2012

Web-Based Risk Analysis for Home Users

R. T. Magaya
Plymouth University

N. L. Clarke
Edith Cowan University

DOI: 10.4225/75/57b55415cd8d4
Originally published in the Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

WEB-BASED RISK ANALYSIS FOR HOME USERS

R.T. Magaya[1] and N.L.Clarke[1,2]
[1]Centre for Security, Communications & Network Research (CSCAN), Plymouth University, United Kingdom
[1,2]SRI – Security Research Institute, Edith Cowan University, Perth, Western Australia
[1,2]info@cscan.org

Abstract

The advancement of the Internet has provided access to a wide variety of online services such as banking, e-commerce, social networking and entertainment. The wide availability and popularity of the Internet has also led to the rise in risks and threats to users, as criminals have taken an increasingly active role in abusing innocent users. Current risk analysis tools, techniques and methods available do not cater for home users but are tailored for large organisations. The tools require expertise to use them and they are expensive to purchase. What is available for home users are generic information portals that provide a whole-host of awareness raising information, much of which will have varying degrees of usefulness depending upon the particular individual, their technology usage and prior knowledge. As such a tool is required that can bridge the gap between bespoke risk assessment approaches that provide tailored information and broad-spectrum approaches that simply provide all information regardless of its relevance. The paper proposes a web-based risk analysis tool for home users that is simple to use, requires no prior knowledge or expertise of security and can provide bespoke and tailored guidance on improving a users security posture. The tool follows a simple step procedure for gathering key asset and behavioural information to inform the risk profiling process. A prototype was developed and evaluated by a sample of home users and 93% of the participants found the tool to be helpful and very informative.

Keywords
Risk analysis, risk assessment, ISO 27002:2005, NIST SP 800-30, SANS 20 Critical Security Controls, home user, information security awareness.

INTRODUCTION

As the cost of the Internet continues to fall more home users can now afford to get connected. According to the latest Ofcom report 80% of UK households now have access to broadband internet (Ofcom, 2012). Internet Service Providers, such as BT and Virgin, have begun rolling out fibre optic broadband that provides connection speeds of up to 100Mbps (Ofcom, 2011). As home users are now always connected to fast broadband Internet, they have come to depend on the Internet for their daily activities with at least 73 % adults in the UK spending about 8.3 hours per week on the internet (Ofcom, 2011).

This increased dependence however exposes users to numerous risks and threats (Furnell *et al*., 2007). A computer connected to the Internet without protection maybe infected with malicious software in under a minute (Postnote, 2006). Recently threats have become more sophisticated operating without the user's knowledge, stealing personal details or in the case of a bot where user's computer is used to for malicious purposes (GSO, 2010).

Several threats exist in different forms, these include but are not limited to malware, spyware, Trojans, denial of service, fraud, identity theft, data and service theft, unauthorised access, destruction of data and systems. In UK, 1 in 5 users have been victims of phishing scams, 40% have experienced a virus attack, and 19% have been victims of online identity theft (GSO, 2010). These figures show a continued increase in home users falling victim to online threats.

There is a requirement therefore to ensure home users understand the threats they face whilst online, both in terms of technology protection and their behaviour. In the Enterprise world, the most effective tool for ensuring organisations are well protected is risk management. It is an approach that ensures that a commensurate approach to protection is provided – providing more security to assets that are more valuable than others. Unfortunately, such approaches are not currently available to home users for a variety reasons – primarily based upon cost and expertise required. Instead, home users are left with blanket-based approaches that provide a complete range of security awareness information but take no consideration of the knowledge and advice a particular individual might need.

There is a need therefore for a solution that will provide home users with effective, tailored and simple to understand guidance on how to protect themselves and their information. This paper presents the results of research project focussed upon developing WEBRA, a web-based risk analysis tool.

BACKGROUND

Risk and Risk Assessment

Risk is the likelihood of a given threat exploiting a particular vulnerability against a particular asset. It is a combination of threats and vulnerabilities that may have adverse impact if they occur (HIPAA, 2010). Risk assessment identifies, quantifies and prioritises risks using a risk acceptance criterion. Risk assessment helps set priorities for managing risks and implementing controls to mitigate identified risks (ISO 27002). It also helps focus security activities on important assets, as well as selecting and implementing measures.

