Journal of Universal Computer Science, vol. 18, no. 6 (2012), 845-856
submitted: 15/10/11, accepted: 15/2/12, appeared: 28/3/12 © *J.UCS*

A Framework for the Comparison of Best Practice Recommendations and Legal Requirements for South African Banks

Carla-Lee Botha
(School of Computing, University of South Africa, Pretoria, South Africa
carlaleebotha_44@live.co.za)

Elmarie Kritzinger
(School of Computing, University of South Africa, Pretoria, South Africa
kritze@unisa.ac.za)

Marianne Loock
(School of Computing, University of South Africa, Pretoria, South Africa
loockm@unisa.ac.za)

Abstract: South African home users of the Internet use it to perform various everyday functions. These functions include, but are not limited to, online shopping, online gaming, social networking and online banking. Home users of online banking face multiple threats, such as phishing and social engineering. These threats come from hackers attempting to obtain confidential information, such as online banking authentication credentials, from home users. It is, thus, essential that home users of online banking be made aware of these threats, how to identify them and what countermeasures to implement to protect themselves from hackers. In this respect, information security awareness (ISA) programmes are an effective way of making the home users of online banking aware of both the threats they face and the countermeasures available to protect themselves from these threats. South African banks have to comply with certain legal requirements when implementing information security awareness initiatives. Non-compliance or failure to demonstrate due care and due diligence, should a security incident occur, will result in financial penalties for the bank as well as possible brand damage and loss of customers. Banks implement international best practice recommendations in an effort to comply with legislation. These include recommendations for information security awareness. This research proposes a framework which, predominantly, can be applied when determining and comparing information security best practice recommendations and information security legal requirements for online banking. The primarily aim of this paper is to investigate whether the implementation of best practices are sufficient to comply with legal requirements. A selected list of information security best practices was investigated for best practice recommendations while a selected list of information security legislation was also investigated for legal requirements imposed on South African banks. A gap analysis was performed on both these recommendations and requirements to determine whether the implementation of best practice recommendations results in compliance with legal requirements. The gap analysis found that the implementation of best practice recommendations does not result in compliance with legal requirements. Accordingly, the outcome of this research highlights the importance of applying such a framework in a comprehensive fashion to understand the legal requirements imposed and ensure that adequate controls are in place for achieving compliance.

Keywords: information security awareness, online banking, home users, legislation, best practice, South Africa
Categories: H.3.5, SD K.3.2, SD K.6.5

1 Introduction

South Africans use the Internet for business purposes and at home. Home users, who have access to the Internet, use it to perform various functions on a daily basis. These functions include online shopping, online gaming, social networking and online banking [Wu et al. 2012]. Online banking is a system which allows home users to conduct their banking over the Internet [Investorwords 2011]. Online banking is a convenient way for carrying out banking tasks, such as managing bank accounts, checking an account transaction history, transferring money and paying accounts [Davinson and Sillence 2010, Kim and Park 2012, Reis et al. 2011]. Online banking eliminates the need to travel to a bank each time the customer has to complete a transaction, giving individuals the option to bank in the comfort of their own homes.

This has become evident in the South African media as major banks launch advertising campaigns displaying the benefits of this service and encouraging home users to make use of this convenient form of banking. The number of Internet users in South Africa has increased from 2.4 million users in 2000 to 5.3 million users in 2009 [South Africa Internet Usage and Marketing Report 2009]. Therefore, a large number of South African home users are becoming aware of and are able to use online banking. From a security perspective, the human element of the security chain must be addressed [Albrechtsen 2007, Da Veiga and Eloff 2010, Siponen, 2001].

While convenient, home users face multiple threats, such as phishing and social engineering, when participating in online banking [Reis et al. 2011, Pezderka, and Sinkovics 2011]. These threats emanate from hackers attempting to obtain confidential information from home users, for example, online banking authentication credentials. It is, thus, essential that the home users of online banking be made aware of these threats, how to identify them and the countermeasures available to protect themselves from the hackers' attempts [Choo 2011, Reis et al. 2011].

An information security awareness programme is an effective means of doing this. Information security awareness comprises one component of an information security programme and it is associated with the education of the end users of an information technology system on relevant information security threats and countermeasures [Wilson and Nash 2003]. This research addresses the responsibilities incumbent on South African banks for the information security awareness of South African home users of online banking.

