Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2012, vol. 17, no.2
(*http://www.arraydev.com/commerce/jibc/*)

A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information

Aaron M. French, PhD
Assistant Professor, Kyungpook National University, Daegu, South Korea
Postal Address: **1370 Sankyuk-dong, Buk-gu, Daegu 702-701, South Korea**
Author's Personal/Organizational Website:
Email: ***afrench@knu.ac.kr***

Aaron French is an Assistant Professor of MIS in the college of Business at Kyungpook National University in Daegu, South Korea. He received his Ph.D. in Business Information Systems at Mississippi State University. His research interests include eCommerce, social networking, cross-cultural studies and technology acceptance.

Abstract

While eBanking security continues to increase in sophistication to protect against threats, the usability of the eBanking decreases resulting in poor security behaviors by the users. The current research evaluates security risks and measures taken for eBanking solutions. A case study is presented describing how increased complexity decreases vulnerabilities online but increases vulnerabilities from internal threats and eBanking users.

Keywords: **ebanking; security; case study**

© Aaron M. French, 2012

INTRODUCTION

People use the Internet for various reasons such as shopping and online banking. One of the major concerns when purchasing online and accessing financial information is security. Information security is the protection of information and the systems used to store and transmit data (Dhillon and Backhouse, 2000). Companies go to great lengths to secure their customer's information and gain their trust. As technology continues to advance, security measures also continue to improve and become more sophisticated. While security continues to get stronger, some studies have argued that increased security could have negative effects on the usability of the system it's trying to protect (Braz and Robert, 2006; Yee, 2004). The question then becomes—who are you trying to secure this information from? Users already have reservations about eBanking with a minimum attitude towards its quality at best (Singh, 2011). When security measures are so sophisticated that users cannot access their own information, then security has gone too far.

The current study evaluates previous literature to establish a foundation of research in this area. A case study describing online banking security will be discussed to show the importance of information security in this sector. First, threats to information security will be identified by previously research. Then, security measures implemented to prevent these various threats from occurring will be discussed. Finally, an analysis of the identified threats and preventative measures will be presented to guide security analysts when determining effective levels of security measures.

ONLINE BANKING CASE STUDY

The current study will discuss two instances of user experiences with online banking as an example for discussion. Due to a strong need for security, online banking has increased security measures to include an access code, password, and several additional security questions required for access. Users of these online banking systems setup their account to access bank statements and conduct other banking activities. Two users discussed their experience with online banking giving insight into the level of security required to gain access.

Person A discussed their experiences with online banking. When setting up their account, person A had created a username, password, was assigned an access number and answered several security questions. The next day, person A attempted to access their account but was unable to remember their access number. Person A then called the bank to request information in order to gain access into their account. Due to person A's inability to remember all the information needed to access their account, person A wrote their login information on a piece of paper that was stored in a desk drawer. This action created a fatal security risk despite the efforts of the bank to secure their user's information. Due to many layers of security and various information required to gain access, many other users are likely to perform the same actions as person A causing risk to their information security.

A second instance of eBanking security was discussed by a user we shall identify as person B. Person B also was unable to remember their password after entering all of their information. After being unable to access their information, person B contacted the bank's help desk using the information provided on the website. Later that day, person B

received an email from the bank stating that they are unable to access password information due to encryption and bank security policies. Instead, the bank representative informed person B that his password was reset to the default password. The bank representative sent user B his default password and bank access number via an unencrypted email. While this allowed person B to gain access to his account, the bank representative also allowed for the possibility of a hacker to intercept that email and access person B's account.

The bank created several layers of security to prevent hackers from accessing customers information. However, these dramatic increases in security resulted in various other security threats. In the situation of person A, they were provided their access number by phone. This creates opportunities for social engineering by someone pretending to be person A or eavesdropping by someone listening in on person A's conversation. Person A's inability to remember all the information needed to access their account resulted in person A writing their bank information on a piece of paper that could easily be read by others. In the case of person B, the bank representative did not take proper measures to encrypt the user's information prior to emailing it. This resulted in the ability of hackers to potentially intercept the email and gain access to person B's account with little to no effort. Online banking systems put forth an abundant amount of effort to prevent hackers from accessing their customer information. When security becomes too complicated, they not only prevent hackers from accessing information but also customers who are performing legitimate activities. This leads to poor security habits by users negating all the security measures establishing by the organizations. The next section will describe security threats in more detail.