There are fundamentally two approaches to risk analysis: quantitative and qualitative. The former, utilising specific values associated to assets, threats and vulnerabilities to provide a numerical ranking of priorities. In recognition of the difficult of associating particular values to every aspect of the risk equation, the latter approach utilises non-numerical labels or categories (such as high, medium and low). In either approach, estimation of the value or label needs to be completed by an experienced risk assessment auditor who is able to set an appropriate level. The approaches, whilst very comprehensive, are very long, complex, time consuming and expensive.

There are several tools and standards available to help identify and manage risks. They however have a number of weaknesses. The available tools such as CRAMM, OCTAVE and COBIT require expertise and are tailored for large organisations. Standards such as the ISO 27002 and NIST SP 800 are designed mainly for large organisations. Many of the processes outlined in the standards are not applicable home users. They are for technical people as they require a certain level of expertise making them less suitable for home users with basic computing skills. Standards act as guidelines for reference; they do not provide information on how to implement controls.

The tool developed in this research will use qualitative risk assessment methodology for assessing risks. This involves determining the probability of an outcome using an interval scale such as High, Medium and Low. Values for threats and vulnerabilities will be predetermined based upon well recognised industry security reports (such as SANS 20 Critical Security Controls, NIST SP 800-53, Defence Signals Directorate (DSD) 35 Strategies and National Security Agency (NSA) Manageable Network Plan Rev. 2.1). The tool will specifically not use complex calculation to assess risk as the same can be achieved with simplicity with minimal impact over the guidance that is provided.

The web-based risk analysis tool will use a questionnaire to gather information about the assets the user has and the currently controls in place. The answers to the questionnaire will determine the user's level of risk and the tool will recommend any missing controls to reduce the risk; also providing assistance to the user in selecting and implementing the controls. Understanding that technical controls are only part of the solution, the tool also seeks to understand users' behaviour so that further specific guidance can be provided.

Awareness

A significant number of users are still unaware of their exposure to security risks (ENISA, 2009). The lack of awareness makes users vulnerable to online threats. According to Spears and Barki (2010) awareness is a pre-requisite for adequate protection. It is important to raise awareness given the ever-increasing risks. Awareness involves educating the user with the aim of focusing the user's attention on security by changing user behaviour and pattern (ENISA, 2010; NIST SP 800-16). The effectiveness of any security measures hugely depends on users' awareness of risks and countermeasures.

Websites like Get Safe Online, Microsoft Security Centre provide awareness and security guidance information to help users stay safe online. They are however not structured in a clear or logical way making it difficult for a user to search for and find specific information. They assume a certain level of computer security knowledge. They do not provide adequate information or assistance about selecting and implementing controls.

WEBRA TOOL

The web-based risk analysis (WEBRA) tool utilises the ISO 27002, NIST SP 800 – 30 standards base guidelines to identify assets and formulate questions. This was to ensure all important security areas outlined by these industry-accepted standards are incorporated.

The tool consists of a two-part questionnaire that is short, easy to use and tailored for a home user environment. Help will be provided throughout the tool in the form of mouse overs, links and pop up description boxes to explain any technical nomenclature to the user. There is also a full glossary page with explanations of risk and security terms. The tool, unlike existing tools, also caters for all home users without requiring any prior knowledge of security. The tool will have four main processes:

- **Asset selection**: the user selects assets they have, data stored on the assets, services used and controls currently implemented.
- **Behavioural practice**: the user answers a series of questions regarding their use of systems
- **Control ranking**: the system analyses the missing controls and determines risk level based on a control priority ranking system.
- **Output/Recommendations**: The tool will provide an overall risk rating for each asset and will recommend missing controls that are required to mitigate the risks. Additional guidance will be provided through a description of each control and links provided to direct the user where they can get the controls or guidance on how to implement them. The WEBRA tool will also recommend safe practice behaviour to the user such as regular updates, scanning removable media, changing passwords etc. In addition the tool will educate the user providing explanations and links to other useful websites. The information on the recommendations page is presented in a simple and comprehensive manner.

The web-based risk analysis tool will be made up of a two part questionnaire divided into section 1 (assets and controls) and section 2 (user behaviour).

Assets and Countermeasures

This section forms the core part of the risk analysis tool. The questions will enable the tool to assess the user's risk level and recommend appropriate controls. The questions help identify the user's exposure to risks based on the assets they have and the missing controls.