This research investigates the latest and most prevalent information security threats home users of online banking should be aware of. However, predominantly, this research will investigate both information security best practice recommendations and information security legal requirements for information security awareness. A selected list of information security best practices will be investigated for best practice recommendations, while a selected list of information security legislation will also be investigated for legal requirements imposed on South African banks. A gap analysis will be performed on both these recommendations and requirements to determine whether implementation of information security awareness best practice recommendations results in compliance with information security awareness legal requirements.

2 Research Methodology

The research methodology used within this research comprises five processes. The first process was an in-depth literature review. A literature review was conducted which found that home users face multiple threats when participating in online banking and should be made aware of these threats and relevant countermeasures through the use of an information security awareness programme. The relevant threats mould the content of an information security awareness programme aimed at home users of online banking. These threats create the need for legislation to regulate information security in the banking industry and banks, and in response to the legal requirements imposed, implement best practice in an effort to comply. The literature review concluded by identifying three unique building blocks ("top ten" threats, legal requirements and best practice recommendations).

The second process within the research methodology included an investigative selection process to add content to the identified building block originating from the literature review. The investigative selection process for each building block will be discussed within appropriate sections.

The third process included a modelling phase where the three building blocks were used in relationship with one another to form the proposed framework. The relationship placement of the different building blocks will be discussed within the rest of the paper.

The fourth process within the research methodology included a gap analysis. A gap analysis was performed on the populated framework. The result of the gap analysis helped determine whether the implementation of best practice recommendations results in compliance with legal requirements. In addition, it highlighted the importance of applying such a framework in a comprehensive fashion to understand the legal requirements imposed and ensure that adequate controls are in place with which to achieve compliance.

The last process to complete the research methodology cycle included a testing phase. To test this framework, a selected list of information security best practices was investigated for best practice recommendations while a selected list of information security legislation was also investigated for legal requirements imposed on South African banks. The building blocks were populated with test data (obtained through the literate review process) for the purposes of testing the framework; therefore, the content of each building block can be adapted to change according to individual specifications and requirements.

3 Current and Prevalent Threats to Online Bankers

Online banking has multiple information security threats associated with its use. These threats should be investigated and should mould the content of an information security awareness programme aimed at home users of online banking. Based on certain criteria, the proposed framework requires an investigation of the latest and most prevalent information security threats facing the home users of online banking. These threats create the need for legislation to regulate information security in the banking industry and motivate for the implementation of information security

initiatives like an information security awareness programme. The objective of the analysis is to create a top ten list of threats facing home users of online banking. These threats are matched with countermeasures that the home user may implement. Selected electronic sources are analysed for information on information security threats. Accordingly, the sources used to identify these threats should have the following attributes:

- an information security focus
- published content, written in the last two years, on current security topics
- including, in their reporting, security threats which would target the home users of online banking

To demonstrate, the electronic sources selected are:

- SANS (www.sans.org);
- National Cyber Security Alliance (www.staysafeonline.org);
- CSOOnline (www.csoonline.com);
- CIO (www.cio.com);
- Bankinfosecurity (www.bankinfosecurity.com); and
- Elsevier academic papers (accessed online via Unisa Library).

Although this is not an exhaustive list, these sources may be considered sufficient for this demonstration. Each of these electronic sources should be analysed for information security threats facing the home users of online banking. The results should be narrowed down, based on frequency, to a top ten list of information security threats facing home users of online banking. To test, the selected electronic sources were analysed and the threats identified. These threats are:

- phishing, spoofed websites
- keystroke logging
- malware
- social engineering
- minimal protection of data
- password guessing or theft
- sensitive information in the user's recycle bin
- shared computer threats
- out-of-date patches and software

The most prevalent information security threats facing the home users of online banking extracted from the identified electronic sources are those aiding identity theft.

4 Information Security Awareness Best Practice

In industry, organisations attempt to gain a competitive edge by providing a better service or product. Methods and procedures used to provide services or produce products are reviewed and improved over time to try to achieve an optimal way of doing things. The methods and procedures considered at the time to produce the most desirable outcome become known as industry best practice. A best practice is a procedure or method which is known to achieve the best possible results [BusinessDictionary 2011, Methods & Tools QA Resources 2009, Wikipedia, 2011].

