Macrothink Institute™

Business Management and Strategy
ISSN 2157-6068
2010, Vol. 1, No. 1: E1

Identifying and Managing Enterprise Security Risks in Online Business Convergence Environments

John Mylonakis
10 Nikiforou str., Glyfada, 166 75, Athens, Greece
E-mail: imylonakis@vodafone.net.gr

Alketas Malioukis
28 Ithakis str., Pallini, 153 44, Athens, Greece
E-mail: alketas_1@hotmail.com

Abstract

Security risks associated with networked enterprise systems is a topic that has become increasingly significant in recent years. Risks to computer systems can be anything from defacing a corporate website to sabotaging a metropolitan electricity distribution system, and anything in between. Information security risk management is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. The scope of this paper is to review the current literature and best practices on risk management and the processes that allow Information Technology (IT) managers to balance the operational and economic costs of protective measures, as well as, achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. Literature suggests that developing a well-planned business continuity plan should be a matter of highest priority for all businesses, regardless of size, structure or function. For business leaders, the most crucial priority is to minimize risk by developing a high standard security system, encompassing the overall organization's safety.

Keywords: Information systems**,** Electronic commerce, Security risks, Enterprise systems, Online channels

1. Introduction

The Internet has played a key role in changing how we interact with other people and how we do business today. Because of the internet, electronic commerce has emerged, allowing organizations to more effectively interact with their customers and other corporations inside and outside their industries. While the internet offers enormous advantages and opportunities, it also presents various securities risks.

Managing the security risks associated with organization's growing reliance on information technology is a continuing challenge. In particular, public agencies, like many private organizations, have struggled to find efficient ways to ensure that they fully understand the information security risks affecting their operations and implement appropriate controls to mitigate these risks.

Organizations are increasingly reliant on automated and interconnected systems to perform functions essential to their welfare. The benefits of such activities include improved information processing, communication and better service of the customer (Marquis, Dean & Knight, 2006). However, the factors that benefit operations - speed of processing and access to information - also increase the risks of computer intrusion, fraud, and disruption.

Information systems have long been at some risk from malicious actions or inadvertent user errors and from natural and manmade disasters. In recent years, (Robinson, 2006) systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are becoming more widely known via the Internet and other media.

Numerous reports published over the last few years indicate that automated operations and electronic data are inadequately protected against these risks (Hiltgen, Kramp & Weigold, 2006). These reports show that poor security program management is one of the major underlying problems. A principal challenge many agencies face is in identifying and ranking the information security risks to their operations, which is the first step in developing and managing an effective security program. Taking this step helps ensure that organizations identify the most

significant risks and determines what actions are appropriate to mitigate them.

2. What is electronic security (e-security)?

E-security touches the very heart of the new economy. For the first time since World War II, global markets and the global community can promise significant benefits to all. But the process of building a global electronic economy demands discussion of important issues, such as how to define and protect privacy, what trust and confidence will mean and how to measure them, and how to determine security.

Overall, electronic security is any tool, technique, or process used to protect a system's information assets. Electronic security enhances or adds value to a naked network and is composed of soft and hard infrastructure. The soft infrastructure components are the policies, processes, protocols, and guidelines that protect the system and the data from compromise. The hard infrastructure consists of hardware and software needed to protect the system and data from threats to security from inside or outside the organization (Bishop, 2005). The degree of electronic security used for any activity should be proportional to the activity's underlying value. Security is a risk management, or risk-mitigation, tool. Appropriate security means that the risk has been mitigated for the underlying transaction in proportion to its value. Given that the Internet is a broadcasting medium, constraints have to be added to target only intended recipients. As a result, the need for security is a constant of doing business over the Internet (Chen & Corriveau, 2007).

E-security can be described on the one hand as those policies, guidelines, processes, and actions needed to enable electronic transactions to be carried out with a minimum risk of breach, intrusion, or theft (Wysopal, Nelson, Zovi & Dustin, 2007). On the other hand, e-security is any tool, technique, or process used to protect a system's information assets. Information is a valuable strategic asset that must be managed and protected accordingly. The degree of e-security used for any activity should be proportional to the activity's underlying value. Thus, security is a risk-management or risk-mitigation tool, and appropriate security means mitigation of the risk for the underlying transaction is in proportion to its value.

