Cyber Security for home users: A New Way of Protection through Awareness Enforcement

E Kritzinger
SH von Solms

Abstract: We are currently living in an age, where the use of the Internet has become second nature to millions of people. Not only do businesses depend on the Internet for all types of electronic transactions, but more and more home users are experiencing the immense benefit of the Internet.

However, this dependence and use of the Internet bring new and dangerous risks. This is due to increasing attempts from unauthorised third parties to compromise private information for their own benefit – the whole wide area of cyber crime.

It is therefore essential that all users understand the risks of using the Internet, the importance of securing their personal information and the consequences if this is not done properly.

It is well known that home users are specifically vulnerable, and that cyber criminals have such users squarely in their target. This vulnerability of home users are due to many factors, but one of the most important ones is the fact that such home users are in many cases not aware of the risks of using the Internet, and often venture into cyber space without any awareness preparation for this journey.

This paper specifically investigates the position of the home user, and proposes a new model, The E-Awareness Model (E-AM), in which home users can be forced to acquaint themselves with the risks involved in venturing into cyber space. The E-AM consists of two components : the awareness component housed in the E-Awareness Portal, and the enforcement component.

This model proposes a way to improve information security awareness amongst home users by presenting some information security content and enforcing the absorption of this content.

The main difference between the presented model and other existing information security awareness models, is that in the presented model the acquiring/absorption of the awareness content is compulsory - the user is forced to proceed via the E-Awareness Portal without the option of bypassing it.

Keywords: information security, information security awareness, regulating service, information service provider

1. Introduction

Personal Internet users are increasingly exposed to security threats while using their home PC systems (Furnell, Bryant & Phippen, 2007). These personal internet users are becoming more vulnerable to security threats due to the use of information communication technologies (Furnell, Bryant & Phippen, 2007; Sophos, 2009; Symantec, 2007). This vulnerability to information security threats is due to the fact that many personal internet users do not possess the information security knowledge to understand and protect their PC and therefore their personal information. There are many ways or domains in which to classify the different personal internet users. This paper will classify such personal internet users into two categories - Home Users (HUs) and Non Home Users (NHUs).

NHUs are those users accessing the Internet from their corporate work stations within their work environments – such users will come from the Industry area, Government areas, Academic areas etc. NHUs most probably have been exposed to compulsory information security awareness courses and will be governed by corporate policies, procedures, guidelines and best practices to complete such awareness courses and perform secure practices when accessing the Interrnet. Information security awareness education and training is one of the most important aspects to enforce information security in an organization.(Shaw, Chen, Harris,& Huang H.J., 2009, Ronald, Carver, & Ferguson, 2007). NHUs therefore obtain vital information security knowledge though their working environments. Such users are constantly under a “watchful eye” of their institutions to ensure that the rules and regulations regarding information security is properly enforced within the users working environment.

HUs do not have this luxury of a “watchful eye”, and have no enforcement to ensure that they obtain information security awareness knowledge and implementing it. Home users are becoming more vulnerable to security threats (Furnell, Bryant & Phippen, 2007). This vulnerability is due to the fact that they do not possess the knowledge to understand and protect themselves. The majority of home users are likely to be vulnerable targets unless safeguards are automatically provided for them (Furnell, Valleria & Phippen, 2008).

A definition of a HU is a citizen with varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments (European Network and Information Security Agency, 2006) A HU is someone who accesses the Internet (cyber environment) from a personal computer at home, and who is self responsible to secure that computer in terms of malware, updates, patches etc.

HUs are therefore users that are not necessarily forced to obtain information security knowledge in any form. This lack of information security knowledge is one of the main risks HUs are exposed to in venturing into the cyber environment. If HUs lack the proper information security awareness knowledge they will also not understand and/or be aware of the cyber risks they are exposed to and that they are ultimately responsible for securing their own cyber environment (Furnell, Valleria & Phippen, 2008; Kumar, Mohan, & Holowczak, 2008).

One of the main reasons for this lack of information security awareness by HUs, is the fact that there is no enforcement by a third party to ensure that HUs are securely using the Internet or that their information security awareness is up to date.

It is this issue of **enforcement** that will be addressed within this paper.

It is also important to mention that the two domains of HUs and NHUs can overlap to some degree. This is depicted in Figure1.

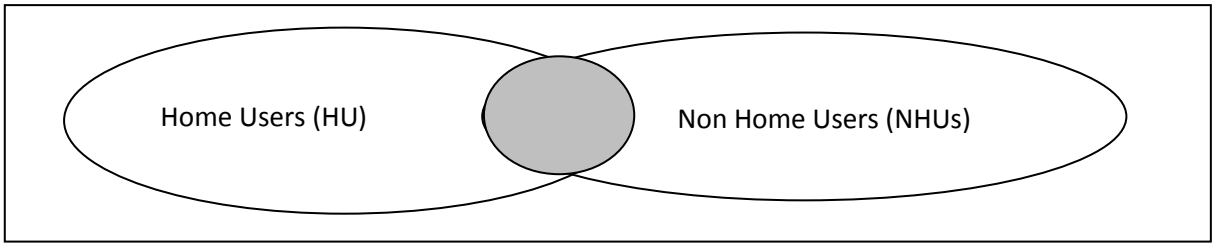

Figure 1: Home Users (HU), Non Home Users (NHU) and overlaps

Figure 1 depicts a grey "Overlap area" where users can be part of both. However this is do not have a serious impact on the reasoning of this paper, but we will basically be interested in those HUs who are not also NHUs. This paper primary focuses on the HU and the lack of information security awareness and enforcement. It is also important to realize that both HUs and NHUs could be further divided according to their current information security knowledge. These levels are novice, intermediate and advance (Furnell, Bryant & Phippen, 2007). These levels are depicted in Figure 2.