In this section, focus is placed on information security best practices and international standards. Information security best practices and international standards are important for effective information security governance [Von Solms and Von Solms 2004]. Banking organisations implement best practices for a number of reasons. These include improving customer confidence in the banks' security programmes and ensuring their information security programmes are at a standard where, should a security breach occur, they are able to demonstrate due care and due diligence and avoid financial and legal consequences [Von Solms and Von Solms 2004, Williams, 2008]. The criteria for the selection of the best practices to be analysed include:

- it must be an internationally accepted information or information security standard which can be implemented in a banking organisation
- it must be available to the public

Based on these criteria, ISO/IEC 27001, COBIT (Version 4.1) and the Standard of Good Practice for Information Security (2007) have been selected for demonstration and are analysed for information security awareness recommendations. This is not an exhaustive list, but sufficient for this demonstration and testing of the framework. Other best practices can be used to populate the framework depending on the individual's specifications and requirements.

The objective of the analysis is to create a list of recommendations organisations must implement when striving to comply with international information security best practices. The recommendations extracted from the selected information security best practices are:

A. Banks should identify what the home users of online banking need to be made aware of through the medium of information security awareness programmes, for example, threats and countermeasures.
B. Banks should identify the home users of online banking as a target audience for user awareness programmes and ensure that awareness materials reach all the home users of online banking.
C. Banks should conduct surveys on the level of security awareness among the home users of online banking after the implementation of an information security awareness programme. These results should serve as an input for improving the next information security awareness programme.
D. Banks should make home users aware of incident-reporting procedures and expected response times.
E. Banks should conduct a survey among home users on their level of satisfaction with the response to online banking incidents reported. These results should be used to improve the incident response procedure. Home users of online banking should then be made aware of new incident reporting procedures and incident response times.
F. Banks should make the home users of online banking aware of ways in which they may protect their information.
G. Banks should make home users aware of, and require them to comply with, certain security requirements as stipulated in the information security policy before signing up for online banking.
H. Banks should demonstrate to the home users of online banking that the banks adopt an uncompromising position in respect of information security management and awareness.

In summary, banks should identify what home users should be made aware of through an information security awareness programme, provide a facility for home users to report incidents and review incidents and feedback from home users to determine how information security awareness programmes can be improved.

5 Information Security Awareness Legislation

Online banking is convenient, but has many information security threats associated with its use. The presence of these information security threats and their consequences motivates for regulation in the industry, increasingly making information security the subject of national and global legislation [Gerber and Von Solms 2008]. This research investigates what requirements selected legislation imposes on South African banks for information security awareness among the home users of online banking.

The proposed framework requires the investigation of what information security awareness requirements legislation imposes on South African banks. To determine which documents should be analysed, it is recommended that an attorney working in the information security risk and compliance space be consulted for their opinion on relevant international banking legislation, South African legislation and other relevant documents. In addition, the South African government's website for publicly available documents should be visited to research other pertinent documents and identify relevant amendments to the final list of documents. To test, legislation was selected based on an interview with Mra Khwar Nyo. Mra is an attorney and Certified Information Privacy Professional (International Association of Privacy Professionals) working in the Security and Privacy Services team at Deloitte & Touche, South Africa. Mra was consulted for her opinion on which legislation should be included in this study. She advised on international banking legislation, South African legislation and suggested other relevant documents. A visit to the South African government's website for publicly available documents was carried out to research other pertinent documents and identify relevant amendments to the final list of documents. The identified legislation is:

- Basel II;
- Sarbanes-Oxley Act of 2002;
- Gramm-Leach-Bliley Act of 1999;
- Electronic Communications and Transactions Act, 2002;
- Protection of Personal Information Bill;
- Promotion of Access to Information Act, 2000;
- The Code of Banking Practice;
- Consumer Protection Act, 2008;
- Constitution of the Republic of South Africa;
- Code of Governance Principles for South Africa (King III), 25 February, 2009; and
- Electronic Communications Act, 2005.

This is not an exhaustive list, but these sources are sufficient for this demonstration. Other legislation can be used to populate the framework, depending on the individual's specifications and requirements. The objective of the analysis is to create a list of legal requirements South African banks must satisfy when

implementing an information security awareness programme aimed at the home users of online banking. The legal requirements extracted from the selected legislation are:

