Web-Based Risk Analysis and Education for Home Users

J. Marston, N.L. Clarke

Network Research Group, School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, United Kingdom

Abstract

Broadband Internet access is now widely available to home users, providing better data transfer rates than dial-up Internet access. However this improvement in technology comes at a price with home users at an increased risk of unauthorised access to their resources and information as a result of the 'always on' nature of Broadband. These new risks mean that there is a need for home users to undertake a risk analysis of their system in order to ensure effective protection is being provided, given the assets they own. Unfortunately to date, current risk analysis tools have been focussed from an organisational perspective where an expectation exists for prior knowledge of information security and risk analysis. Therefore, a requirement exists for a risk analysis tool specifically tailored for home users.

The tool proposed in this paper is designed around the ISO17799 standard in order to provide a solid foundation, yet only takes advantage of key sections within the standard that are relevant to home user environments. The tool carefully considers the unique circumstances home users present, with varying degrees of security education and knowledge. To this end, the tool is carefully crafted to present a series of questions to the user with varying degrees of additional support and information as and where required. The output of the risk analysis process is a simple easy to understand webpage with links to appropriate sources for additional information and security controls.

Keywords: *Risk Assessment, ISO17799, Home User, Security Education*

1. Introduction

Until recently residential users generally accessed the Internet using a dial-up connection. The main limitation of a dial-up service is the data rate available for information transfer. This can be anything from $28.8kbs^{-1}$ to $33.6kbs^{-1}$ (Bates, 2000). This technology is now being replaced by Broadband access which can be defined as a high capacity bi-directional connection (France, 2004), with data capacities exceeding $16Mbs^{-1}$. In addition to the increased data transfer rates, the industry has experienced extremely competitive market forces, resulting in lower subscription rates for users (Bailey, 2007). This has led to a formidable growth in Broadband adoption on a global scale: with over 60 million households in the US predicted to be connected by the end of 2007; representing 55% of all households (Ferguson, 2007). The UK is marginally behind this level with 49% of all households.

The flat fee charged for Broadband subscription connections mean they are often left on for long periods of time making home users computer resources and information an easy target for intruders (Kuhn *et al,* 2002). Surveys conducted have highlighted

that home user's lack knowledge in terms of computer security. One survey conducted showed that 52% of the people interviewed had little or no knowledge of computer security and 53% did not know how to improve their computer security (HM Government, 2005). Another survey showed that 81% of home users did not have at least one of the minimum protection mechanisms installed, namely updated Antivirus software, Spyware protection software, and a secure firewall (AOL/NCSA, 2005). These problems are compounded by the fact that vulnerabilities exist in the operating systems themselves and the change in Internet usage habits as a direct result of its accessibility (Orvis *et al*, 2005).

Standards and techniques are available that guide users through risk analysis but these are costly, require expertise and are aimed at organisations rather than home users (Mash, 2002). As a result there is a need to develop a suitable alternative and this paper proposes a web-based risk analysis tool, based on the ISO17799 standard, aimed specifically at home users.

The remainder of the paper is organised as follows. Section two introduces the new risks associated with Broadband Internet access. In section three the risk management concept is described and how it will be captured by the web-based tool. Some current standards and techniques are identified along with reasons why they do not match the requirements of the home user. The paper then outlines the structure of the proposed web-based tool in section four and section five.

2. The Risks Associated with Broadband Access

Unfortunately, the improvements in data transfer rates provided by a Broadband connection come at the cost of an increased risk for unauthorised access to the home user's computers. For Broadband connections a computer may be left on all day and therefore the Internet Protocol (IP) address will remain fixed for longer periods of time thus providing hackers more time to compromise the computer (Kuhn *et al,* 2002). The main reasons for hackers targeting a Broadband connection are as follows (Glass, 2001):

- **Bandwidth** – in general a home user will only use a small amount of the available bandwidth. Hackers can therefore use the spare bandwidth without having a detrimental affect on the home user's data transfer rates. This means they go unnoticed and can utilise this bandwidth for Distributed Denial of Service (DDoS) attacks and illegal file sharing.
- **Resources** – the Central Processing Unit (CPU) capabilities and memory are useful to hackers. They can use home computers as servers for chat rooms or for storing illegal copies of software. Due to the amount of processing power and memory available on modern computers the loss of performance and storage could go unnoticed by the home user.
- **Information** – personal and financial information is generally stored on the home user's computer. If online transactions have been made or bank account details stored then sufficient information may be available for identity theft.

