that the users have been trained in IT security issues and will adhere to a formal security policy. This is considered to be the ideal level of awareness in organisational environments. Moving upwards, there exists a higher level of training where education is provided to impart a level of IT specialism to users. This may however only be necessary for users who need to understand the underlying complexities in order to develop further protection or update existing mechanisms, i.e. IT support staff.

2.2 Developing an Information Security Awareness Program

Past research has also highlighted the importance of the proper development of an awareness program that not only considers how it should be implemented but also how it can be used to maintain user awareness going forward [19]. In total, four stages have been defined in order to deliver an effective program; Analysis, Design, Implementation, and Maintenance.

The steps discussed above such as user identification and training level represent the core points of the *Analysis* stage. This should also be put in an organisational context by first conducting a needs assessment and then refined to establish more fine-grained priorities. The *Design* stage will then take the output of the analysis and develop awareness training material based on the critical topics that have been identified, and select the optimal means to deliver them. From there, the *Implementation* stage will present the awareness program to users in an effective manner [20] and incorporate a feedback mechanism to refine further delivery based on user response. Beyond this, the program should include a fully considered *Maintenance* stage that measures user compliance and plans for further developments, perhaps as part of a wider professional development program.

This paper aims to present the best practices of how to present (methods of implementing) a web-based security awareness program for an organizations users. The specific focus of this work is to highlight the relationship between an organization's website and its information security awareness program. This relationship is an amalgamation one. We believe that by including the information security awareness program into the organization's website, it will contribute positively to increasing the level of users' security awareness while ensuring the program is sustainable. This solution is an alternative to having a separate mechanism for promoting the security awareness program.

3. METHODS OF CONDUCTING INFORMATION SECURITY AWARENESS RAISING

As we have seen, continuous education, and training are the best practices to conduct any information security awareness program. Learning from previous experience is a good way to develop future working plans and, in this regard, in order to build a security awareness culture we need to learn from previous lessons and avoid their mistakes. Two decades ago when organisations started to use personal computers in conjunction with the Internet, they asked their users to be aware of and use simple security measures, such as employing user-names and passwords, and installing antivirus software. Nowadays changes in technology challenge users to become ever more immersed with computers and the Internet, and, therefore stronger and more thorough security issues should be introduced and enforced. For example, the South Carolina Department of Revenue IT Security failure happened when hackers managed to get valid user credentials and use them to gain access to sensitive files. The credentials were handed over when a user clicked on a malicious email link [21].

Increasing the level of user awareness can be achieved most quickly by building a security awareness culture. As an example, using strong user-names and passwords is now deeply incorporated in our daily working actions not just for logging onto computers but when accessing any online service. The results in [2] show that the majority of surveyed users (96%) believe in the importance of using user-name and password and 97.5% are using them. This result has been achieved because of: firstly, the academic environment they belong to, and secondly, many years have passed since E-Society encouraged and in many cases enforced the use of user-name and passwords. We want to build upon this experience to promote mass collective education as a means of increasing the level of users' security awareness both in the academic and wider environment. Of course, this is just an example of how a security culture can be manifested, other examples include:

- User education and training
- Analysis of user behaviors
- Setting organizational policies and regulations
- Monitoring for compliance to policies and regulations.
- Identifying security threats and vulnerabilities
- Deploying effective security tools and instruments.

3.1. Experimental Approach

In previous works [2, 3] we presented the results that show the importance of raising users' security awareness where, in summary, we surveyed a range of educational organization's employees to gather information and statistics about the current level of user's security awareness. We also interviewed computer center staff at an organization to identify the challenges faced when dealing with problems caused by users, to learn about the frequency of breaches, and to understand the computer center's wider security goals. Based on this, we created a number of posters to be distributed at different locations around the organization premises and developed a security awareness website to be used by the organization's users (employees and students). We also conducted security awareness sessions and workshops that aim to introduce users to the organizations security policies and available tools. We consider this work as a necessary first steps towards achieving the overall objective of the program. The main outcomes of this work showed the importance of measuring the level of security awareness levels among the organization’s users. In few areas this level was acceptable but in many others this level was low and needed to be raised to avoid the potential of security issues.