1. Banks should identify the home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all the home users of online banking.
2. Banks should make consumers aware, in plain language, of any risk associated with the online banking service that an ordinarily alert consumer would not expect.
3. Banks should promote a culture of cyber security by developing and implementing an information security awareness programme aimed at home users of online banking.
4. Banks should make home users of online banking aware that they take a stern stance on the security of online banking transactions and privacy of personal information.
5. The bank should make timely and frequent public disclosures of information which will assist the public in determining how effective a bank is at risk identification, assessment, monitoring and control. This should include the use of an independent auditor.
6. Banks should make home users of online banking aware of the threats they face when participating in online banking, including threats to the privacy of their personal information, and recommend countermeasures they should implement to mitigate the associated risks.
7. Banks should make antivirus software available to home users of online banking.
8. Banks should make home users aware of incident-reporting procedures and expected response times.
9. Banks should review the content of information security awareness programmes to include new threats, changes in incident-reporting procedures and response times and make home users aware of these new threats.
10. Banks should make the home users of online banking aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
11. Banks should make home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before collection or processing takes place.
12. Banks should make the home users of online banking aware that they will be notified if it can be established that their personal information has been compromised.
13. Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking.
14. Banks should make home users of online banking aware that they will be informed should a requestor other than the home user attempt to access their

personal information or financial information. The bank should also inform the home user of their rights to refuse access to their personal information by the requestor.

15. Banks should recommend to personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis.
16. Banks should make personal clients using online banking aware that security of their personal computer is the responsibility of the personal client.
17. Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service.
18. Banks should recommend to personal clients using online banking that they be careful to enter accurate transaction information as transactions cannot be reversed without the recipient's consent.

In summary, banks need to demonstrate to home users a stern stance on information security, make home users of online banking aware of the risks they face when making use of the online banking service and advise home users on what personal information they need to keep confidential.

Figure 1 illustrates the gap between the selected legal requirements and selected best practice recommendations by showing which best practice requirements support each legal requirement. Regarding figure 1, the legal requirements (numbers 1 to 18) were discussed in section 5 and the best practices recommendations (letters A to H) were discussed in section 4.

6 Comparison of Best Practice Recommendations and Legal Requirements

There is a close link between information security best practice and legal requirements for information security, making them hard to separate [British Standards Institution 2005, King Committee on Governance 2009]. For example, in control section A.15, international best practice ISO/IEC27001 deals with compliance with legal requirements, including laws, regulations, statutes and contractual obligations. In addition, compliance with legal requirements can be achieved by implementing best practice controls, such as implementing COBIT to comply with Sarbanes-Oxley. Compliance ensures that, should a legal breach occur, the organisation is able to demonstrate due care and due diligence, avoiding financial and legal consequences [Von Solms and Von Solms, 2004, Williams 2008].

Information security programme best practice recommendations and information security programme legal requirements were discussed in sections 4 and 5, respectively. In this section, in accordance with the proposed framework, a comparison between these recommendations and requirements is demonstrated to determine if implementation of the identified information security programme best practice recommendations will result in compliance with the identified information security programme legal requirements. This is depicted in Figure 1.