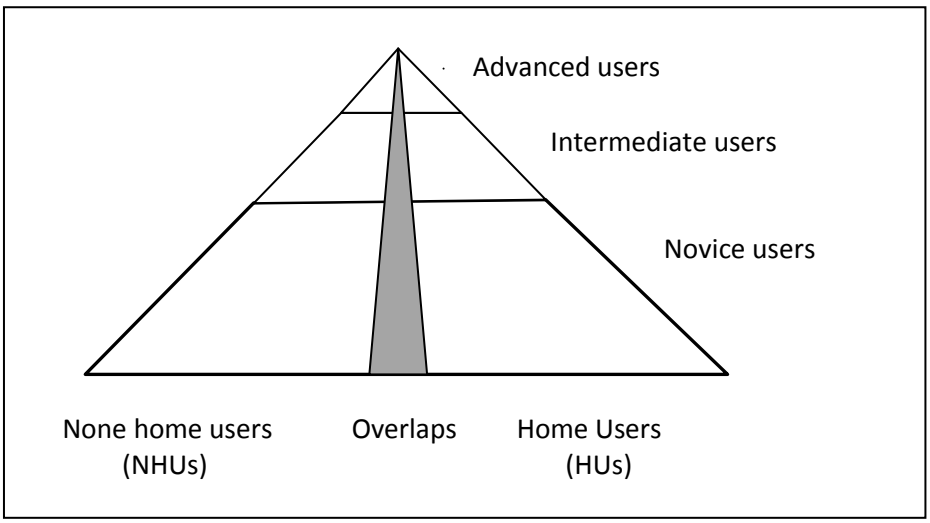

Figure 2: Different levels of information security knowledge among users

These different levels depicted in Figure 2 will be used later on in this paper. The next section of this paper will investigate in more detail the differences between NHUs and HUs and how information security awareness is viewed, addressed and implemented.

2. Non Home Users and Information Security Awareness

A lot of research has already been published on how to protect information properly within the NHU domain (academic, industry and government). This has led to the development and implementation of numerous information security awareness programmes within these domains (Bishop, 2000; Crowley, 2003; Hilburn, 1999; Kritzinger & Smith, 2006; The White House, 2000; Yasubsac, 2002). Within these domains, users are forced by their organizations to make themselves information security aware and to apply a wide range of information security awareness tools. These include information security policies, procedures, guidelines and awareness courses. These tools are compulsory and ensure that users are aware of the risks of accessing the Internet, and take precautions to mediate such risks.

Two aspects of this NHU approach is clear – information security awareness and enforcement. NHUs are usually forced, via policies and procedures, to expose themselves to the relevant corporate information security awareness courses, and to ensure safe practices when accessing cyber space. The NHU does not actually have a choice in any of these matters.

This forces NHUs to access the Internet via a secured route to gain access to the Internet and web. Relevant corporate policies, procedures, guidelines and best practices enforce this.

This is depicted in Figure 3 and Figure 4.