SECURITY THREATS

Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solutions and managerial actions (Gordon and Loeb, 2002). All commercial operating systems have vulnerabilities, also known as weaknesses in the computer system (Landwehr, 2001). These vulnerabilities create opportunities for possible threats to the information housed on these systems. Security threats can be classified into several categories from internal to external, human or non-human, and intentional or non-intentional (Loch, et al, 1992; Whitman, 2003). These threats can lead to the possibilities of disclosure, modification, destruction, or denial of use of that information.

There are various threats to information security that protectors of information must be aware of and account for. Table 1 lists many threats to information security but is not exhaustive of all possible threats that may exist.

Table 1: Security Threats

		Accidental	**Intentional**
Internal	**Human**	- Acts by employees - Accidental entry bad data - Accidental destruction of data by employees - Administrative Procedures - Weak/ineffective physical control	- Acts by employees - Intentionally destroy data by employee - Intentional entry of bad data by employees - Unauthorized access by employees
	Non-Human	- Mechanical and Electrical - Program problems	- Mechanical and Electrical - Program problems
External	**Human**	- Competitors - Media	- Hackers - Denial of Service Attacks - Social Engineering
	Non-Human	- Fire - Earth - Wind - Water	- Computer Virus - Worms - Trojan - Spyware

Research has shown that more than two thirds of all Americans view external threats, such as hackers and cyber criminals, as a higher risk to security than internal threats (McCrohan, 2003). Furthermore, it was reported that between 50 and 75 percent of all security related incidents originate from within the organization (D'Arcy et al, 2009). Companies often emphasize the need for security measures concerning external threat over internal threats despite previous research showing internal threats to be a higher risk (Dinnie, 1999). The first category of threats discussed is related to internal threats, which involve human and non-human threats that can be either accidental or intentional.

Internal threats can stem from three areas: the application development department, the infrastructure, and the data center (Hyle, 2006). Despite the risk of internal threats, it is highly believed that threats from employees are largely unintentional (Keller et al., 2005). Threats stemming from the application development department could result from logical errors in the applications developed by the programming team. An application that is not programmed correctly could potentially cause vulnerabilities in the security mechanisms allowing unauthorized individuals to access private information. A programmer could also intentionally access data for personal gain or malicious purposes. An organization's infrastructure possesses significant security implications by determining access level and privileges granted to employees. Granting access to information that is unrelated to an employee's job functions increases the probably of a user compromising the data either intentionally or unintentionally. Data centers present a large threat to the security of information because users enter, delete, and maintain important company data.

These threats include both negligence and deliberate acts by the users that encompass behaviors such as (Leach, 2003):

- A lack of security common sense
- Not applying security procedures
- Taking inappropriate risks
- Deliberate acts of negligence
- Deliberate attacks

Managers often address these issues through security awareness and training. However, being aware of security policies and procedures does not always result in employees following them. Some people respond positively with cooperation and acceptance of policies and procedures while others respond negatively with repulsiveness and resistance (Siponen and Kajava, 1998). Security incidents suffered by a company can be significantly attributed to poor or unacceptable behavior by its users (Leach, 2003). Therefore, security audits should frequently be performed to ensure employees are following proper procedures.