3. Security Risks on Enterprise Network Systems

Security risks associated with networked enterprise systems is a topic that has become increasingly significant in recent years. As corporations rely ever more on technology to run their businesses, connecting enterprise systems to each other to perform seamless business transactions in a virtually borderless world, security is becoming a concern rather than an afterthought for IS managers around the world.

Lewis (2000) describes the importance of linking security issues to business issues. He points out that lack of security can decrease revenue due to loss of confidence by the market. According to Lewis, too much security can also lower revenue by obstructing access and creating obstacles for customers. He suggests that the trick is to provide the right balance of strong security measures that the right people access the right information at the right time.

Risks to computer systems can be anything from defacing a corporate website to sabotaging a metropolitan electricity distribution system, and anything in between. Each of these risks is associated with business risks. Freeh (2000) observes that an intrusion that results in a theft of credit card numbers from an online vendor can result in significant financial losses and reduce customer willingness to engage in business (Tipton & Krause, 2008). In addition, having to shutdown a defaced e-commerce site can have disastrous consequences for a business.

Apart from the most obvious financial risks, many experts believe that security is all about managing risks. The level of security that needs to be put in can be treated as an indication of the level of risk that a business is willing to accept (Lewis, 2000). Lewis suggests that one should be looking at security systems as a way to conduct risk management. To do that, the risks are to be quantified first, then to determine the liability, and finally take remedial actions. The remedial actions could involve imposing appropriate security measures.

4. The Importance of Information Security Risk Management

It would be prohibitively expensive and impractical to protect the enterprise against every vulnerability because information security attacks come in many forms, and attackers constantly evolve new tactics as we develop new defenses and controls. We need a way to identify the most likely attack vectors to support the development of optimal security strategies.

Information security risk management is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. In its simplest form, a risk management assessment consists of the identification and valuation of assets and an analysis of those assets in relation to

potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks (Brancheau, Janz & Wetherbe, 1996).

An adequate risk management assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities (Fink, 2005). A risk management assessment is a pre-requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk management assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program.

Early information security efforts in the IT industry concentrated on specific controls such as firewalls, virus scans, authentication and logon credentials, intrusion detection and prevention packages, and cryptography (Bellissimo, Burgess & Fu, 2006). These are important controls but are not easily sustainable as they rely on closing all emerging vulnerabilities. As the number of new vulnerabilities discovered each year has skyrocketed, this model of "fixing everything" becomes more costly while losing effectiveness, as soon as one hole is patched, two new holes appear. The information security industry has been searching for a rational method to narrow threats in a practical manner that can be applied to strategy, tactics, prioritization, and resource management.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed, it pervades decision-making in all areas of our daily lives. Take the case of home security, for example (Pritsker, 1997). Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need. The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission (Hertzum, Jørgense & Nørgaar, 2004). These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

5. Which are the security systems objectives?

Information security enables an organization to meet its business objectives by implementing business systems with due consideration of information technology (IT) - related risks to the organization business (Whittacker & Thompson, 2008) and trading partners, technology service providers, and customers. Organizations meet this goal by striving to accomplish the following:

5.1 Availability. The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.

5.2 Integrity of Data or Systems. System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

5.3 Confidentiality of Data or Systems. Confidentiality covers the processes, policies, and controls employed to protect information of customers and the organization against unauthorized access or use.

5.4 Accountability. Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

5.5 Assurance. Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

6. When does a security issue become a risk?

Technically, risk is the probability associated with losses or (failure) of a system multiplied by the euro loss if the risk is realized. By this definition, it is evident that risks are subjective. It is up to the management to assess risks

and to classify them based on their severity. The economic aspect of managing risks also plays a role in it, because, sometimes the benefits from mitigating a risk may not justify the costs involved. At the same time, chances of occurrence of some risks may be less than the others.

The following are the components for the design of information security architectures, which are particularly relevant to the case being investigated in this project:

6.1 Intrusion. Ensuring that access to systems and information can only be gained though authorized access methods.

6.2 Authentication. Ensuring that only authorized personnel are able to access the systems and information.

6.3 Authorization. Ensuring that access to systems and information is restricted to those with an authorized requirement for such access.

6.4 Encryption. Protecting information in transit and in storage through the use of : encryption.

6.5 Accountability. Ensuring that access to systems and information by users is appropriately recorded.

6.6 Availability. Ensuring that systems and information are available to authorized users whenever required.

6.7 Endurability. Ensuring that security risks are maintained at acceptable levels over time.

It is widely accepted that countermeasures or strategies adopted to reduce security risks, fall into four categories of sequential actions, namely: (1) deterrence, (2) prevention, (3) detection, and (4) recovery.