The tool begins by building an asset profile for the user by identifying the assets. For each asset, a number of questions will be asked regarding what the asset is commonly used for. The user will also be asked to indicate the current security controls they have in place. The system ranks all controls according to priority based on the SANS 20 Critical Security Control List (SANS, 2011); any controls missing will be highlighted as recommendations and links to relevant websites provided in the guidance.

Key to the design of WEBRA was usability. The system had to be simple, easy to understand and easy to complete. All questions in section 1 are in tabular form (as shown in Figure 1 below). This was done to simplify the user input process and for a good interface that makes navigation easier and quicker for the user.

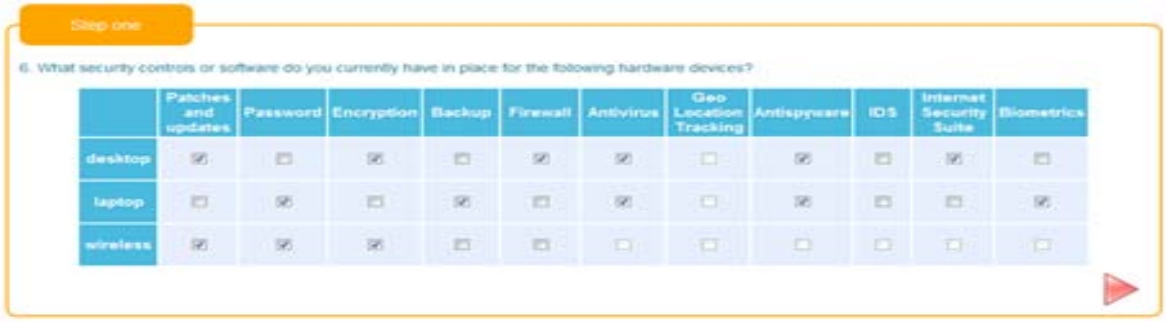

Figure 1: Asset Questionnaire.

User Behaviour

The second part of the web-based risk analysis questionnaire aims to inform and educate the user about staying secure. The questionnaire evaluates user behaviour and awareness. The questions are in a multiple-choice form and assess existing security practices in a number of areas outlined in both the ISO 27002 and NIST SP 800 – 30 standards.

The 18 questions cover user behaviour in the home environment; for example how regularly a user updates their security software, change passwords, perform backups etc. Several other topics are covered including access controls, security policy, authentication, encryption and privacy. See Figure 2 below for sample questionnaire.

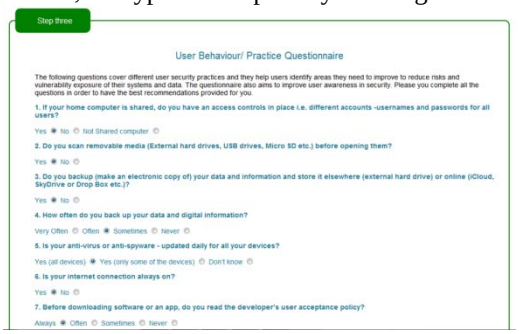

Figure 2: Behavioural Questionnaire.

Once the user has completed all the questions in this section the tool will provide recommendations for best practices. Links are provided to websites that offer best practice guidelines that will address any insecure user behaviour.

Determining the Risk Level

Critical Controls	WEBRA Controls	Priority
Inventory of Authorized and Unauthorized Devices	Identify the assets the user has done by the tool (Stage 1 WEBRA)	RA tool
Secure Configurations for Hardware and Software on Laptops, Workstations, and mobile devices	Secure configuration of security software and system settings	High
Continuous Vulnerability Assessment and Remediation	Patches and updates	High
Malware Defences	Anti- Virus, Anti-Spyware	High
Controlled Use of Administrative Privileges	Passwords	High
Application Software Security	Encryption	Moderate
Data Recovery Capability	Backups	Moderate
Secure Configurations for Network Devices such as Firewalls, Routers incl. wireless, and Switches	Firewalls	Moderate
Boundary Defence	Physical security, case, pouch	Moderate
Controlled Access Based on the Need to Know	User Accounts for different users	Low
Account Monitoring and Control	Biometrics	Low
Data Loss Prevention Capability	GPS tracking	Low
Incident Response Capability	IDS	Low

Figure 3: Asset Priority List. (Adapted from SANS, 2011).