It is evident that there are new risks associated with Broadband Internet access but there are relatively simple ways for home users to counter these risks. Problems caused by the shortfall in the home user's lack of computer security knowledge, their

Internet usage habits and system vulnerabilities can be overcome by providing a web-based risk analysis tool that educates the home user, informs them how to implement the protection measures available and provides advice on secure computing practices.

3. Information Security and Risk Analysis

At home people will invest time and effort using their computer to create documents and store information. The computer and its applications will be used as tools to help with various tasks and to track different types of information i.e. finances. This type of information has a value to the home user and can be considered as an asset that needs to be protected. The web-based risk analysis tool will provide information security using a risk management strategy consisting of the following three separate processes (Stoneburner *et al,* 2002):

- **Risk assessment or risk analysis** – identifying assets and then considering what the threats are to those assets. This will be the primary aim of the web-based tool. Answers to a security questionnaire will be used to determine the level of risk to the home user.
- **Risk mitigation** – putting controls in place to protect the assets from the identified threats. This will be the secondary aim of the web-based tool. Guidance will be provided with regard to the protection measures available and how to implement them.
- **Evaluation** – risks and mitigation tools should be continually reviewed to ensure that security is maintained. The web-based tool will indicate the importance of this and will be updated by the developer as new threats and protection methods are realised.

Conducting a risk assessment is not an easy exercise, particularly if trying to comply with one of the security standards as well as catering for the varying degrees of computer literacy. For small-to-medium enterprises (SME) the expertise may not be available internally and the cost of employing a consultant may prove too expensive. These problems are also applicable to the home user. However the risks are the same (if perhaps a subset) of those faced by larger organisations and therefore it is important that an assessment is conducted (Mash, 2002).

A suitable alternative for an SME is to purchase an off-the-shelf product, which guides a user through the risk assessment process identifying the security threats and vulnerabilities and the controls required to mitigate these risks (Mash, 2002). However, for the home user the cost will again be too high and they will be largely oriented towards organisations. This reinforces the need for designing an easy to access and simple to understand risk analysis tool specifically aimed at the home user.

3.1 Risk Assessment Standards and Techniques

To aid the development of a suitable alternative, existing risk assessment methodologies were reviewed to identify one that provided a useful framework that could be adapted to suit the home user. There are numerous standards and techniques available. Some can be downloaded free from the Internet whilst others are available at a cost. The standards and techniques that have been reviewed include:

- *Operationally Critical Threat, Asset And Vulnerability Evaluation (OCTAVE®);* (Alberts *et al*, 2003)
- *Control OBjectives for Information Technology (COBIT);* (ISACA, 2005)
- *Site Security Handbook, RFC2196;* (Fraser, 1997)
- *Common Criteria (CC), ISO15408;* (ISO, 2005)
- *Risk Management Guide for Information Technology Systems, SP800-30;* (Stoneburner *et al*, 2002)
- *Information Technology – Code of practice for information security management, ISO17799.* (ISO, 2005)

It was decided that the ISO17799 standard, which is becoming the de facto standard in Europe (Walsh, 2002) would provide a good framework around which a web-based tool could be designed. The output from the risk assessment would identify the risks and provide recommendations on controls that would reduce these risks to an acceptably low level. Using ISO17799 as a guide for identifying these controls provides a consistent strategy, which is in compliance with a widely used and recognised standard (Mash, 2002).

It is intended that the web-based tool will be hosted on a web server for access to home users at no cost. It will use a simple questionnaire oriented specifically towards the home user environment, with supporting information to help users answer the questions. It will assume no prior knowledge, hence overcoming the disadvantages of existing techniques.

In addition to the standards and techniques there are a number of websites available from authoritative organisations, such as Microsoft that give advice and guidance on home user security. However the disadvantage is that they are biased towards their products, which often need to be purchased. The advantage of the web-based tool is that it is unbiased and will provide links to resources that are free and equally as effective.

4. Application of the ISO17799 Standard to Home Users

The ISO17799 is a high level standard identifying what best practice but not actually how to implement the security measures (Kairab, 2005) or even how to determine the level of risk. It does provide details on various controls that are required to provide information security. The controls that are applicable to the home user environment have been used to create a number of questions, which together make up the risk assessment.

The web-based tool combines these questions with an extended version of the Jacobson's Window risk model, which has quantitative values assigned as shown in Figure 1. The values assigned to the potential impacts LOW, MEDIUM and HIGH are 0.1, 0.5 and 1.0 respectively. The values assigned to the probabilities LOW, MEDIUM and HIGH are 10, 50 and 100 respectively. The risk score based on these values will range from 1 to 100.