7. Top 10 security risks

Typical dangers faced are third parties accessing, deleting or tampering with the data while it is being transmitted or obtaining information under false pretences. This may achieved with the help of:

7. 1 Viruses and worms: Programs that self-replicate or are sent over the internet by email and can damage your PC .Viruses are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in. Worms, on the other hand, are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to others. The computer worm is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses (Blascovich, 2008).

7.2 Trojans: Programs that, unbeknown to the user, compromise computer security by intercepting passwords, for example, ‘A Trojan is a program that may appear to be legitimate, but in fact does something malicious’. Trojans are often used to gain backdoor access - that is to say remote, surreptitious access, to a user's system. Trojans do not replicate as viruses do, nor make copies of themselves as worms do.

7.3 Phishing: Is the process of using a false name, website or address for fraudulent purposes (Dhamija, Tygar & Hearst, 2006).

7.4 Pharming: Redirecting users to a fraudulent server.

7.5 Rootkits: Malicious software giving unauthorized administrator-level access without the real administrator noticing, they share certain features with Trojans. A rootkit gives attackers full access to the system (hence the term 'root') and typically hides the files, folders, registry edits, and other components it uses. In addition to hiding itself, a rootkit typically hides other malicious files that it may be bundled with.

7.6 Hacking: Unauthorized access to a pc via the internet is the act of gaining access without legal authorization to a computer or computer network.

7.7 Keyloggers: Is one of the most insidious threats to a user’s personal information. Passwords, credit card numbers, PII etc. are potentially exposed, and the incidence of keyloggers in-the-wild is apparently growing rapidly. Unlike Phishing, this is not an attack that alert and sophisticated users can avoid. Writing a keylogger is a trivially easy task. There are numerous freeware offerings, and many of them make efforts to conceal their presence. For example, they will not show up in the Task Manager process list.

7.8 Botnets: A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are

home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet.

7.9 Online payment Fraud: Payment fraud is fraud or theft committed using online technology to illegally remove money from, or transfer it to, a different bank account. Types of internet banking fraud include phishing and mule recruitment.

7.10 Data loss: The issue of data loss encompasses everything from confidential information about one customer being exposed, to thousands of source code files for a company's product being sent to a competitor. Whether deliberate or accidental, data loss occurs any time employees, consultants, or other insiders release sensitive data about customers, finances, intellectual property, or other confidential information (in violation of company policies and regulatory requirements). Moreover, data loss could be caused by hardware fail outs during operations.

8. Best Solutions for Mitigating Risks

8.1 Protect information/systems/networks from damage by viruses, spyware, and other malicious code.

Install, use (in "real-time" mode, if available), and keep regularly updated anti-virus and anti-spyware software on every computer used. This will protect the organization and users from various risks as worms, viruses and other malicious software.

8.2 Provide security for your Internet connection.

Nowadays all of us have broadband (high speed) access to the Internet. Therefore, computers or any network our computer is attached to, is exposed to threats from the Internet on a 24 hour a day/7 day a week basis.

For broadband Internet access, it is critical to install and keep operational a hardware firewall between your internal network and the Internet. This may be a function of a wireless access point/router or may be a function of a router provided by the Internet Service Provider (ISP). There are many hardware vendors which provide firewall wireless access points/routers, firewall routers, and firewalls.

8.3 Install and activate software firewalls on all your business systems.

Install, use, and keep updated a software firewall on each computer system used in our organization. If you use the Microsoft Windows operating system, it probably has a firewall included. You have to ensure that the firewall is operating, but it should be available.

It is necessary to have software firewalls on each computer even if we have a hardware firewall protecting our network. If our hardware firewall is compromised by a hacker or by malicious code of some kind, we do not want the intruder or malicious program to have unlimited access to our computers and the information on those computers (Zviran & Haga, 2009).

8.4 Patch your operating systems and applications.

All operating system vendors provide patches and updates to their products to correct security problems and to improve functionality.

8.5 Make backup/recovery copies of important business data/information.

It is highly recommended to back up our data on each computer used. Our data includes (but is not limited to) word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, and other information used in or generated by your business.

It is necessary to back up our data because computers die, hard disks fail, employees make mistakes, and malicious programs can destroy data on computers. Without data backups, you can easily get into a situation where you have to recreate your business data from paper copies and other manual files

It is important to make a full backup once a month and store it away from our office location in a protected place. If something happens to our office (fire, flood, tornado, theft, etc) then our data is safe in another location and we can restore our business operations using our backup data and replacement computers and other necessary hardware and software.