The web-based risk analysis tool uses a modified control prioritisation list tailored for home users (an example of which is illustrated in Figure 3). All controls listed apply to home users. The 20 Critical Controls takes into consideration the latest threats and vulnerabilities. This eliminates the need quantitative estimate values for threats and vulnerabilities and significantly reduces the complexity of the resulting risk assessment process.

Input data from Assets and Countermeasures questionnaire is used to determine the level of risks. The process allows controls in place to be mapped to the assets and indicate areas where controls need to be implemented. The tool will rank each control in order to give a view of relative importance (IRM, 2002). The controls are ranked according to their importance in keeping assets secure.

The WEBRA will use a simple rating scale of High, Medium and Low to represent the degree of risk from a security perspective in terms of the priority of the control. The rating will be based on the prioritisation of controls in terms of their effectiveness and potential impact in reducing common threats and vulnerabilities. This will help user prioritise resources and effort on critical areas in order to prevent attacks and intrusions. It will also help ensure that systems have the most critical baseline controls in place.

Several controls can be used to secure assets and their importance differs depending on the threats and vulnerability of not having the controls in place. For example for some controls like backups, the risk of not having them is low to medium while the absence of antivirus software results in high risk exposure of the asset.

The reason for using this methodology was to eliminate the subjectivity inherent in qualitative analysis methods while ensuring the score reflects the importance of controls based on statistics (such as the 20 Critical Security Controls in Figure 2) that reflect vulnerabilities and threats affecting users today.

The result of the risk assessment questionnaire will lead to recommendations tailored to the user's assets. An overall risk rating for each, missing controls and their priority ranking will be displayed on the recommendations page.

Overall Risk Rating

The tool provides the overall risk rating as High (Red), Medium (Amber) and Low (Green). The determination of which rating to provide the overall assessment is based upon if at least one of the missing controls is at a higher priority, the overall system is at that higher priority. For example, it an assessment has a single High priority ranking in the controls list then the overall risk is High. Whilst this approach is likely to lead to an overall rating which is higher than normal, it is important to ensure users are not given a false sense of security. Given it only takes a single missing countermeasure to compromise a system, this high-watermark approach was deemed the most appropriate.

WEBRA DESIGN

The WEBRA prototype was developed to demonstrate the functionality, usability and the suitability of the tool for home users. The tool consists of a front-end website for the user interface, and a back-end database that stores all the input data, asset lists, countermeasures and priorities.

The Interface

Usability was a key design requirement enabling users to complete the process quickly and easily. The interface determines whether the user can quickly learn to use the tool. Figures 3 and 4 below shows the interface of the tool. Functionalities like navigation through menus, colours for different risk levels and priorities, mouse over and hovering makes the tool more usable and easy to follow. Figures 4 to 7 below shows screenshots of the tool's interface