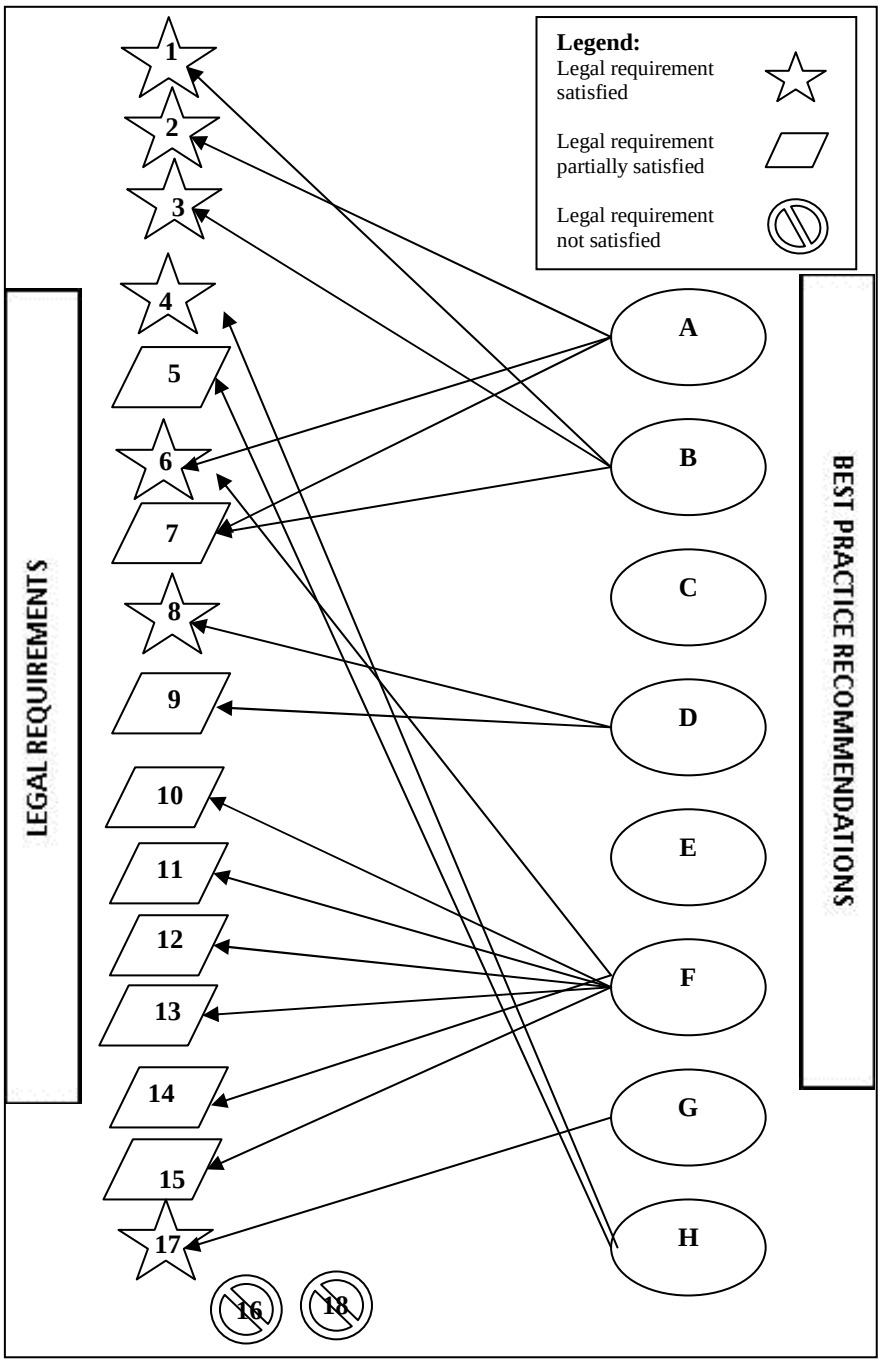

Figure 1: Comparison of legal requirements and best practice recommendations

According to the mapping in Figure 1, the following findings were identified. Each finding will be discussed:

Finding 1: The results show that the implementation of the selected best practice recommendations would fully satisfy only seven of the 18 legal requirements and partially satisfy the other nine. There are no other recommendations offered for two of the 18 legal requirements.

Finding 2: Compliance with legal requirements 1 to 4, 6, 8 and 17 may be achieved through the implementation of best practice recommendations.

Finding 3: Legal requirement number 5 is partially satisfied by the selected best practices. Selected best practices require a bank to demonstrate a stern stance on risk management, but do not explicitly require a bank to disclose incidents which would be material to the home users' decisions to continue making use of the online banking service.

Finding 4: Legal requirement number 7 is partially satisfied by the implementation of best practice recommendations. The selected best practice recommendations do not explicitly require banks to make security software available to home users of online banking, as required by legal requirement number 7. However, the selected best practices recommend that banks make home users of online banking aware of countermeasures they can implement and recommend that awareness materials reach all home users. Security software may be included in the awareness materials.

Finding 5: Legal requirement number 9 is only partially satisfied by the implementation of selected best practice recommendations. The recommendations do not state the need to update the content of the information security awareness programme to include new threats. However, the Standard of Good Practice for Information Security statement UE6.2.6 recommends that banks should review security incidents and use findings to update the next information security awareness programme aimed at home users of online banking. Such a review would reveal previously unidentified threats to home users of online banking.

Finding 6: Although the selected best practices recommend that banks make home users aware of how they can protect their personal information, legal requirements 10 to 15 suggest that best practices do not offer sufficient guidance on ensuring privacy of personal information. However, the Standard of Good Practice for Information Security section UE6.1 does address information privacy, recommending that banks develop and implement approved methods for handling personally identifiable information.

Finding 7: No matches for legal requirements numbers 16 and 18 suggest that the selected best practices do not stipulate the need for home users to be made aware of what their responsibilities are when protecting themselves.

It may, thus, be concluded that implementing the information security programme recommendations identified in the selected best practices does not result in compliance with the information security programme requirements identified in the selected legislation.