Assigning the values in this way means there will only be one case of high risk, which is when both the potential impact and probability are high. This is done intentionally

so that the importance and immediacy of a high risk can be seen and acted upon urgently (Kairab, 2005).

Probability Of Threat	Potential Impact		
	LOW (10)	**MEDIUM (50)**	**HIGH (100)**
HIGH (1.0)	LOW 1.0 x 10 = **10**	MEDIUM 1.0 x 50 = **50**	HIGH 1.0 x 100 = **100**
MEDIUM (0.5)	LOW 0.5 x 10 = **5**	MEDIUM 0.5 x 50 = **25**	MEDIUM 0.5 x 100 = **50**
LOW (0.1)	LOW 0.1 x 10 = **1**	LOW 0.1 x 50 = **5**	LOW 0.1 x 100 = **10**

Risk scale: HIGH (>50 to 100); **MEDIUM** (>10 to 50); **LOW** (1 to 10)

Figure 1: Risk level matrix (Stoneburner *et al,* 2002)

Having determined a suitable risk scale it is important that the potential impact and probability of threats are described in order to allow consistency in the risk assessment. Examples of the potential impact to home users for each category are shown in Table 1.

HIGH IMPACT = 100
Potential Impact
Total loss of personal data
Total loss of system and application software
Intruder access to personal information
Intruder access to financial information
Intruder access through 'back door'
Intruder access to hardware i.e. memory, CPU, bandwidth
Monitoring of home users Internet activities
All contacts adversely affected
Computer system unavailable for an extended period
MEDIUM IMPACT = 50
Potential Impact
Personal data recoverable with significant effort
System and application software recoverable with significant effort
Intruder access to personal information only
Abnormal display and computer activity
Internet activity monitoring detected and addressed
Parts of the computer system unavailable for significant period
LOW IMPACT = 10
Potential Impact
No loss of personal data
No loss of system or application software
No intruder access to personal information
No intruder access to financial information
No intruder access to hardware i.e. memory, CPU, bandwidth
No monitoring of home users Internet activities
Contacts not affected
Computer system remains available

Table 1: Potential impact to a home user

For each category of potential impact not necessarily all listed items will or indeed need to occur. For example if all personal information is lost then this is certainly as a consequence of being at a high risk, even if none of the other impacts listed occur. When a home user is connected to the Internet using a Broadband connection they are susceptible to a number of threats and vulnerabilities. The probability of these threats occurring and vulnerabilities being exploited will relate to the level of protection already in place and to the way in which the Internet is used. Table 2 identifies the

common threats and quantifies them according to both the home user's level of protection and their Internet usage.

THREAT	PROBABILITY	COMMENT
Virus	**1.0**	If no Antivirus software installed
	0.5	If Antivirus software installed but not up to date
	0.1	If Antivirus software installed and up to date
Trojan Horse	**1.0**	If no Antivirus software installed
	0.5	If Antivirus software installed but not up to date
	0.1	If Antivirus software installed and up to date
Worm	**1.0**	If no Antivirus software installed
	0.5	If Antivirus software installed but not up to date
	0.1	If Antivirus software installed and up to date
Spyware	**1.0**	If no anti-spyware installed and regular freeware downloads
	0.5	If no anti-spyware installed and some freeware downloaded
	0.1	If anti-spyware installed and/or no freeware downloaded
Adware	**1.0**	If no anti-spyware installed and regular freeware downloads
	0.5	If no anti-spyware installed and some freeware downloaded
	0.1	If anti-spyware installed and/or no freeware downloaded
Back door	**1.0**	If Windows automatic updates disabled
	0.5	If Windows automatic updates done manually
	0.1	If Windows automatic updates enabled
Identity theft	**1.0**	If personal information is stored on the computer without password protection
	0.5	If all personal information stored is protected using strong passwords
	0.1	If no personal information is stored
Financial loss	**1.0**	If financial transactions are made without checking for a secure connection
	0.5	If checks are made sometimes to ensure a secure connection during financial transactions
	0.1	If either checks are always made to ensure a secure connection during financial transactions or no financial transactions are carried out
Phishing	**1.0**	If you respond to emails asking for personal account details
	0.5	If you respond to some emails asking for personal account details
	0.1	If you delete all emails allegedly from banks, eBay, etc asking for personal account details
Spam	**1.0**	If no Spam filtering installed
	0.5	If Spam filtering done manually by the user
	0.1	If Spam filtering done automatically