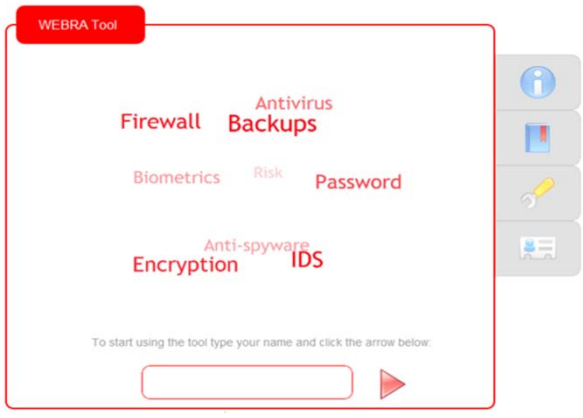

Figure 4: Home Interface

Figure 5: Asset Interface

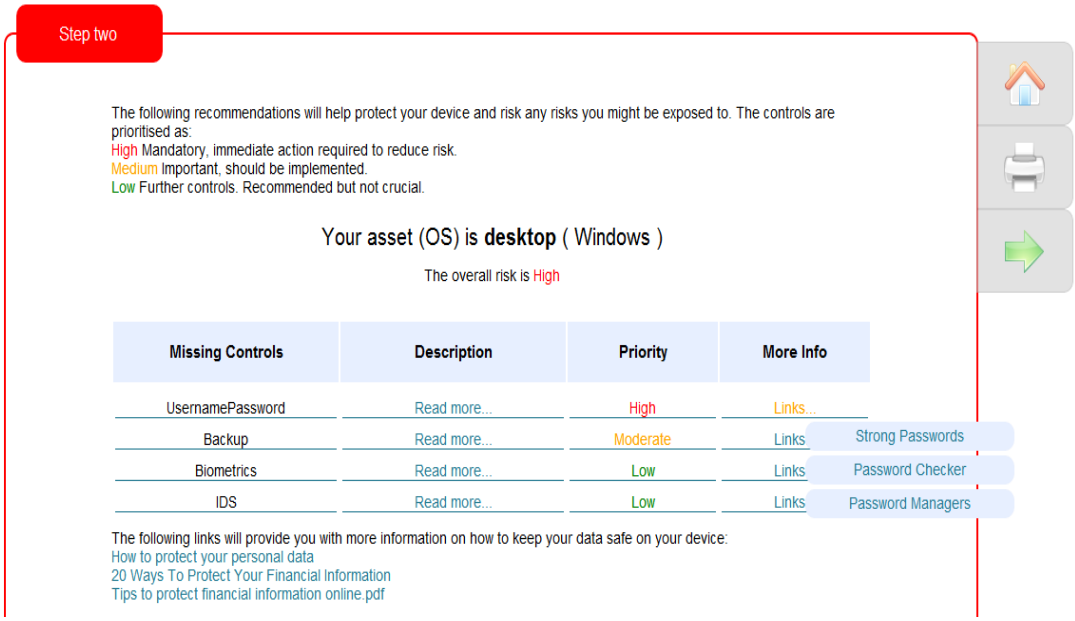

Figure 6: WEBRA Asset Assessment

Figure 7: User Behaviour Assessment

WEBRA EVALUATION

The prototype was evaluated to test its suitability for home users and to see if it met the requirements of home users that existing tools are not addressing. To this end, two types of evaluations were undertaken.

- A quantitative evaluation of the tool by home users involving a sample of 50 participants.
- A qualitative evaluation involving a focus group of information security professionals.

The quantitative evaluation provided an opportunity to canvas a large number of home user attitudes and opinions specifically with regards to WEBRA. The second evaluation provided for more in-depth analysis and discussion of the WEBRA tool but importantly also to provide an analysis of the tool in comparison to the current state of the art. The focus group tested the WEBRA tool alongside a number of existing tools such as Secunia PSI, Get Safe Online, and Microsoft Baseline Security Analyser (MBSA). The usability of the tool, cost, help provided, recommendations and links to other information were some of the criterion used to evaluate these tools.

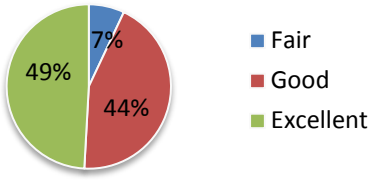

Figure 8: Usability of the Tool (Ease of use)

Feedback from the users indicated that most (93%) users found the tool very easy to use and the interface was user friendly (as illustrated in Figure 8). More than 80% of users who tested the tool said the tool was easy to understand and could be used with minimum technical knowledge (as illustrated in Figure 9).

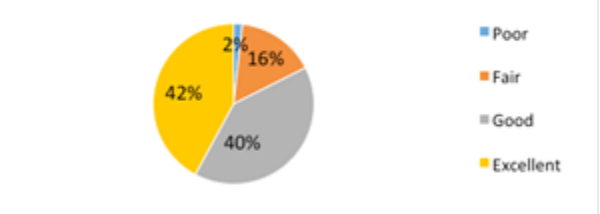

Figure 9: Degree of Technical Knowledge Required

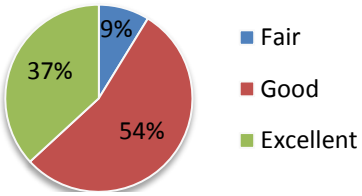

Figure 10: Provided implementation assistance

As shown in Figure 10, the majority of users (91%) felt the tool had provided adequate assistance and links to help them select and implement recommended controls. Users also found the recommendations to be helpful because they were tailored to their needs.