7 Conclusion

A large number of South African home users are becoming aware of and are able to use online banking, facing multiple information security threats while they do so. From a security perspective, the human element of the security chain must be addressed. South African banks need to protect their home users from the information security threats they face as online bankers, be able to demonstrate due care and due diligence when addressing these information security threats by implementing best practice, and must recognise and comply with the legal requirements imposed on them.

This research shows how to select relevant legal requirements and best practice recommendations; and, prompts a comparison of these to determine whether implementation of information security programme best practice recommendations results in compliance with information security programme legal requirements in South African banks when raising information security awareness amongst the home users of online banking. The research found that the implementation of the identified best practice recommendations does not result in compliance with the identified legal requirements, highlighting the importance of applying such a framework in a comprehensive fashion to understand the legal requirements imposed and ensure that adequate controls are in place with which to achieve compliance.

References

[Albrechtsen 2007] Albrechtsen, E.:"A qualitative study of users' views on information security"; Computers & Security, 26, 4 (2007), 276–289.

[British Standards Institution 2005] British Standards Institution; “Information technology – Security techniques – Information security management systems – Requirements”; BS ISO/IEC 27001, (2005), British Standards Publishing Limited.

[Business Security Information 2011] Business Security Information, 2011. Online banking risks. http://www.businessecurityinformation.com/2011/ (last access: January 2011).

[BusinessDictionary 2011] BusinessDictionary, http://www.businessdictionary.com/definition/best-practice.html (last access: Marach 2011).

[Choo 2011] Choo, K-K.R.: “The cyber threat landscape: Challenges and future research directions”; Computer & Security, 30, 8 (2011), 719-731.

[Da Veiga and Eloff 2010] Da Veiga, A., Eloff, J.H.P.: "A framework and assessment instrument for information security culture"; Computers & Security, 29, 2 (2010), 196–207.

[Davinson and Sillence 2010] Davinson, N., Sillence, E.; “It won’t happen to me: Promoting security behaviour among internet users”; Computers in Human Behaviour, 26, 6 (2010), 1739-1747.

[Gerber and Von Solms 2008] Gerber, M., Von Solms, R.: "Information security requirements: interpreting the legal aspects"; Computers & Security, 27, 5–6 (2008), 124–135.

[Investorwords 2011] Investorwords, http://www.investorwords.com/3420/online_banking.html (last access: July 2011).

[Kim and Park 2012] Kim, B.C., Park, Y.W.: “Security versus convenience? An experimental study of user misperceptions of wireless internet service quality”; Decision Support Systems. (2012). Article in Press.

[King Committee on Governance 2009] King Committee on Governance: “Code of Governance Principles for South Africa (King III)”; (2009). Institute of Directors in Southern Africa, South Africa.

[Methods & Tools QA Resources 2009] Methods & Tools QA Resources 2009, http://www.qaproject.org/methods/resglossary.html (last access: December 2010).

[Pezderka and Sinkovcs 2011] Pezderka, N., Sinkovics, R.R.: “A conceptualization of e-risk perceptions and implications for small firm active online internationalization”; International Business Review, 20, 4 (2011), 409-422.

[Reis et al. 2011] Reis, Z.A., Gulsecen, S., Byarakdar, B.: “To develop and Education System for Secure Internet Banking: GIBES”; Procedia Computer Science, 3 (2011), 1333-1340.

[Siponen 2001] Siponen, M.T.: "Five dimensions of information security awareness"; Computers and Society (ACM SIGCAS), 31, 2 (2001), 24-29.

[South Africa Internet Usage and Marketing Report 2009] South Africa Internet Usage and Marketing Report 2009, http://www.internetworldstats.com/af/za.htm (last access: July 2010).

[Von Solms and Von Solms 2004] Von Solms, B., Von Solms, R.: "The 10 deadly sins of information security management"; Computers & Security, 23, 5 (2004), 371–376.

[Wikipedia 2011] Best Practices, http://en.wikipedia.org/wiki/Best_practice (last access: July 2011).

[Williams 2008] Williams, P.A.H.: "In a 'trusting' environment, everyone is responsible for information security"; Information Security Technical Report, 13, 4 (2008), 207–215.

[Wilson and Nash 2003] Wilson, M., Nash, J.: “Building an Information Technology Security Awareness and Training Program”; NIST Special Publication 800-50 (2003), National Institute of Standards and Technology, USA.

[Wu et al. 2012] Wu, K-W., Huang, S.Y,. Yen D. Popova, I.: “The effect of online privacy policy on consumer privacy concern and trust”; Computers in Human Behaviour (2012). Article in press.