Table 2: The probability of a threat occurring or a vulnerability being exploited

The questions that make up the risk assessment and the associated ISO17799 section are shown in Table 3. The web-based tool splits the questions into two sets, the first set, questions 1-14, relate to the controls that can be implemented to protect the user and their computer and the second set, questions 15-28, relate to best practices. The home user's answers to questions 1-14 will be quantified using appropriate values from Tables 1 and 2 to calculate a risk score which will be displayed to the home user as LOW, MEDIUM or HIGH at the end of the risk assessment. If their score is either MEDIUM or HIGH a hyperlink will be provided to a web page indicating ways in which the risk can be reduced and providing links to the resources required (i.e. Antivirus software). If their score is LOW they will be informed that their configuration is optimal and no changes are required.

As an example consider questions 1 and 2 which relate to Antivirus software. There are three possible scenarios. First if a home user answers yes to both questions then their risk score will be 100 (potential impact – Table 1) x 0.1 (probability – Table 2) = 10, which according to the risk level matrix in Figure 1 is LOW. Based on this they will be told that they do not need any additional controls. Second if a home user

answers yes to the first question but no to the second question then their risk score will be 100 (potential impact) x 0.5 (probability) = 50, which according to the risk level matrix is MEDIUM. Based on this they will be advised to check that the automatic update facility of their Antivirus software is enabled. Third if the home user answers no to question 1 then question 2 will not be displayed and their risk score will be 100 (potential impact) x 1.0 (probability – by default) = 100, which according to the risk level matrix is HIGH. Based on this they will be guided towards suitable Antivirus software and advised to install it as soon as possible. The same principle will be used for the other questions and where necessary.

The home user's answers to questions 15-28 will be recorded for each user. When the user has completed the questionnaire a hyperlink will be provided to a web page that will identify best practice based on any weaknesses highlighted in their answers i.e. scanning all email attachments for viruses.

As an example consider question 15 relating to the physical Internet connection. In this instance if the home user leaves their Broadband connected when not in use it will be recommended that they disconnect it as soon as they have finished with the Internet to minimise the risk because the longer they are connected the greater the opportunity for an intruder to identify it and gain unauthorised access.

Question number	Question	ISO17799 section
1	Do you have Antivirus software installed?	8.3.1
2	Do you regularly update the Antivirus software?	
3	Do you have Anti-spyware software installed?	
4	Do you download freeware or shareware from the Internet?	
5	Do you have a software firewall installed?	9.4.2
6	Do you have a hardware firewall installed?	
7	Do you have automatic updates for Microsoft Windows enabled?	10.4
8	Do you store personal information on the computer i.e. address?	9.6.1
9	Do you store financial information on your computer i.e. bank account details?	
10	Do you use strong passwords to protect personal and financial information?	9.3.1
11	Do you use online banking?	8.5.1
12	Do you purchase goods from Internet websites?	
13	Do you respond to emails asking for user account and password details?	8.7.4
14	Do you open all emails, even those from unknown sources?	
15	Do you leave your Internet connection on when not in use?	9.5.8
16	Do you regularly back-up your files to a suitable storage device i.e. CD?	8.4.1
17	Have you recently upgraded any software or hardware?	4.1.4 & 10.1.1
18	Have you recently installed any new software or hardware?	
19	Have you registered your system and application software?	10.4
20	Do you change your passwords at regular intervals i.e. monthly?	9.3.1
21	Do you use the same password for all accounts?	
22	Do you store your passwords on the computer?	
23	Do you always scan email attachments received for viruses?	8.7.4
24	Do you check that digital signatures are valid?	10.3
25	Do you scan files on all storage media for viruses before accessing them?	8.6.1
26	Do you only accept media from authorised or trusted sources?	
27	Do you regularly check the firewall log?	9.7.2
28	Do you know how the security settings on your Internet browser are configured?	9.4.1

Table 3: Risk assessment questions mapped from the ISO17799 standard (ISO, 2005)

Questions 15-28 are very important. For example, consider a home user with up to date Antivirus software installed. Although the control is installed the user may

regularly open email attachments without first scanning them for viruses. Their actions put them at a risk of a virus attack and this has not been captured in questions 1-14 but it is clear that the protection software and the user behaviour are both important in terms of information security.

Questions 1-28 will be the core part of the risk analysis tool. As a minimum the home user should be able to work their way through these questions and be presented with a set of risk scores along with the support needed to minimise them and a set of best practices which together with the controls will provide the best possible security solution.