While successful external threats are not as common as internal threats, they do pose a significantly different challenge. External threats may include hackers, viruses, denial of service attacks and even natural disasters. While the risk of natural disasters might seem minimal, security measures must still be accounted for. In the unlikely event that a natural disaster was to occur, the organization would need to have procedures in place to recover any lost data. Backup and storage is one preventative measure for handling these types of situations. Accidental leaks of corporate information are another risk that could result in bad publicity through the news media or other outlets damaging the reputation of the company. An even more prevalent threat to information security, which typically gets the most attention, is the threats of hackers and computer viruses. These are intentional acts to compromise the security of information systems in malicious ways. The first step towards securing and organizations information is identifying the possible threats. Once a threat analysis has been completed the organization can then set its goal to developing countermeasures against these threats. Countermeasures are functions or features that reduce or eliminate vulnerabilities in the system (Oppliger, 2003).

The next section discusses these counter measures and gives more information about security practices that are taken to ensure the confidentiality, integrity, and availability of an organization's information.

SECURITY MEASURES

A variety of security threats were discussed in the previous section that could compromise the security of information. Many threats can be minimized or prevented through various procedures. For instance, the threat of user errors could be minimized with validation procedures upon data entry and increased training for information users. While some threats are a result of user error, other threats may occur for malicious purposes. For malicious threats to occur there has to be motivation and the capability for the threat agent to carry out the threat, which are modified by access, catalysts, inhibitors, and amplifiers (Kovacich, 2003). Motivations for malicious attacks stem from various reasons such as personal gain, political, religious, curiosity, revenge, and so on. Motivation alone is not enough for a threat to occur; the threat agent must also have the

capability to perform the act.

Capabilities that could enable a threat agent to perform a malicious act might include personality, access to facilities, software, technology, and education. Inhibitors can be implemented to reduce motivations in order to deter a threat agent from performing malicious acts. Inhibitors may consist of increasing security, resulting in higher capabilities required to perform malicious acts, or more severe consequences for improper use or harm to corporate data. While inhibitors are put in place to deter malicious acts, amplifiers may exist that could increase the likelihood of threat agents to perform these acts. Amplifiers may include peer pressure, fame, easy access to information, and increased skill and educational levels which result in higher capabilities.

Organizations must take preventative measures to protect their sensitive corporate information. This includes information about the company's strategy, financial information, customer information, or any other information that could be damaging to the company and its reputation. It was reported that information security management is currently the top technology initiative among organizations and has been since 2002 (Barlas et al, 2007). As discussed earlier, security threats can be internal or external, human or non-human, accidental or intentional (Loch, et al, 1992). Oppliger (2003) operationalized security into five aspects:

- Security Policy
- Host Security
- Network Security
- Organizational Security
- Legal Security

While each aspects of security must be addressed individually, they must collectively work together to provide security and manage vulnerabilities to corporate information. Each of these operationalizations of security will be described next.

Security Policy

Policies govern behaviors serving as a guide in the decision-making process when using a system (Sloman, 1994). They tell the users of these systems what activities are acceptable and what activities are not. When evaluating security policies and procedures, there are two aspects that companies typically follow: descriptive and prescriptive. The descriptive aspect involves making employees aware of the policies and procedures while the prescriptive aspect requires employees to internalize and follow the security guidelines (Siponen and Kajava, 1998). Security policies are the governing ideas that get integrated into host security, network security, and organizational security. Security policies set the rules that must be followed for host and network security. Then it's up to the organization to train users and make them aware of the policies and procedures.

Host Security

Host security includes the authentication of users, effective control and access to system resources, securely storing data, and audit trial of the information being access (Oppliger, 2003). Authentication procedures are typically divided into two stages: Identification and authentication of users (Adams and Sasse, 1999).

There different types of authentication that have been developed for authenticating users: knowledge based systems, token-based systems, and systems based on biometrics (Dhamija and Perrig, 2000). Typical user identification and authentication requires the user to enter a username and password to gain access to the system. This provides security by not allowing anybody to randomly access the system. However, several vulnerabilities exist that can be exploited using a single user name and password. Fegghi et al (1999) identified a number of threats to using reusable passwords:

- Guessing
- Social engineering
- Eavesdropping
- Capture and replay
- Penetration
- Brute force
- Point of entry
- Revealing secret

Research has shown that more than 85 percent of passwords used can be broken through the use of a dictionary or a simple exhaustive search of short passwords (Braz and Robert, 2006; Morris and Thompson, 1979). One possible solution to several of these threats includes having a password policy where users must create strong passwords and change them often. This decreases several threats previously identified such as guessing, capture and replay, and brute force. However, it often leads to poor security habits by users, such as a user not being able to remember their password and having to write it down on a piece of paper that easily be obtained by unauthorized individuals (Adams and Sasse, 1999).