One of the challenges in the process of designing and developing the security awareness program is collecting the right material for targeted groups of users. As an example, a poster that includes technical tips in a number of steps may be appropriate for an educational organization’s users while a poster with more drawings is better for another type of users. Another example, advanced and up-to-date security tips could be presented to skilled IT users while simple and more basic tips will be more appropriate for novice-IT users. Having the material ready for use by the implementers, it can then be distributed via different available communication channels. One of the most powerful communication tools is the organization’s website which can be accessed by the organization’s intranet users. Our primary goal is therefore to explore how this mechanism can be used to disseminate the information security awareness program and how this forms an important part of the security life cycle

4. METHODS OF DISTRIBUTING THE SECURITY AWARENESS PROGRAM

In order to drive towards continuous user education, we have designed and developed a website for disseminating our information security awareness program. This channel of distribution is the best candidate amongst other mechanisms as it intrinsically satisfies the requirement for reaching a large number of targeted users as the employees and students of the organization will likely be the prime users of website. The website includes several ways to educate users and to keep them informed with the latest news, updates, and training that might be used to secure users' and the organization’s assets. One of the other main services provided by the website is the possibility to enable users to participate in different periodic surveys to monitor awareness.

Moreover, the website provides a channel for IT Support staff to distribute necessary information and updates on security issues to keep organization’s users informed with emerging security threats and vulnerabilities. It also works as an E-learning tool to conduct training on topics related to users security awareness such as how to use a certain security tool. Moreover the website has many other ancillary features such as poster galleries, forums and bulletin boards, and blogging.
One issue we identified after initially implementing the program was deploying it as a separate website, which had the effect of limiting the number of website visitors as it was designed and developed as an independent entity. The reasons for this limitation were: first; the website popularity as the URL is not well known for users. Second; users usually don’t see a reason to browse a security website when he/she has no perceived security problem. For three months of publishing the website we recorded less than 1% of potential users who had accessed the website.

4.1 Awareness Program Analysis

As a result of these findings we decided to incorporate the information security awareness program into the organization’s website. By doing this we aim to have a clear component built straight into the website so all registered users will be able to locate and use the program easily. This is an especially powerful mechanism where organizations default their browser homepage to their website.

In order to generalize this process into any website development life cycle, we have conducted a seminar with 30 web developers gathered at a specialized workshop for web developers in the Arab world [22]. A survey that was performed at the workshop highlighted the following facts:

- 53% of surveyed web developers are not familiar with information security awareness programs.
- Only 18% of surveyed web developers confirm the existence of information security awareness program on their websites.
- 33% of those who answered positively on the existence of information security awareness program on their website indicate that they don't use a reference model for development.
- Only 10% of surveyed web developers confirm that the material of information security awareness program is presented explicitly.

The above facts formed the basis for us to propose adding a requirement of information security awareness programs to be added into the requirements phase of any web site design methodology such as the waterfall model.

5. GENERAL MODEL

In this section we propose our general model for an Information Security Awareness Program (ISAPM). Figure 4 shows our model which is built around seven core blocks. This model has been adopted based on the proven concept of educating users is the best practice to increase users security awareness level. Any organization starts its program by learning its own security goals. This information will be used to design the program, after that the program will be developed and implemented. Maintaining the program is also a crucial stage, which aims to keep the program running with up to date information. As the aim of the program is to raise security awareness, it is necessary to measure this on a regular basis. Finally, it is important to review the program by taking into consideration the results of these measurements with any changes in the organization's security goals feeding back into the design block for any further updates. In this work we have focused on the design and development blocks and we leave details of other blocks for further work. However, we will give a brief description of the whole model in this section.

The requirements process in the model starts with identification of organization's security goals. This initial process includes interviewing computer center staff (and the staff responsible for managing and running computer and Internet services in the organization). The purpose of these interviews is to identify and understand the organization's security goals, taking into consideration the nature of its business, it's customers' needs for computer and Internet services, it's employees qualifications and expertise, the methods of IT security employed and existing policies and procedures.