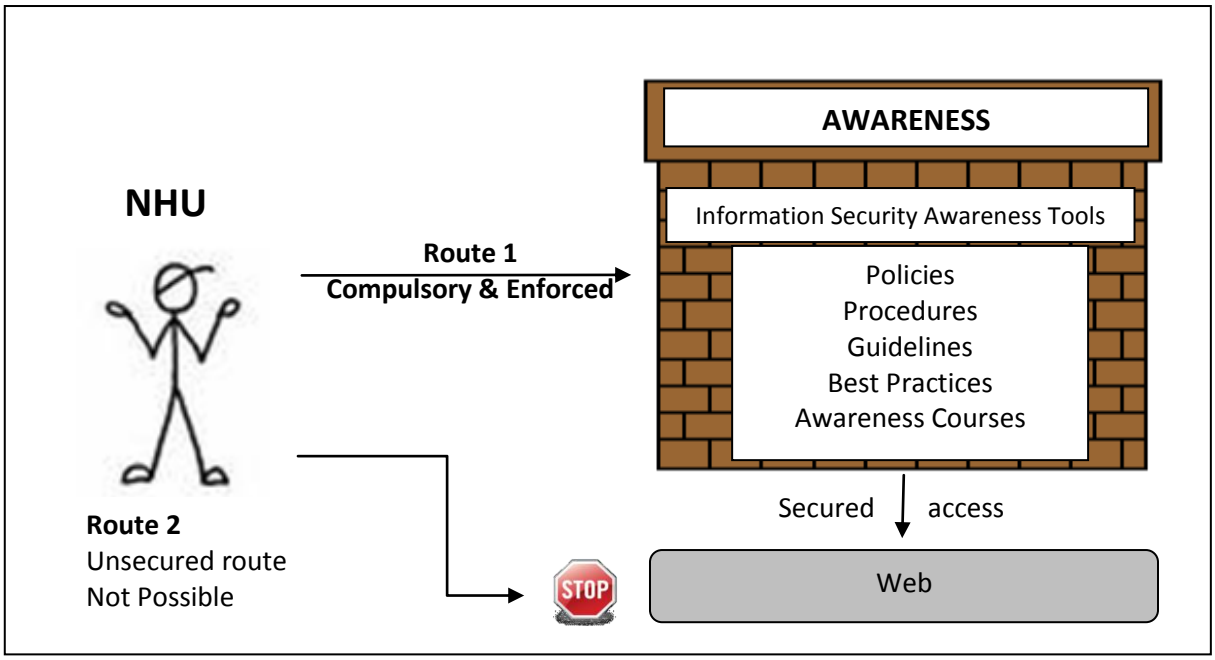

Figure 3: Compulsory secured access to web for NHUs

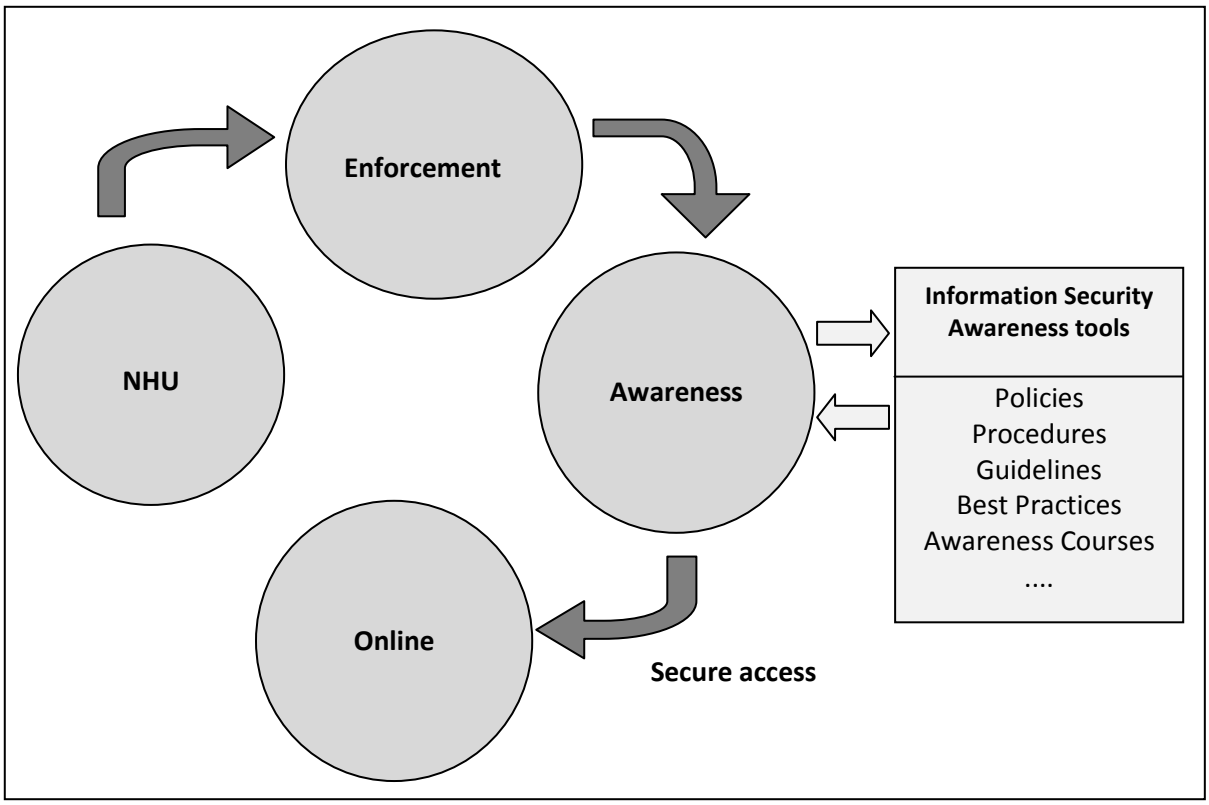

Figure 4: Compulsory secured access to web for NHUs

3. Home Users and Information Security Awareness

In the case of the HU, the situation is totally different. Although research had been done on making home users aware of the importance of securing their own information, the enforcement to do so does not usually exist. HUs therefore in many cases venture onto the Internet without any idea of what the risks are and what they must do to protect themselves.

That HUs should be information security aware, are supported by the following statistics:

- Home users account for 95% of internet attacks (Symantec, 2007).
- Novice users are likely to face a range of internet threats as their unfamiliarity with the technology can limit their ability to recognise the threats and understand the requisite protection (Furnell, Tsaganidi & Phippen, 2008).
- Three million computers have been infected with Koobface – a social networking site (CISCO, 2009).
- Spam levels are expected to rise 30-40 per cent in 2010 (CISCO, 2009).
- One in every 600 PDF files downloaded from the web contains malicious software (CISCO, 2009).
- 23 500 infected websites are discovered every day. That is one every 3.6 seconds – four times worse than the same period in 2008 (Sophos, 2009).
- 15 new bogus anti-virus vendor websites are discovered every day. This number has tripled, up from average of 5 during 2008 (Sophos, 2009).
- 89.7 % of all business e-mail is spam (Sophos, 2009).