One method that has been created to overcome the difficulties of remembering passwords is Hash Visualization (Perrig and Song, 1999). Hash Visualization is where a user has various pictures in their portfolio and upon logging in they must identify their portfolio pictures among a series of pictures displayed. The idea is that users can remember visual images much easier than strong passwords, avoiding the need for users to write them down. While various security techniques have been developed in recent years, the main goal is to create a secure way for users to access the system while limiting the vulnerabilities to the system.

Network Security

Network security is highly integrated with other operationalizations of security such as security policies, host security, organizational security and legal security. Security policies must be put in place to govern user activity and take preventative measures for security on networks. Host security, as previously described, includes authentication of users who access the networks. Network security is integrated in the technical, organizational, and legal security measures that must be designed and implemented (Oppliger, 2007). Network security may include passwords, authentication, firewalls and proxy servers among other things.

Newhouse (2007) discusses six resolutions to creating a secured network:

- Change Passwords Quarterly
- Download Patches and Updates
- Hire a hacker
- Monthly Risk Assessments
- Communicate and Review Data Security Policy
- Keep Network Virus Free

The use of strong passwords and requiring users to regularly change their password will create a higher level of security on the network. However, there are limitations to strong passwords as previously discuss, such as users inability to remember and improper handling of security by the users. Downloading patches and updates for operating systems and networks is another action that could be taken to increase security on the network. This ensures that the latest security threats and vulnerabilities are accounted for as they are discovered. However, no system is completely hack proof. One recommendation is to hire a hacker as part of the network security team. Hackers typically use creative techniques to infiltrate a system. Therefore, hiring a proven hacker could offset other hackers as they try to exploit vulnerabilities not previous accounted for. As hackers become more sophisticated, tools such as firewalls become less sufficient on their own. Using additional tools such as intrusion detection software can help prevent access from unauthorized individuals and increase security (Green, et al, 2007). Anti-virus software and other tools should be used and kept up to date in order to prevent the spreading of viruses across the network. While these tools help limit the potential threats to information security, rarely are security issues solved with products and services alone. Incorporating these methods with the other aspects of security will significantly decrease the likelihood of falling victim to security threats (Oppliger, 2007).

However, organizations must continuously review the security policy and communicating them to the organization. This will ensure that proper procedures take place and employees are aware of what these procedures are.

Organizational Security

The biggest threats to security are the users. Hackers often try to exploit users through tactics known as social engineering (Winkler and Dealy, 1995). It is the organization's responsibility to educate employees about vulnerabilities and make them aware of proper procedures to protect the organization's information (D'Arcy and Hovav, 2007; Hong et al, 2007). The primary way to accomplish this is for the organization to train users and make them aware of policies, procedures, and vulnerabilities to information and security. Security awareness training is identified as the weakest link in information security. Siponen (2001) identifies five dimensions of security awareness:

- Organizational
- General Public
- Socio-Political
- Computer Ethical
- Institutional Education

The organizational dimension consists of various groups of people within the organization that security awareness training should target. The general public dimension entails all users outside of the IT department. The social-political dimension is the security awareness training that is required by law. The Computer ethical dimension is the prevention of activities that are interpreted as abuse. The institutional dimension describes what information should be included in a security awareness program. Desman (2003) describes user awareness training as a people issue rather than a technical issue where training should be formalized. Without proper knowledge of procedures and awareness of security vulnerabilities, users will not be able to protect against potential threats.