5. Home User Risk Analysis Prototype

Apart from the structure and content of the risk analysis tool, the effectiveness of the tool depends very much upon the presentation and usability of the interface. For the proposed web-based risk analysis tool users will consist of a wide variety of people with differing computer literacy, from novices to competent computer users. Although all users will have a common purpose, their differing security awareness and education needs to be considered in order to design a tool that is effective across the broad spectrum of skill sets (i.e. not providing too much information for users who do not need it, yet providing sufficient information for those that do).

To this end, the prototype was designed with a simple interface with minimal possible user interactions permitted. For instance, as illustrated in Figure 2, a user has one of three options to select for each question: 'Yes', 'No' or 'Check'. The 'Check' button is provided to ensure users who have no understanding or knowledge of the question being posed are still able to answer the question by providing detailed instructions on where to find the information. Figures 3 and 4 illustrate an example of this assistance with respect to identifying the presence of Anti-Virus software.

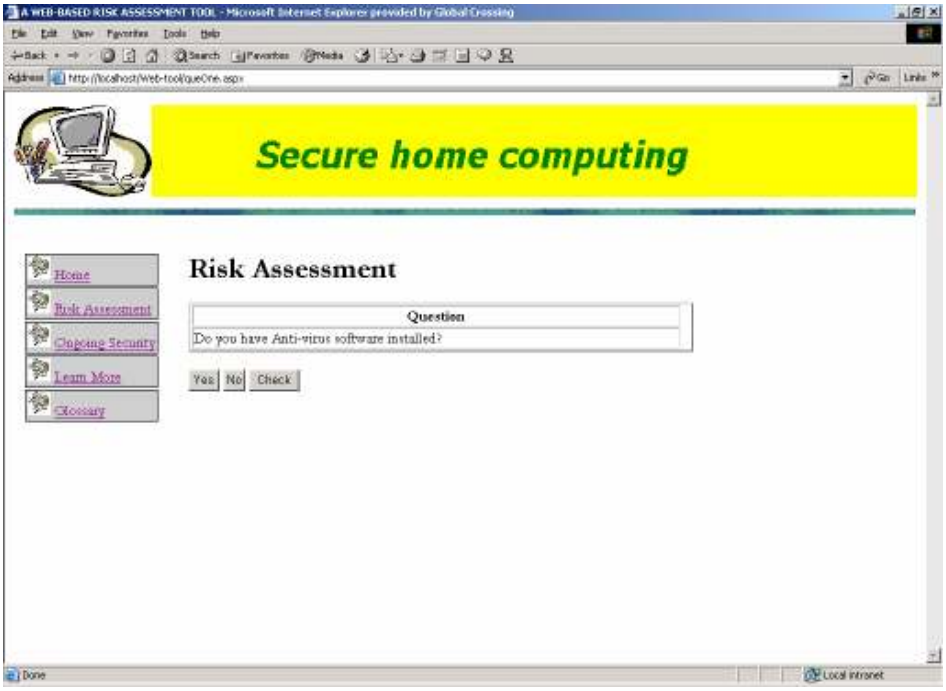

Figure 2: An Example of a Risk Assessment Question

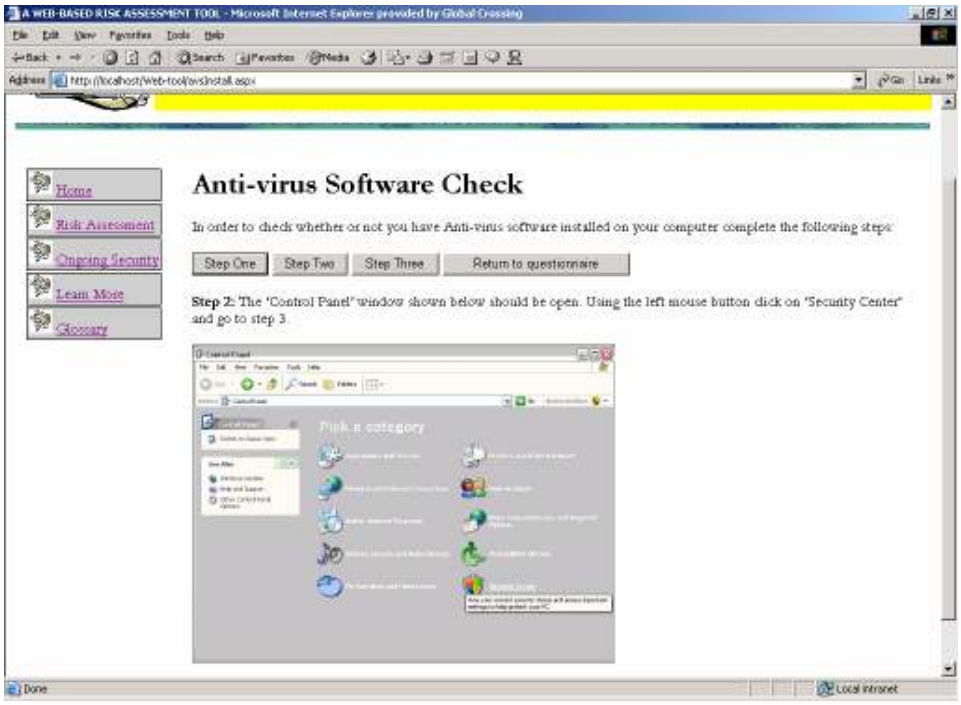

Figure 3: Step 1 of the Antivirus Installation Check

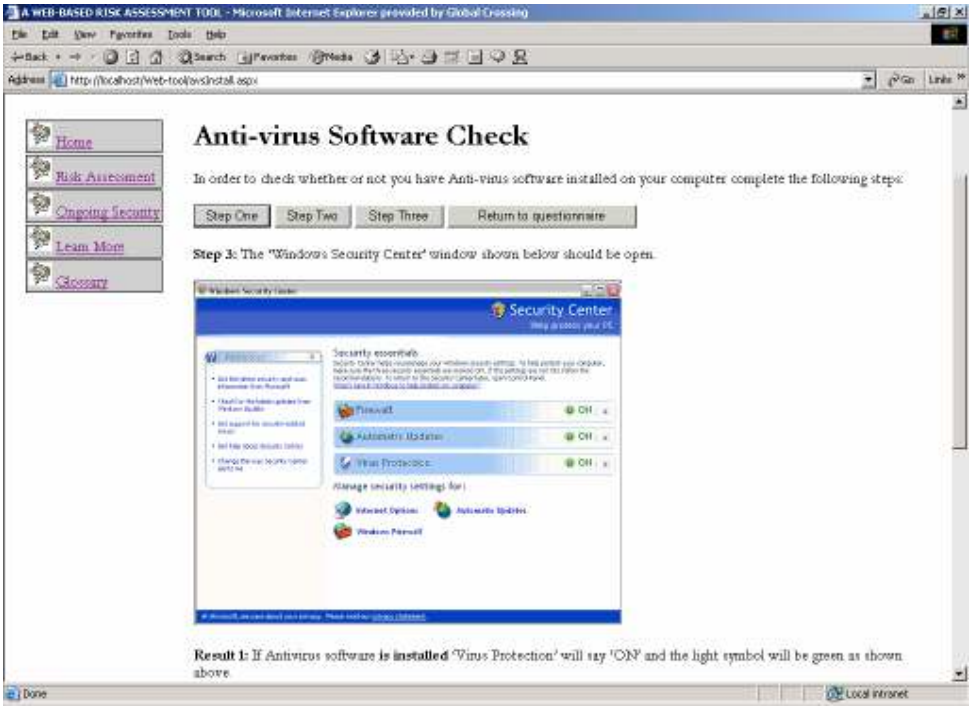

Figure 4: Step 2 of the Antivirus Installation Check

Having completed all the questions in a similar fashion to that presented, the user is presented with a results screen, as illustrated in Figure 5.