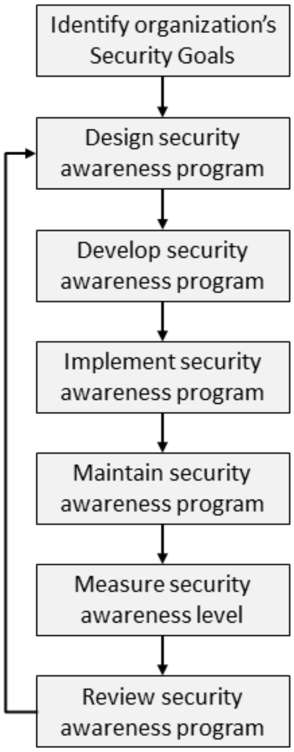
Identify organization's Security Goals
Design security awareness program
Develop security awareness program
Implement security awareness program
Maintain security awareness program
Measure security awareness level
Review security awareness program

Figure 4 – The ISAPM model

The design process mainly concerns identifying the required program elements that should be included in the security awareness program. Among the program's elements could be guidelines booklets, posters, awareness training workshops, online forums to enable users to interact, alert and news sections, and online surveys and statistics. Such a system needs to be easily accessed, have clear content, and be interactive by utilizing different multimedia elements.

The development process of the security awareness program can be done using a range of web based development tools such as ASP.NET or PHP. The decision should be made based on available resources and developers' expertise. The system should be built based on the concept of a Content Management System (CMS) to provide an online platform for enabling users' contributions to enrich the system's content and emphasize their responsibilities towards raising security awareness for all.

The implementation process includes selecting one of three ways to run and distribute the program: as part of the organization' website, as part of organization's administrative tools, or as a separate website. We propose in this paper to integrate the program within the organization's website for the reasons discussed in section 4. We believe this solution will increase the visibility of the program and make it more accessible to all organization's users.

The maintenance process includes defining a procedure to maintain the program by consistently providing up to date and appropriate content. To ensure proper maintenance, the organization should employ skilled staff that are qualified to run and maintain the program.

The measuring process concerns establishing ways to evaluate and measure the current users' security awareness level. This should be done on a regular basis both online or offline. Based on this, a number of periodical reports and statistics should be generated and published so it can be made available to any authorized users, potentially via the main security awareness website.

The reviewing process is performed offline by administrative and technical staff (a reviewing team). They will periodically review all reports and statistics gathered from the measuring process and approve or define a new set of requirements to be included in the program. The reviewing team's recommendations will be forwarded to the development process for further actions, which forms the closed system.

6. CONCLUSIONS

Organizations are part of the E-society where the Internet, computers, and mobile devices become the main tools that help us to participate as users and perform our daily activities. However, E-business adds new security challenges since its users are businesses and employees. We have shown that in order to protect an organization's IT assets against emerging threats, there is an on-going need to educate and train the systems users to be aware of possible threats and guard against them as part of their everyday working practices. In this paper we have shown the importance of incorporating an information security awareness program into an organization's website and proposed a general model that could be integrated into the development life cycle. For future work we intend to investigate the impact of integrating the security awareness program requirements into various software development models and investigate different measurement methods to evaluate and monitor users' security awareness levels.

ACKNOWLEDGEMENTS

This research was supported and funded by the Scientific Research Deanship at Petra University.

REFERENCES

[1] Corporate Technology Group 2008, "The threat within: is your company safe from itself?", Corporate Technology Group Web site:
http://www.ctgyourit.com/newsletter.php. Feb 2009.

[2] A. Maqousi, T. Balikhina, "Building Security Awareness Culture to Serve E-Government Initiative", book chapter in Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements, Editors Dr. Abid Al Ajeeli and Yousif Al Bastaki, 2010, Ch 24, Information Science Reference (IGI Global), Hershey-New York, USA. ISBN 978-1-61520-789-3

[3] A. Maqousi, and T.Balikhina, "User Security Awareness in E-Society", International Arab Conference of e-Technology, IACeT 2008, 5th - 16th October 2008, Amman, Jordan.