8.6 Control physical access to computers and network components

We must not allow unauthorized persons to have physical access to or to use of any of our business computers. This includes locking up laptops when they are not in use. It is a good idea to position each computer's display so that people walking by cannot see the information on the screen.

8.7 Secure wireless access point and networks

If we use wireless networking, it is a good idea to set the wireless access point so that it does not broadcast its Service Set Identifier (SSID). In addition, it is critical to change the default administrative password. It is important to use strong encryption so that our data being transmitted between our computers and the wireless access point cannot be easily intercepted and read by electronic eavesdroppers.

8.8 Train employees in basic security principles

Employees who use any computer programs containing sensitive information should be told about that information and must be taught how to properly use and protect that information. On the first day that our new employees start work, they need to be taught what our information security policies are and what they are expected to do to protect our sensitive business information. They need to be taught what our policies require for their use of our computers, networks, and Internet connections.

8.9 Require individual user accounts for each employee on business computers and for business applications

We must set up a separate account for each individual and require that good passwords be used for each account. Good passwords consist of a random sequence of letters, numbers, and special characters – and are at least 8 to 10 characters long.

To better protect systems and information, ensure that all employees use computer accounts which do not have administrative privileges. This will stop any attempt – automated or not – by employees to install unauthorized software.

Passwords which stay the same, will, over time, be shared and become common knowledge to an individual user's coworkers. Therefore, passwords should be changed at least every 3 months.

8.10 Limit employee access to data and information, and limit authority to install software

We must use good business practices to protect your information. We must not provide access to all data to any employee. We must not provide access to all systems (financial, personnel, inventory, manufacturing, etc) to any employee. For all employees, we must provide access to only those systems and only to the specific information that they need to do their jobs.

To better protect systems and information, we must ensure that all employees use computer accounts which do not have administrative privileges. This will stop any attempt – automated or not – by employees to install unauthorized software.

8.11 Use authentication methods

There are a variety of technologies and methodologies organizations can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others (Gaw & Felten, 2009). The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the organization's risk assessment process.

8.12 Safety with online credit card payment

When a citizen enters his credit card details it must be cryptographically secured transmitted to the card issuer. If the card number would not be encrypted a network technician could find the number in a server log file and use it for his own shopping. The 128-bit encryption method is considered to be safe unless you are dealing with the CIA. **A secure transaction** can be recognized by a yellow key or lock symbol  in the lower status bar of a web browser and the http**s** in the address bar. However, the MS Internet-Explorer does not show a lock symbol if the webpage has mixed content or layers. Reasonably customer data is encrypted while images like item photographs can be Cleary transmitted. A missing lock symbol can also still mean that the shop is safe. There are several mechanisms that secure safe payment transactions like **3D-Secure**: VISA and MasterCard offer with "Verified by VISA" and "MasterCard SecureCode" an additional security check with a submitted question that can only be answered by the legal card owner. The enquiry comes directly from the card processor and cannot be monitored by the shop owner. Using a contract for 3D-Secure will get a guaranty for all payments that there is no reversal debit (Smith, Milberg & Burke, 2009).

8.13 Loss of Physical Facilities, Trunks and Lines

Complete loss of Internet routing infrastructure is unlikely due to the intentionally distributed nature of its physical and operational underpinnings, but varying degrees of impact could be caused by localized damage at specific portions of the routing infrastructure. Damage to hardware and facilities supporting the network and the

concentration of infrastructure within exchanges, collocation, and hotelling environments could cause significant and lasting security and economic consequences (King, Chen, Wang & Verbowski, 2006).

8.14 Business Continuity/Incident response plan (IRP)

This is the primary document used by an organization to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically.

8.15 Reliable Data hosting Center

Choosing a reliable partner for our data hosting is a critical issue that can determine our stability and long time prosperity.

9. Conclusions

Disruptive events do happen, and in most cases, they are a 'when' rather than an 'if' question. Organizations that assume something will occur that will disrupt their ability to do business, and then plan for that eventuality before it happens will be well ahead of the curve in terms of their ability to survive the event and continue to service customers. Developing a well-planned business continuity plan should be a matter of highest priority for all businesses, regardless of size, structure or function.