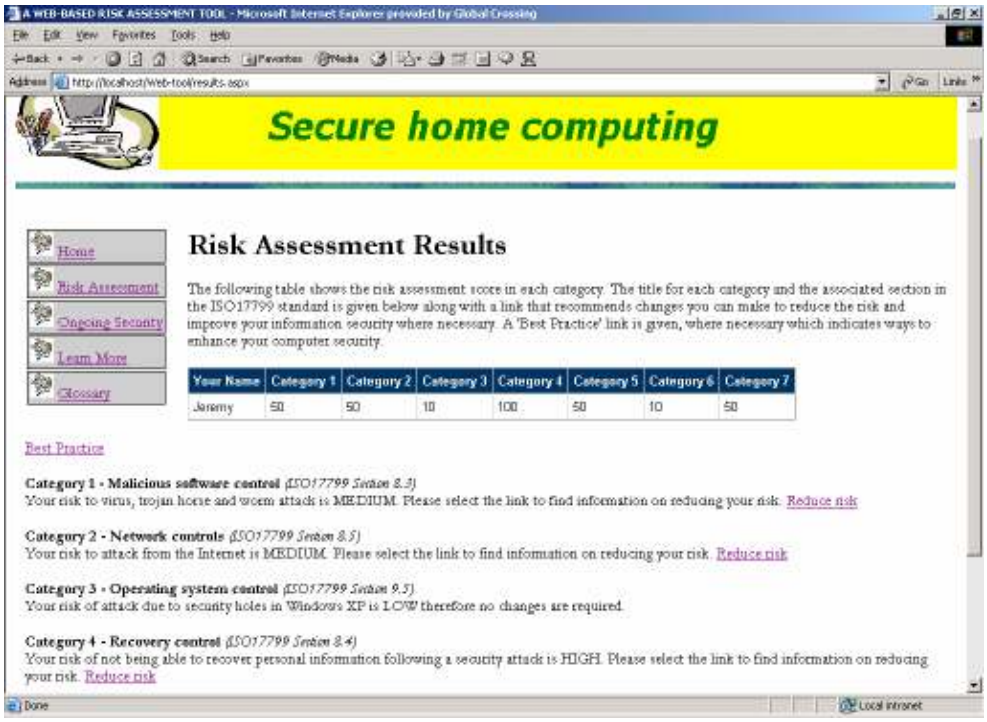

Figure 5: The Risk Assessment Results

The web page shows a table containing the user's name along with a number of categories and their associated risk score. The categories are associated with the various sections of the ISO17799 standard (as indicated on the page). The risk scores have been calculated using the risk matrix and the potential impact and probability previously presented. Each category from the table is listed explicitly underneath the table with a statement and hyperlink to additional information where appropriate (i.e. if the risk score is medium or above).

Depending upon the answers to questions 15-28 a 'Best Practice' hyperlink will be displayed as shown under the navigation menu. This will provide information of secure computing practices, such as good password management.

In addition to providing the risk analysis it was considered that additional educational information could be included to provide details on the various threats and vulnerabilities and indeed the protection mechanisms. This can be accessed by the home user clicking on the 'Learn More' link in the navigation menu from any page. This means that it would be up to the home user if they wanted to access this information and it would serve as an educational tool. For example, when the user selects the 'Learn More' option they could be presented with the web page similar to Figure 6.

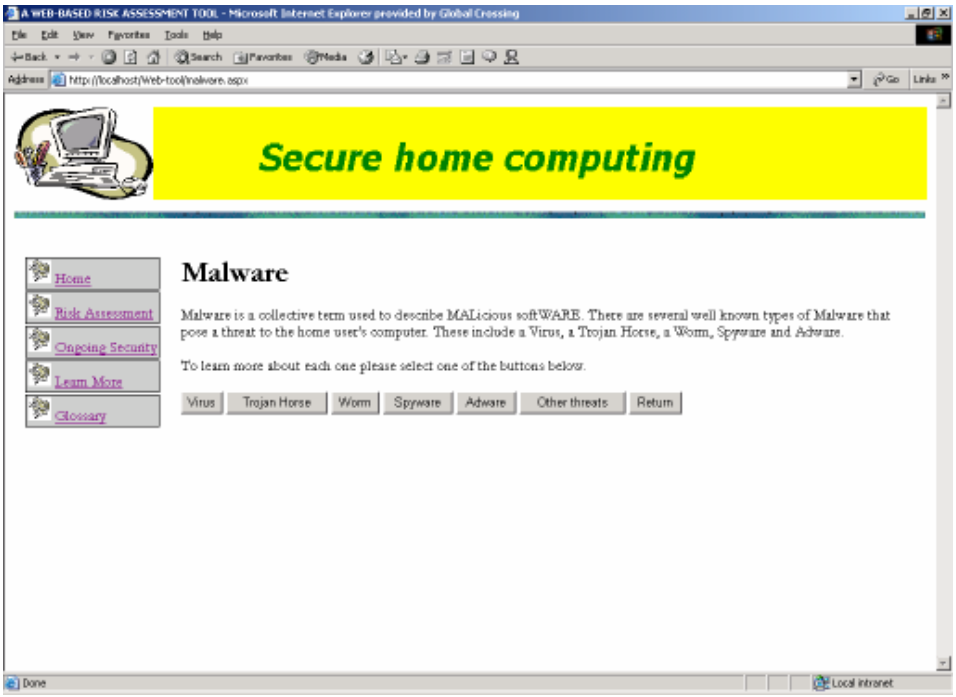

Figure 6: An Example of the Additional Information that can be Obtained

6. Conclusion

The widespread use of Broadband Internet access has led to the increased likelihood of hackers gaining unauthorised access to the home users computer resources and information. This problem is exacerbated by the users' lack of knowledge and the vulnerabilities of the computer software itself. Standards and techniques are available that provide a risk analysis. However these require expertise, are oriented towards organisations and may be expensive. Organisations offering online advice on home user security are generally biased towards their own products and often assume a certain level of knowledge.