An extremely worrying aspect reported is the fact that *trusted legitimate websites are the perfect vehicle for malware distribution. It is estimated that more than 79% of the websites hosting malicious code are legitimate websites that have been exploited* (CISCO, 2009).

With growing numbers of HUs accessing the Internet for social networking, Internet banking and many other reasons, the big problem and worry is that in many cases such HUs are not information security aware, and are therefore potentially exposing themselves in a big way. This is depicted in Figure 5 and Figure 6 where a typical home user gains access to the web. Figure 5 and Figure 6 clearly shows that the component of awareness and enforcement is not present.

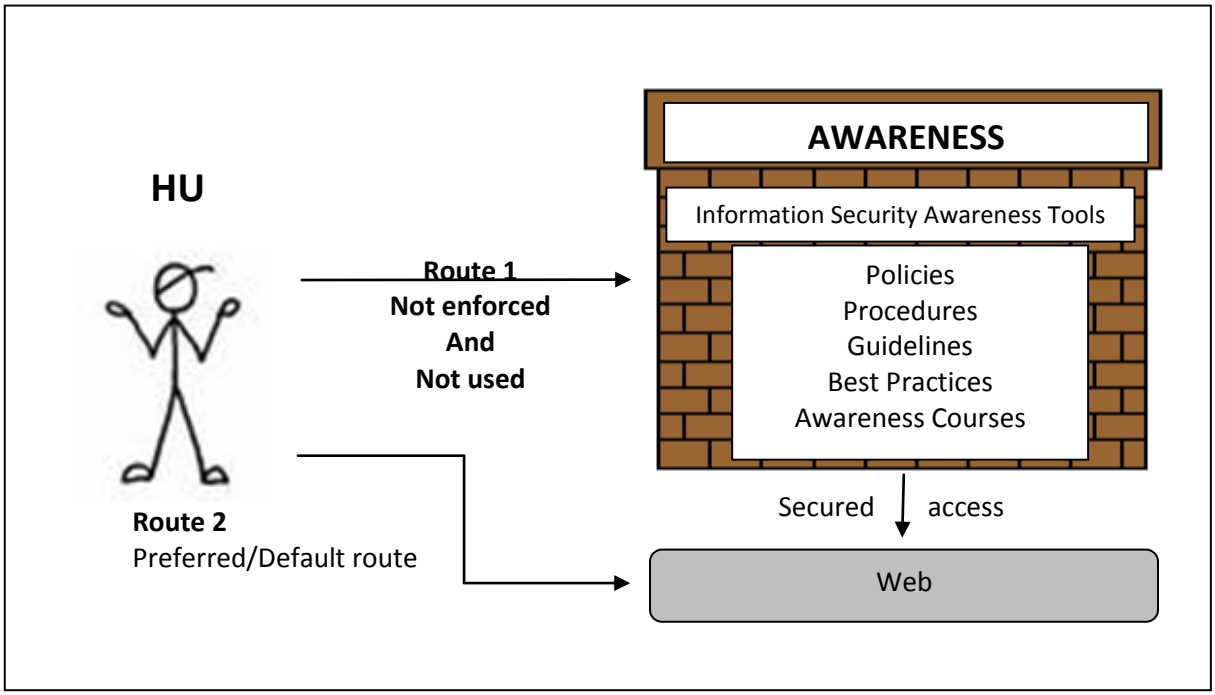

Figure 5: Non-secured access by HUs

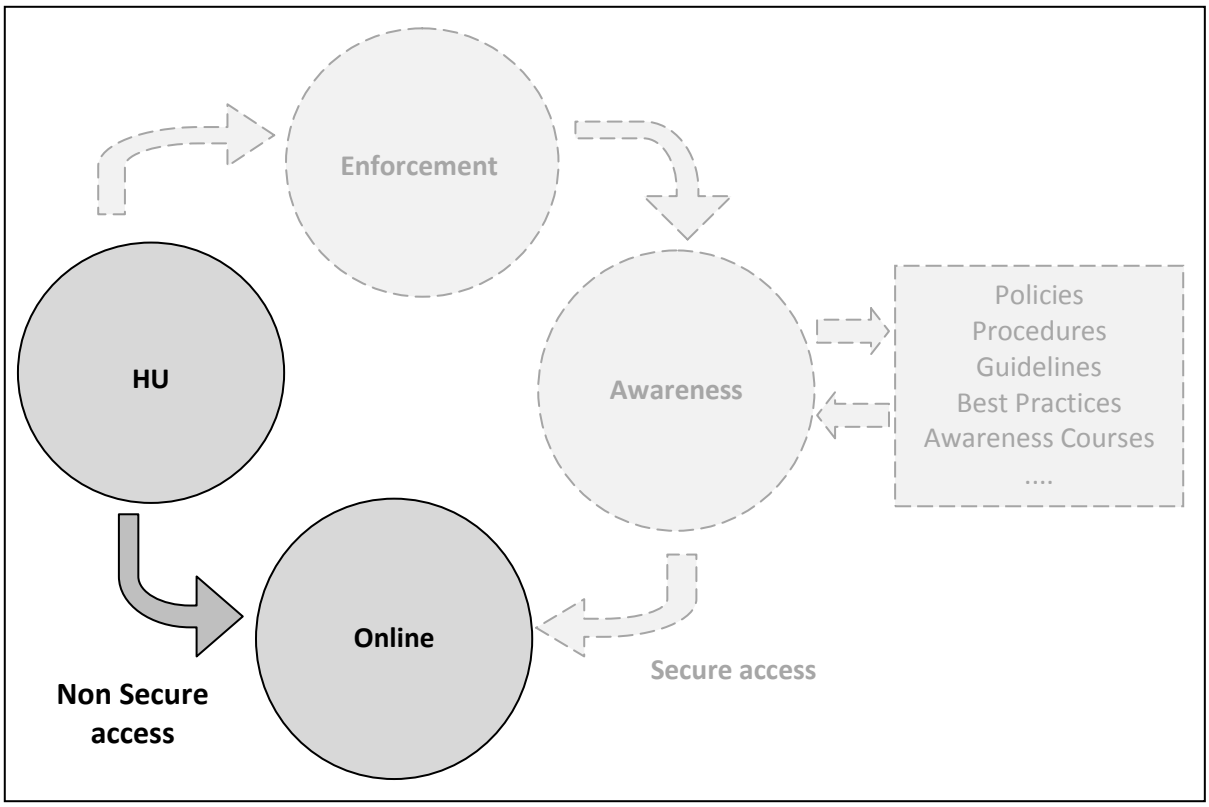

Figure 6: Non-secured access by HUs

The main difference between Figure 3 & Figure 4 and Figure 5 & Figure 6 is the enforcement component – ie the fact that the HU can get access without being exposed (in a compulsory way) to the relevant information security awareness tools and support that are essential. These tools and support may be available as options to the HU, but in most cases the HU does not make use of them because they are not enforced.

Table 1 provides a comparison of these tools, and shows that because of the optional character in the HU's case, the HU does not get the benefit of these tools.

Table 1: Comparison between Information Security Awareness Tools

	Non Home Users	Home user
Policies	✓	**x**
Procedures	✓	**x**
Guidelines	✓	**x**
Disciplinary actions	✓	**x**
Best practices	✓	**x**
Job responsibility	✓	**x**
Job accountability	✓	**x**
Continuous upgrading of new threats	✓	**x**
Information Security Awareness programmes	✓	✓ **and x**

From Table 1 it is clear that because of non-enforcement, HUs are not necessarily exposed to the benefits of such awareness tools. Table 1 also indicate that there is a

conflicting situation with the current information security awareness programmes for HUs. This investigation identified that are a number of research projects which identified that information security awareness is a problem among home users but there are minimum research done on designing and implementing information security awareness programmes to solve the problem. From the information security awareness programmes that are available for HUs, the following issues came up.

The amount of information security awareness programmes available for HU is far less than for NHU. The few that are available to HUs are mostly online programmes. These programmes are in most cases not easy to find and a novice HU will not have the skills and knowledge to find these programmes. If a HU manages to find these programmes they are in most cases not comprehensive enough, and do not include all relevant information security issue. These sites start to address the information security awareness for home users but only provide limited beginner's information. There are no options for users to obtain more or in-depth information security knowledge. There are also no dynamic interaction with the users by means of testing, examples and exercises. Another problem found is that these programmes are not regularity updated with new emerging technologies, for example the security issues regarding social networking.