The areas of risk outlined above are not exhaustive but cover very important aspects of information systems security. What is crucial in minimizing risk is for development to be done to a high standard, which will hopefully ensure there are fewer weaknesses in the first place. Secondly, all changes in technology must be tested thoroughly to identify problem areas in order that the organization can undertake remedial work and prevent future problems.

For the best picture of the situation, testing should be as objective as possible to ensure there is 360-degree coverage eliminating as many weak spots as possible.

Breaches of security can damage an organization's brand, reputation, and impact on the bottom line, particularly for organizations that generate the majority of their operations through online channels. As such, business leaders need to have it high on their agenda and everything must be done to ensure your organization's safety.

References

Bellissimo, A., Burgess, J. & Fu, K. (2006). *Secure software updates: Disappointments and new challenges*. InUSENIX Workshop on Hot Topics in Security (HotSec).

Bishop, M. (2005). *Psychological acceptability revisited*. In "Security and Usability: Designing Secure Systems that People Can Use." Edited by L. Cranor and S. Garfinkel. O'Reilly.

Blascovich, J. (2008). *Mind games: A psychological analysis of common email scams*. McAfee Avert Labs white paper (June 25).

Brancheau, J.C, Janz, B.D. & Wetherbe, J.C. (1996). Key issues in information systems management: 1994-95 SIM Delphi results, *MIS Quarterly*, Minneapolis, June, *20 (2),* p. 225.

Chen, H. & Corriveau, J.P. (2007). *Security Features and Technologies for E-business Architecture Design*. Proceedings of the International Multi Conference of Engineers and Computer Scientists. (IMECS '07), March 21 - 27, 2007, Hong Kong, 1150-1156, Newswood Limited.

Dhamija, R., Tygar, J.D. & Hearst, M. (2006). *Why phishing works*. In CHI.

Hiltgen, A., Kramp, T., Weigold, T. (2006). Secure Internet-banking Authentication. *IEEE Security and Privacy, 4(2),* 21-29.

Fink, D. (2005). IS security issues for the 1990s: Implications for Management. *Journal of Systems Management*, Cleveland, Mar/Apr., *46 (2),* 46

Freeh, L.J. (2000). Congressional statement of cybercrime before the senate committee on judiciary by the direct of FBI, Online at:

URL: http://www.fbi.gov/congress00/cyber032800.htm

Hertzum, M., Jørgense, N., & Nørgaar, M. (2004). Usable security and e-banking: Ease of use vis-`a-vis security. *Australasian Journal of Information Systems*, 11.

Gaw, S. & Felten, E.W. (2009). *Password management strategies for online accounts*. In SOUPS.

King, S.T., Chen, P.M., Wang, Y.M., Verbowski, C., Wang, H.J. & Lorch J.R. (2006). *SubVirt: Implementing malware with virtual machines*. In IEEE Symposium on Security and Privacy.

Lewis, J. (2000). Security strategy must focus on business issue of managing risk. *Internetweek*, Manhasset, Oct 2, 831, 41

Marquis, S., Dean, T., & Knight, G.S.N. (2006). *SCL: A Language for Security Testing of Network Applications.* Proc. CASCON 2005, Toronto, Oct. 2005. G. McGraw, Software Security: Building Security In, Addison-Wesley.

Pritsker, M. (1997). Evaluating value at risk methodologies: accuracy versus computational time. *Journal of Financial Services Research.*

Robinson, M. (2006). What every manager should know about system architecture. *Journal of Systems Management*, Cleveland, Jan/Feb, *47(1),* 18.

Smith, S.J., Milberg, S.J. & Burke, S.J. (2009). .Information privacy: Measuring individuals' concern about organizational practices. *MIS Quarterly*, Minneapolis, June, *20(2),* 167.

Tipton, H.F., & Krause, M. (2008). *Information Security Management Handbook*. Sixth edition, Vol.2, Auerbach Publiations, Taylor & Francis Group.

Whittacker, J.A., & Thompson, H.H. (2008). *How to Break Software Security*. Addison-Wesley Longman, Amsterdam.

Wysopal, C., Nelson, L., Zovi, D., & Dustin, E. (2007). Testing Fault Injection in Local Applications. *In The Art of Software Security Testing: Identifying Software Security Flaws*. Addison-Wesley Professional, part of the Symantec Press series.

Zviran, M. & Haga, W.J. (2009). Password security: An empirical study. *Journal of Management Information Systems,* Armonk, Spring, 15(4), 161-185.