[4] Enisa, European Network and Information Security Agency "A user's Guide: how to raise information security awareness", June, 2006.

[5] Kruger H.A., Drevin L., Steyn T. A framework for evaluating ICT security awareness.
http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index.jsp?&pName=security_level1_article&TheCat=1001&path=security/2006/v4n5&file=bsi.xml& May, 2008

[6] ISF,https://www.securityforum.org/index.htm June, 2008

[7] ENISA,http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf, May 2008

[8] Robert Ayoub, The 2011 (ISC) 2 Global Information Security Workforce Study, Frost &sullivan, 2011.

[9] The Guardian 16/10/12, "Police force fined £120,000 after theft of unencrypted memory stick", http://www.guardian.co.uk/uk/2012/oct/16/police-force-fine-theft-memory-stick (last accessed 04/12/12).

[10] Bruce Schneier on the Insider Threat: December 19, 2005, http://www.schneier.com/blog/archives/2005/12/insider_threat.html.

[11] McAfee Threats Report: First Quarter 2012.

[12] M. Wilson, J. Hash, "Building an Information Technology Security Awareness and Training Program", NIST Special Publication 800-50, October 2003.

[13] University of Arizona Security Homepage: http://security.arizona.edu/basics (last accessed 30/11/12).

[14] BBC webwise safety page: http://www.bbc.co.uk/webwise/topics/safety-and-privacy/ (last accessed 30/12/12).

[15] Microsoft Safety and Security Centre, http://www.microsoft.com/protect/promotions/us/cybersecuritymonth_us.mspx May, 2008

[16] A. Marks, Y. Rezgui, "A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing," Management and Service Science, 2009 (MASS '09), pp.1-7, 20-22 September 2009.

[17] T. R. Peltier, "Implementing an Information Security Awareness Program", Information Systems Security, 14:2, 37-49 (2005).

[18] F. Aloul, "The Need for Effective Information Security Awareness", Journal of Advances in Information Technology, Vol 3No 3, August 2012.

[19] F. H. Katz, "Integrating a security awareness program into an information security course", Journal of Computing Sciences in Colleges, v.23 n.2, p.181-187, December 2007.

[20] W. A. Al-Hamdani. "Assessment of need and method of delivery for information security awareness program", 3rd conference on Information security curriculum development (InfoSecCD '06), pp102-108. 2006.

[21] Internet Evolution 11/12/12, "South Carolina's IT Security failure Teaches Valuable Lessons", http://www.internetevolution.com/author.asp?section_id=679&doc_id=254786 (last accessed 11/12/12).

[22] Training Conference. "*Strategies* andsubstantive and technical skillsto manage anddevelopWebsitesand checkingthem andprotect them*" 21-25 Feb, 2010,* Amman, Jordan.

[23] Swarnpreet Singh and Tarun Jangwal "Cost Breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues ", International Journal of Computer Science & Information Technology (IJCSIT), Vol 4 No 2, April 2012.

[24] Palson Kennedy "Shaping of Location Conscious Information", International Journal of Computer Science & Information Technology (IJCSIT), Vol 4 No 6, December 2012.

AUTHORS

Ali Maqousi (amaqousi@uop.edu.jo). He is an assistance professor at Petra University, Faculty of Information Technology, Amman-Jordan. He is acting as a head of the department of Computer Science and Computer Networks. He received his PhD in computer science from Oxford Brookes University, UK, 2003 for his work on providing Quality of Service (QoS) in packet switched networks. He was a network administrator and part-time teacher assistant at Petra University (PU) from 1993–1997 and full-time teacher assistant from 1999-2003. Since 2003 he is an assistant professor at the Faculty of Information Technology at PU and currently he is the head of computer science and networking department. He is ITSAF Secretary - General (Information Technology Students Activity Fair, ITSAF is a yearly event for University students since 2005). He is the university liaison officer for European Union 7th framework program (FP7) and Tempus since 2007. He is involved in research relating to multi-service networking, network performance, security and privacy, and social networks.