However, all these information security programmes do addresses information security in some way but the main problem still remains that if the HU does not know that he/she is information security illiterate, the user will not know to search for these awareness programmes online. From the investigation above two challenges were derived. The first is to create a framework for the design and implementation of information security awareness tools. This addresses the challenge to ensure that HUs obtain the relevant information security awareness to safely use the Internet.

The second challenge is to investigate ways in which HUs can be forced (or guided) to be exposed to such awareness tools to prepare them for the possible risks when obtaining access to the web. This challenge addresses the enforcement of information security awareness.

The two challenges will be addressed by proposing a model. The proposed model provides one way of addressing these challenges.

4. The Challenge – Awareness and Enforcement

The challenge set out in this paper is firstly to establish the issues involved in such a awareness programme, it is what a HU should know (the **what**), and secondly how the absorption of the content can be enforced (the **how**). This is done by defining the Electronic Awareness Model (E-AM), consisting of two components:

- The Awareness component or the **what,** called the E-Awareness Portal
- The Enforcement component or the **how**

The following section will first investigate the awareness component or the **what**. This is followed by suggesting a way to help home users by implementing a possible method for the enforcement component or the **how**.

4.1 E- Awareness Portal (The Awareness component)

The first component of the model is the awareness component, called the E-Awareness Portal (E-AP). The main function of the E-AP is to provide up to date content regarding information security risks within the home user environment. This component will address the information security awareness content. The aim is therefore to introduce home users to relevant information security issues such as what information security is, why it is important and how to use it. It is important to understand that those users who will use this portal have limited or no information security background. It is therefore essential that the design and implementation of the portal is:

- easy to follow
- integrated
- easy to access
- user-friendly
- usable regarding the downloads
- comprehensive
- relevant topics
- knowledge based appropriate
- up to date

Another aspect of the E-AP is that it should be scalable. This means that a user can start with introductory material regarding information security and then move on to more advanced terminology. Each level will have a testing environment where the HU can be evaluated regarding the material of each level. The three levels depicted in Figure 7 include novice, intermediate and advanced (Furnell, Bryant & Phippen, 2007).