Legal Security

Legal security consists of legal actions to be taken against an attacker with the possibility of prosecution (Oppliger, 2003). It is important to have consequences in place to deter potential threat agents from compromising the organization's information. These consequences act as inhibitors decreasing the motivation of threat agents to violate security procedures. Legal security should be embedded within the security policy that is implemented within organizational. All agents associated with the organization should be made aware of security policies and consequences. Each of the five aspects of security provides different means of securing information. They must all be addressed and used together to decrease the vulnerabilities of security threats. Table 2 lists security measures (Keller et al., 2005; Landwehr, 2001; Loch, et al, 1992) that have been identified in association with the different categories of security.

Table 2: Security Methods

		Accidental	**Intentional**
Internal	**Human**	- Policies and Procedures - Security Awareness Training - Employee education - Ethics training	- Policies and Procedures - Audit procedures strengthened - Monitor computer usage - Reporting violations encouraged - Ethics training
	Non-Human	- Update Software	- Company provided software only
External	**Human**	- Security Awareness Training - No outside BBS connections	- Use of passwords - Encryption - Authentication (images, text, etc.) - Security questions - Auto terminal/account logoff - Install and Properly Configure a Firewall

	Non-Human	- Backup procedures schedules - Implement Physical Security Measures - Backup Power Supply	- Authentication (images, text, etc.) - Use of virus scanning software - Protect against Viruses, Worms, and Trojans

As shown in table 2, the majority of technical solutions for information security are directed at external human threats. While internal threats have proved to be the biggest threat for security, external threats are the most recognized by the general population. It is important for organizations to protect their information from all viable threats. However, organizations should also take in consideration how increased security could inhibit their users from taking proper measures to secure themselves. The following section will revisit the case study of online banking and discuss the implemented security procedures followed by an analysis of information security.

ONLINE BANKS AND SECURITY

Online banks have invested heavily to make efforts in securing the financial information of their customers. Many online banks throughout the United States have implemented a five-step approach for online banking access in efforts to protect against external threats. Figure 1 outlines the steps required for customers to access their bank accounts online.

In the first step, the user must enter the access ID for their account that is provided by the bank. The immediate problem associated with this access number is the length of the number and lack of relevance to the user. If the user is unable to remember this access ID easily, then they are likely to write their login information on a piece of paper as person A did in the case previously discussed. This creates poor security habits on the part of the user and leaves the opportunity for someone to steal the paper containing their login information. Users may also be vulnerable to social engineering by home service technicians or others who may try to gain access to areas where password information may be stored.

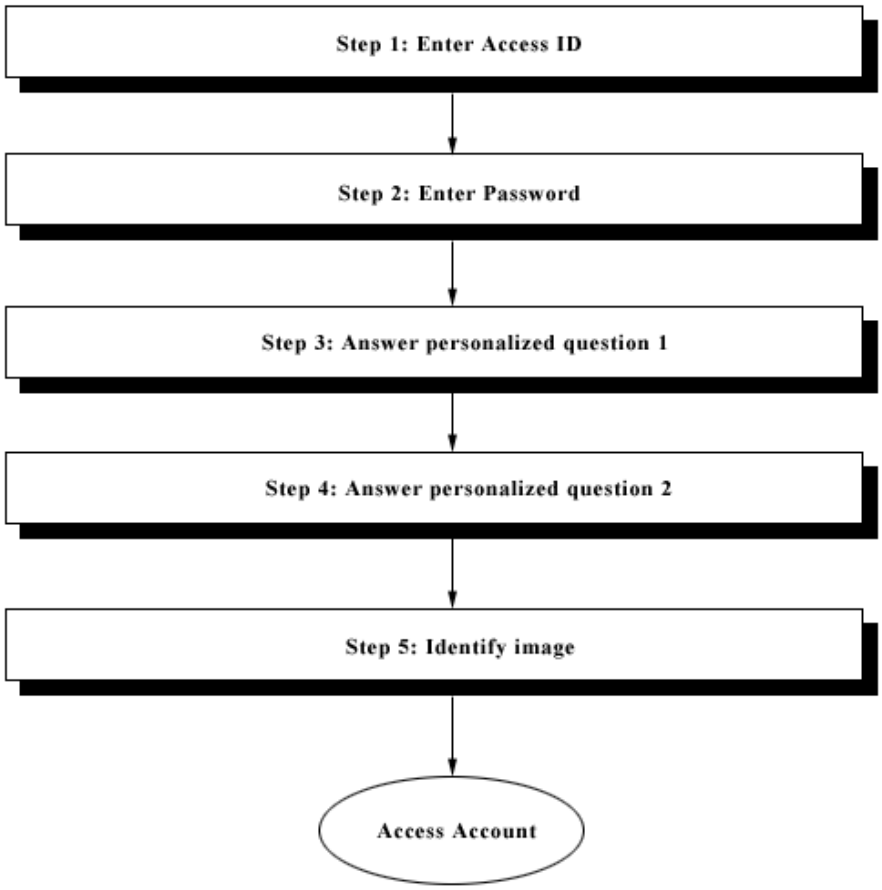
Step 2 requires the user to enter a password to gain access to their account. A password alone is vulnerable to several security issues that were discussed above. By implementing a password with other security measures, as seen in the banking example, several vulnerabilities can be decreased compared to the use of passwords alone. However, in the instance that a user forgets their password, as was the case of person B in the case presented above, there should be procedures in place to help the user recover the password or reset it to a default without allowing unauthorized individuals aware of this situation. In the case described above, the security threat could have been eliminated through proper training and the use of an encrypted email to contact the user with their account information.