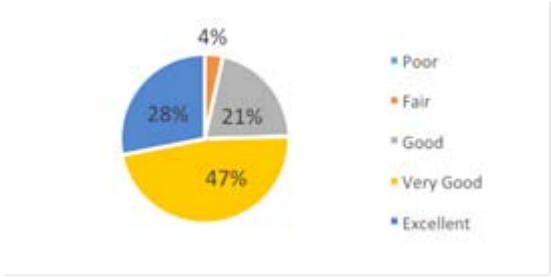

Figure 11: Improvement in Security Awareness

Feedback from the participants was that the recommendations were very helpful and 78% of users said the tool had improved their security awareness (as illustrated in Figure 11). Some users said the tool encouraged them to step up the security of their devices.

Overall, respondents liked the friendly user interface that made the tool easy to follow and use. Users found the questions easy to understand and the tool improved their security awareness. The process took reasonable time to complete. Some issues were raised regarding the use of technical language such as intrusion detection and digital certificates; however, this manifested due to an incomplete glossary within the prototype rather than a fundamental issue with the WEBRA tool.

Feedback from the focus group was broadly inline with the quantitative evaluation – the tool was comprehensive covering all aspects from risk assessment, control recommendation and implementation guidance to educating the user. Other tools only covered a few areas like awareness and patches and updates. The group also noted that WEBRA supported different devices and platforms. The group also liked the simple and comprehensive report specific to the user's assets.

Overall the group concluded that the WEBRA tool was *"excellent and offered tailored recommendations to the user"*. WEBRA was also easy to use for users with little experience, taking reasonable time to complete and very educational – making it more suitable for home users than other tools. Areas the group felt could be improved include adding more controls and automatic detection of some controls like firewall.

CONCLUSION AND FUTURE WORK

This research looked at risk analysis and how it affects home users. This paper proposes a tool that is designed based upon industry standards such as ISO 27002 and NIST SP 800. A web-based risk analysis tool was designed and developed to help users analyse and assess their security requirements: requesting and providing information in a simple and easy to use manner. Whilst not performing in-depth risk analysis, as is undertaken in Enterprise organisations, WEBRA's approach focuses upon usability and provides a tailored list of recommendations for the home users – with associated links to further information where required. The prototype needs further refinement to include more controls and more information. Thought will be given to providing an interface and process for administrators to easily update the system – assets and countermeasures database, latest threats and vulnerabilities. Future work will also focus upon the automatic detection of assets and services – this will remove the need for the user to input this information, thereby further reducing any possible user inconvenience.

REFERENCES

Elky, S (2006). *An Introduction to Information System Risk Management.* SANS Institute. InfoSec Reading Room.

ENISA (2009). *Awareness Raising. European Network and Information Security Agency.* Retrieved from http://www.enisa.europa.eu/media/key-documents/fact-sheets/Awareness-1.pdf

ENISA. (2010). *The new users' guide: How to raise information security awareness.* Retrieved from http://www.enisa.europa.eu/

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). *Assessing the security perceptions of personal Internet users.* Computers & Security, 26 (5). pp 410-417.

GSO. (2010). *UK Internet Security: State of the Nation. The Get Safe Online Report.* November. Retrieved from http://www.getsafeonline.org/media/Get_Safe_Online_Report_2010.pdf

HIPAA. (2007). *Basics of Risk Analysis and Risk Management.* HIPAA Security Series. Volume 2: 6/2005: rev. 3/2007

IRM (2002). *A Risk Management Standard.* The Institute of Risk Management (irm). Retrieved from http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

IS0 27002. (2005). *Information technology. Code of practice for information security management.* British Standards Institution. BS ISO/IEC 27002:2005. ISBN 0 580 46262 5.

NIST SP 800 – 30. *National Institute of Standards and Technology (NIST) Special Publication 800-30. Risk Management Guide for Information Technology Systems.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST SP 800-16. *Information technology security training requirements: A role- and performance-based model.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

Ofcom. (2011). Communications Market Report: UK. Retrieved from http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf

Ofcom. (2012). *Communications Market Report: UK.* Retrieved from http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf

Postnote. (2006). *Computer Crime.* The Parliamentary Office of Science and Technology. Retrieved from http://www.parliament.uk/documents/post/postpn271.pdf

SANS (2011). *20 Critical Security Controls - Version 3.1*. Retrieved from http://www.sans.org/critical-security-controls/guidelines.php

Spears, J. L. and Barki, H. (2010). User Participation and Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503-522.