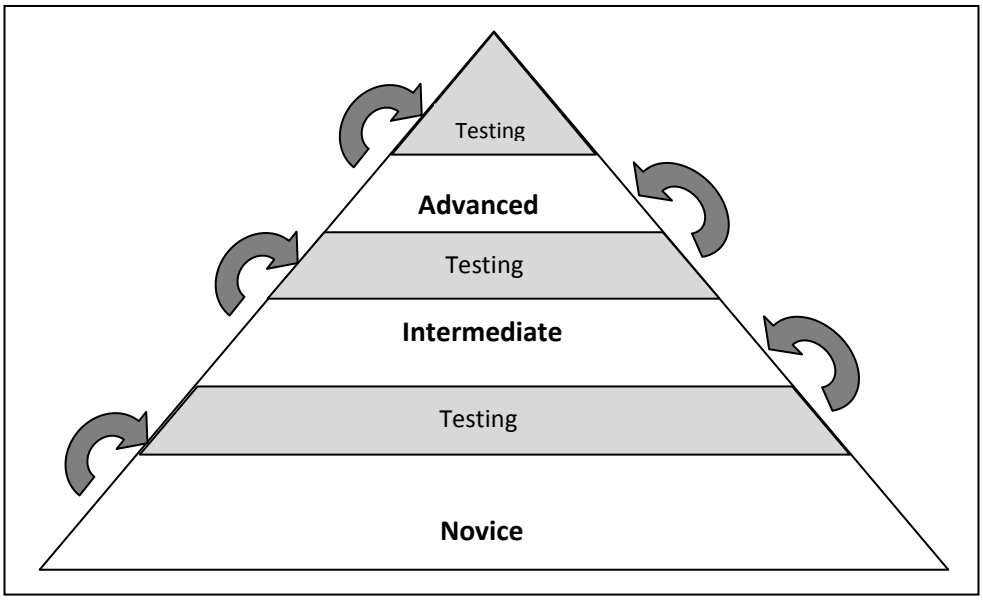

Figure 7: Layout of E-AP

It is also vital that the E-AP must be regularly updated to keep track of new developments. The scope of the article is not on what must be included in the E-AP but rather that the E-AP is designed and implemented for HUs, accessible for HUs

and ensures that HUs are presented with the all the information security knowledge to safely access the Internet. The other important aspect of the E-AP is that it must be enforced.

The solution to this enforcement problem is to host the E-AP within with regulating services, for example information service providers (ISPs) or financial institutions (FIs), since almost all users must gain access through these regulating services. Such regulating services must then ensure that access to the Internet is only provided after passing via the awareness content part in the E-AP. The next section will focus on regulating services and their role regarding enforcement of the information security content among HUs.

4.2 Regulating Services (Enforcement Component)

We use the term "regulating services" to represent the body through which the user can connect to the web. The best example is an information service provider (ISP), although increasingly other bodies are also starting to supply connection facilities to the web. Regulating services provide the enforcement aspect as depicted in Figure 3 & Figure 4 and lacking in Figure 5 & Figure 6. This paper of course accepts that ISPs will be willing to provide the type of service discussed above.

While most, if not all ISPs may at this time reject this expanded type of responsibility, there seems to be a growing international movement towards getting ISPs more involved.

In 2008, The Controller of the Communications Authority in Zambia, urged ISPs to *'protect their customers from fraud and thefts that may arise as a result of sharing personal information online'* (Lusaka Times, 2009).

Also in 2008, the Council of Europe at its Strasbourg Conference in France, asked ISPs to help battle cyber crime (Lemos, R, 2008). In a BCS paper, it is stated that there had been

' .. increased calls for ISPs to play a more central role in detecting, monitoring and preventing illegal file sharing, in addition to their ongoing contribution to fight against other, perhaps more serious, criminal activities like online fraud, identity theft, phishing, terrorism and paedophilia' (BCS, 2009).

In a very recent document, the aspect of the liability of Internet providers are addressed (ITU, 2009:216)

' .. Internet Service Providers have ever since been in the focus of criminal investigations that involve offenders who use the ISP's services to commit an offence'

At the end of 2009, the Australian Government proposed measures to improve safety of the Internet for families. This proposal included 'mandatory ISP-level filtering' to be implemented by ISPs. *'These additional filtering services will help parents to choose what they want filtered without having to download and install software to their home computers'*. (Australia, 2009)

Therefore the idea that ISPs can in future get much more involved in providing security and other types of services, for eg those suggested in this paper, is definitely possible.

4.3 Some practical considerations, limitations and challenges related to the proposed E-Awareness Model (E-AM)

The model presented in this paper is, of course, a theoretical model, and that was specifically the purpose of the paper.