Steps 3 and 4 ask the user to answer security questions that were previously answered by the user. A list of common security questions used includes:

- What is your mother's maiden name?

- What is the name of your favorite restaurant?
- Who is your favorite actor?
- What is your favorite color?
- What is the name of your first pet?

Figure 1: Online bank's five step approach to security



While these questions add additional security, they are also subject to vulnerabilities from people who know the user intimately or from others engaging in social engineering. Creating questions that are too complicated might result in the user not remembering the answers and leave them unable to access their account. In this situation, the user would likely revert to writing their answers on a piece of paper along with their access ID. Once again, displaying poor security habits as demonstrated in the case of person A.

The last step, step 5, is where the user identifies a picture that they have previously marked and labeled. This uses a form of hash visualization that was described previously in this article.

This five-step approach creates a very secure environment protecting against external threat agents but can significantly decrease usability among the users of the system. In

the case describe above, both user A and user B chose to decease using online banking due to concerns about security. While the increase of security measures may protect information from threats, it may also hinder the user's ability to access their account information causing inconvenience and decreasing the user's perception of usefulness of the system (Ting et al, 2005). While online banks take measures to protect against external threats, they should also be aware of internal threats. If users are forced to call the help desk to request information about their account then they are requiring internal staff to access their information creating an opportunity for mismanagement. If internal threats are not addressed then the advantages gained from increased security protecting against external threats will be offset by the increased vulnerabilities of internal threats. In addition, as a user's ability to access their information because more complicated, their ability to protect themselves will decrease.

CONCLUSION

Various threats and countermeasures for protecting against those threats were evaluated. A case study was presenting discussing two users and their difficulties with complicated eBanking security procedures. It has been shown that organizations, online banking in particular, are spending the majority of their efforts on external security without properly assessing the importance of internal security. With internal security being of a higher risk than external security, these additional security measures give users a false sense of security.

This study addresses the need for increased awareness of internal threats through security measures such as security awareness, policies, practices, and procedures. Online banks and other organizations should evaluate every aspect of security while taking into account the needs of the user. Technology should be an added convenience to the customer and not prohibit them from accessing their information. While security is important, organizations should balance the need for increased security with the desire to make systems easy to use and useful to the consumer.

REFERENCES

Adams, A. and Sasse, M. (1999). Users are not the enemy, in Association for Computing Machinery. *Communications of the ACM*, 42 (12), 40-46.