The proposed web-based risk analysis tool overcomes these problems. It assumes no prior knowledge of risk management, it is aimed specifically at the home users and will be hosted on a web server for access free of charge. It uses a simple questionnaire with supporting information, to highlight the areas of risk and provides links to the resources required to reduce these risks to an acceptable level, educating the users in the process. The risk assessment questions focus on the home user environment with the controls being selected in accordance with those identified in the ISO17799 standard. In addition, the importance of secure working practice has been emphasised.

The advantage of using the ISO17799 standard as a framework for developing the tool is that it provides a consistent strategy, which is in compliance with a widely used and recognised standard. The next phase is user testing of a prototype tool that has been developed. The feedback will be used to improve the functionality of the tool as necessary.

7. References

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), '*Introduction to the OCTAVE® approach*', http://www.cert.org/octave/approach_intro.pdf, (Accessed 6 September 2005)
America Online and the National Cyber Security Alliance, AOL/NCSA (2005), '*AOL/NCSA Online Safety Study*', http://www.staysafeonline.info/pdf/safety_study_2005.pdf, (Accessed 2 August 2006)
Bailey, D. (2007), 'Broadband competition heats up', IT Week, http://www.computing.co.uk/itweek/news/2172007/broadband-competition-heats (Accessed: 20/2/2007)
Bates, R.J. (2000), '*Broadband Telecommunications Handbook*', McGraw-Hill
Ferguson, T. (2007), 'Broadband & ISPs', Silicon.Com, http://networks.silicon.com/broadband/0,39024661,39165842,00.htm?r=2 (Accessed: 20/2/2007)
France, P. (2004), *'Local Access Network Technologies'*, The Institution of Electrical Engineers
Fraser, B. (1997), '*Site Security Handbook*', http://www.ietf.org/rfc/rfc2196.txt, (Accessed 16 September 2005)
Glass, B. (2001), '*Got Broadband? You're under attack*', http://www.extremetech.com/article2/0,1558,23886,00.asp (Accessed 18 August 2005)
HM Government (2005), '*Get Safe Online Report*', http://www.egovmonitor.com/reports/rep12338.pdf (Accessed 21 August 2006)
ISACA (2005), '*COBIT and related products - Guidance material for IT Governance*', http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT.pdf, (Accessed 5 September 2005)
ISO (2005), 'Information technology – Security techniques – Code of practice for information security management', *ISO/IEC 17799:2005 International Organisation for Standardisation*
ISO (2005), 'Information technology – Security techniques – Evaluation criteria for IT security', *ISO/IEC 15408:2005 International Organisation for Standardisation*
Kairab, S. (2005), *'A Practical Guide to Security Assessments'*, Auerbach Publications
Kuhn, R., Tracy, C.M. & Frankel, S.E. (2002) 'Security for Telecommuting and Broadband Communications', *Special Publication 800-46*, *Recommendations of the National Institute of Standards and Technology*
Mash, S. (2002), 'Risk Assessment for Dummies', *Computer Fraud & Security Journal*, Vol. 2002, Iss. 12, pp. 11-13
Ofcom (2005), '*The Communications Market 2005 – 3. Telecommunications*' http://www.ofcom.org.uk/research/cm/cm05/telecommunications.pdf (Accessed 16 August 2005)
Orvis, W.J., Krystosek, P. and Smith, J. (2005), '*Connecting to the Internet Securely; Protecting Home Networks*', Computer Incident Advisory Capability CIAC-2324, www.ciac.org/ciac/documents/CIAC-2324_Connecting_to_the_Internet_Securely_Protecting_Home_Networks.pdf, (Accessed 22 August 2005)
Stoneburner, G., Goguen, A. and Feringa, A. (2002), 'Risk Management Guide for Information Technology Systems', *Special Publication 800-30*, *Recommendations of the National Institute of Standards and Technology*
Walsh, L.M. (2002), '*Security Standards*', http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml, (Accessed: 2/9/2005)