However, it is good to briefly identify some practical aspects related to implementing the model at some stage. In implementing such a model, the major challenges lie in the social, legal and technical areas. Some of the aspects which will have to be taken into account in these 3 areas include :

- The social impact of the model, including
    - User acceptance of such a model
    - the impact on the HU as far as changing the way he/she has done things before (some behavioral change),
    - the establishment and consequences of a trust relationship which is directly or indirectly, established between the HU and the ISP in using such a model,
- The legal environment in which the model will operate, including aspects such as
    - contractual aspects including whether the user can now hold the ISP responsible if something ‘bad’ happens,
    - the precise scope of the agreement between the HU and ISP
    - the privacy of HU information created by the E-AM model and stored by the ISP
    - the way this form of ‘control’ is managed to prevent undesirable ‘down stream’ consequences
- The technical aspects, including
    - The way the model is enforced, ie should it be compulsory or can the user choose to be exposed to the model as well as categorizing different types of users
    - impact on response time and delays which are necessarily introduced by the model and the effect on the HU,
    - ease of use and the user interface

    - other as yet undetermined technical problems

- Other uses of the model, and other impacts which are unclear at the moment.

The first two points are more socially and legally oriented, while the third is a more technical aspect. The fourth point relates to uses of the model. The presented E-AM model is specialized in the sense that it only relates to accessing the web via 'traditional' ISPs, and does not try to address any other aspects of Internet services or forms of enforcement. However, the concept of the model can possibly be extended to a wider sphere. That is something which can be investigated at a later time when the prototype under development (mentioned below) provides answers to some of the challenges mentioned above.

A post graduate project has started to actually create a prototype to implement the model, and specifically look at the technical aspects, like point 3 above. When finished, it is planned to test the prototype in a school environment to try to evaluate more of the social consequences.

It is planned to report on the results of the prototype when that is available.

As far as the legal aspects are concerned, national and international developments will be studied, in the light of paragraph 4.2 above.

The authors are convinced that the first challenge now is to get a prototype working to help address the type of challenges mentioned in this paragraph.

4.4 The full E-Awareness Model (E-AM)

To summarize, the full E-AM is depicted below.

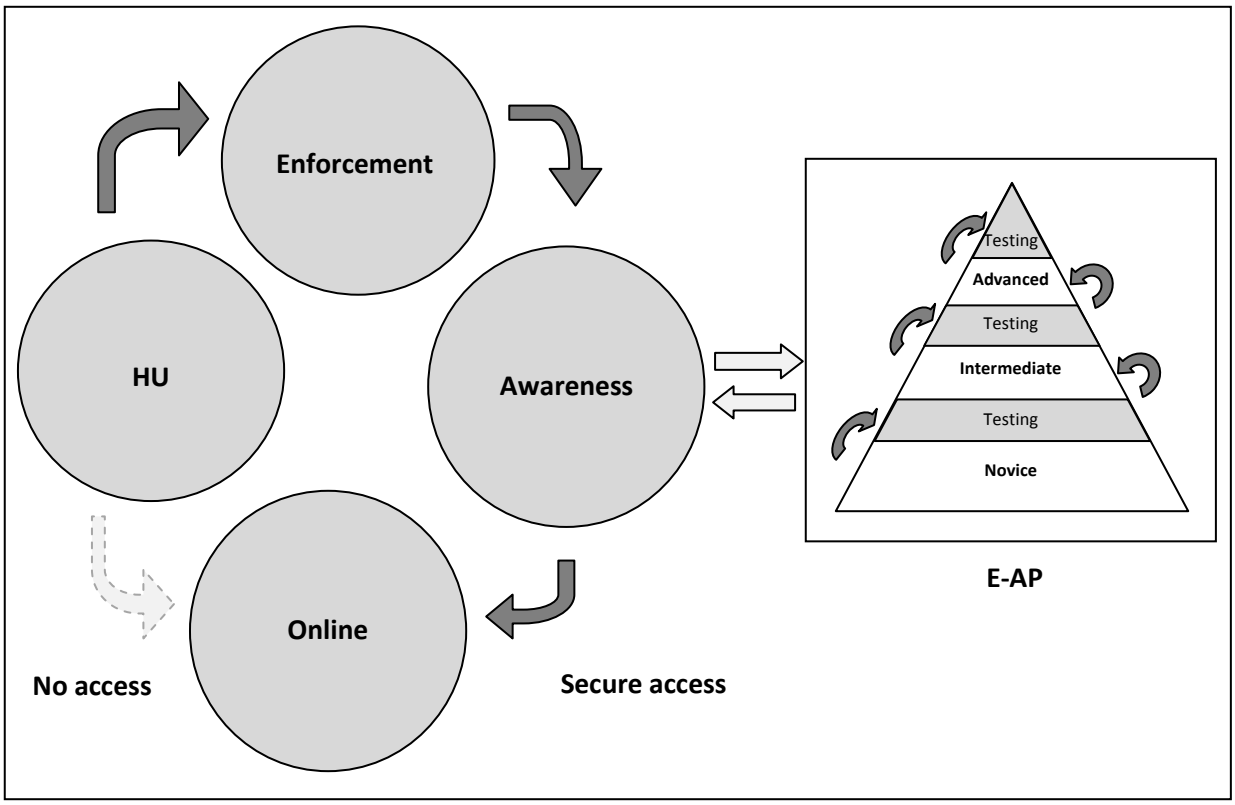

Figure 8: The full E-Awareness Model (E-AM)

This paper will not expand on precisely how the ISP will manage and control to which levels in the E-AP the user should be exposed to at what times. The authors see that as very much an implementation issue.