Barlas, S., Queen, R., Radowitz, R., Shillam, P. and Williams, K. (2007). Top 10 Technology Concerns. *Strategic Finance*, 88 (10), 21-23.

Braz, C. and Robert, J. (2006). Security and Usability: The Case of the User Authentication Methods. *In Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine*, Montréal, Québec.

D'Arcy, J. and Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM*, 50 (10), 113-117.

D'Arcy, J., Hovav, A. and Galleta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20 (1), 79-98.

Desman, M. (2003). The Ten Commandments of Information Security Awareness Training. *Security Management Practices*, 11 (6), 39-44.

Dhamija, R. and Perrig, A. (2000). Deja Vu: A User Study Using Images for Authentication. *Proceedings of the Ninth USENIX UNIX Security Symposium*, Berkeley, CA, USA.

Dhillon, G. and Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, 43 (7), 125-128.

Dinnie, G. (1999). The Second Annual Global Information Security Survey. *Information Management and Computer Security*, 7 (3), 112-120.

Feghhi, J., Feghhi, J. and Williams, P. (1999). *Digital Certificates: Applied Internet Security*. Massachusetts: Addison Wesley Longman Inc.

Gordon, L. and Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5 (4), 438–457.

Green, I., Raz, T. and Zviran, M. (2007). Analysis Of Active Intrusion Prevention Data For Predicting Hostile Activity In Computer Networks. *Communications of the ACM*, 50 (4), 63-68.

Hong, K., Chi, Y., Chao, L. and Tang, J. (2007). An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan. *Information Management and Computer Security*, 14 (2), 104-115.

Hyle, R. (2006). The Oops Factor. *TechDecisions*, 8 (4), 20-24.

Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management*, 22 (2), 7-19.

Kovacich, G. (2003). *Information Systems Security Officer's Guide*. 2nd ed., Burlington: Elsevier Science.

Landwehr, C. (2001). Computer security. *International Journal of Information Security*, 1 (1), 11.

Leach, J. (2003). Improving User Security Behaviour. *Computers and Security*, 22 (8), 685-692.

Loch, K., Carr, H. and Warkentin, M. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, 17 (2), 173-186.

McCrohan, K. (2003). Facing the Threats to Electronic Commerce. *Journal of Business and Industrial Marketing*, 18 (2), 133-145.

Morris, R. and Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM*, 22 (11), 594-597.

Newhouse, K. (2007). Six Security Resolutions. *Credit Union Magazine*, 73 (2), 52.

Oppliger, R. (2003). *Security Technologies for the World Wide Web*. 2nd ed. Boston: Artech House.

Oppliger, R. (2007). IT Security: In Search of the Holy Grail. *Communications of the ACM*, 50 (2), 96-98.

Perrig, A. and Song, D. (1999). Hash visualization: A new technique to improve real-world security. *In Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*..

Singh, K. (2011). Innovated Technology in Banking Services. *Journal of Internet Banking and Commerce*, 16 (2), 1-15.

Siponen, M. (2001). Five Dimensions of Information Security Awareness. *Computers and Society*, 31 (2), 24-29.

Siponen, M. and Kajava, J. (1998). Ontology of Organizational IT Security Awareness - From Theoretical Foundations to Practical Framework. *In Proceedings of the Seventh IEEE Workshop on Infrastructure for Collaborative Enterprises*, 327-331.

Sloman, M. (1994). Policy Driven Management for Distributed Systems. *Journal of Network and Systems Management*, 2 (4), 333-360.

Ting, C., Woon, I. and Kankanhalli, A. (2005). Impact of Security Measures on the Usefulness of Knowledge Management Systems. *In Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, Bangkok, Thailand.

Whitman, M. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46 (8), 91-95.

Winkler, I. and Dealy, B. (1995). Information Security Technology?...Don't Rely on It. A Case Study in Social Engineering. *Proceedings of the Fifth USENIX UNIX Security Symposium*, Salt Lake City, Utah, 1–6.

Yee, K. (2004). Aligning Security and Usability. *Security and Privacy*, 2 (5), 48-55.