It is important to note that no matter which level the users choose, they are “forced” to go the route via the E-AP. The E-AP can be used by regulating services, governments, educational bodies and so forth to provide comprehensive national campaigns to inform users of the risks of using the web (Von Solms, 2010).

The E-AM model presented above, is in a sense, a one way model, addressing communication from the HU to the ISP.

In the next version of the E-AM model, the model is extended to also move technical aspects like antivirus protection, patching and other matter away from the HU and hosting that at the regulating service (Von Solms & Kritzinger, 2010). This will change the model into more of a two way model.

5. Conclusion and future research

Accessing the web has many risks possibly with dire consequences for the HU who has limited information security knowledge. Allowing such users to access the web results in the HU being exposed to serious risks, which should, in the benefit of all, be prevented as far as possible. It is therefore essential to ensure that users are educated and understand the security risks involved and how to limit them.

This paper proposes an E-Awareness Model that can empower users by giving them a better understanding of security issues, possible threats and how to avoid them. This model puts a responsibility on the regulating service to force the user to absorb the required awareness content before venturing onto the cyber highway. As the model as proposed is still very abstract, future research will concentrate on actually implementing the model in terms of a prototype, and then experimenting with the prototype to try to answer many open questions – including those mentioned throughout this paper.

6. References

Australia, (2009). *Measures to improve safety of the internet for families.* http://www.minister.dbcde.gov.au/media/media_releases/2009/115. (Accessed on 22 April 2010).

BCS, (2009). *What future for internet service providers?* http://www.bcs.org/server.php?show=ConWebDoc.24111. (Accessed on 22 April 2010).

Bishop, M,. (2000). *Academia and education in information security: Four years later.* Proceedings of the Fourth National Colloquium on Information System Security Education. Washington, DC (Keynote address).

CISCO, (2009). *A comprehensive proactive approach to web-based threats.* CISCO IronPort Web Reputation White Paper. http://www.ironport.com/pdf/ironport_web_reputation_whitepaper.pdf. (Accessed 20 April 2010).

Crowley, E. (2003). *Information systems security curricula development.* Proceedings of the 4th Conference on IT Curriculum on IT Education. Lafayette, Indiana, USA.

European Network and Information Security Agency - ENISA, (2006). *A users' Guide: How to Raise Information Security Awareness.* http://www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en. (Accessed on 22 April 2010).

Furnell, S, Bryant, P. & Phippen, D., (2007). *Assessing the security perceptions of personal Internet users*. Computers & Security 26, 410-417.

Furnell, S., Valleria T. & Phippen, D., (2008). *Security beliefs and barriers for novice Internet users*. Computers & Security 27: 235-240.

Furnell, S., Tsaganidi, V. & Phippen, A. (2008). *Security beliefs and barriers for novice Internet users*. Computers & Security, 27: 235-240.

Hilburn, T.B., Hirmanpour, I., Khajenoori, S., Turner, R. & Qasem, A. (1999). *A software engineering body of knowledge*, Version 1.0, Software Engineering Institute, Pittsburgh, United States of America.

ITU, (2009). *Understanding Cybercrime: A Guide for Developing Countries.*

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed on 22 April 2010)

Kritzinger, E. & Smith, E. (2006). *An information security retrieval and awareness model for industry*. PhD, University of South Africa, Pretoria.

Kumar, N., Mohan, K. & Holowczak. R., (2008). *Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls.* Decision Support System 46, 254-264.

Lusaka Times, (2000). Zambia: Internet service providers urged to fight cyber crime. http://www.lusakatimes.com/?p=704. (Accessed on 22 April 2010)

Lemos, R,(2008). Europe asks ISPs to help battle cybercrime. *http://www.securityfocus.com/print/brief/71.(Accessed on 22 April 2010)*

Ronald, C., Carver, C. & Ferguson, A., (2007). *Phishing for user security awareness.* Computers & Security 26: 73-80.

Sophos, (2009), *The Sophos Security Threat Report – 2009*, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf .(Accessed on 20 April 2010).

Shaw, R. Chen, C. Harris, A & Huang H.J., (2009). *The impact of information richness on information security awareness.* Computers & Education, 52: 92-100.

Symantec. (2007). *Symantec internet security threat report*. Trends for January-June 07. Vol. XII. http://www.zdnetasia.com/whitepaper/symantec-internet-security-threat-report-trends-for-january-june-07-volume-xii_wp-333829.htm. Accessed (22 April 2010).

The White House, (2000). *Defending America's cyberspace: National Plan for Information Systems Protection*. http://ww.fas.org/irp/offdocs/pdd/CIP-plan.pdf. (Accessed on 17 April 2005).

Von Solms, S.H. (2010*). Securing the Internet : Fact or Fiction?* Proceedings of the IFIP iNetSec Conference, Sofia, Bulgaria.

Von Solms S.H & Kritzinger E. (2010). *Cyber security for home users: From Thick User Clients to Thin User Clients* (Work in progress).

Yasubsac, A. (2002). *Information security curricula in computer science departments: Theory and practice*. Journal of Information Security, 1(2).