*J. Basic. Appl. Sci. Res.*, 2(3)3046-3053, 2012
© 2012, TextRoad Publication

ISSN 2090-4304
**Journal of Basic and Applied Scientific Research**
*www.textroad.com*

# Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce, and Providing the Improvement Strategies

**Amir Ghotbi , Nazanin Nassir Gharechehdaghi**

Department of Information Technology, Shahid Beheshti University, Tehran, Iran

## ABSTRACT

The emergence of new technologies creates continuous changes in modern societies; the Information Technology is the most effective one of these technologies. Gradually, due to the widespread benefits of information technology in comparison with the traditional methods such as cost effectiveness, being easy and fast, companies have started their own electronic business. The current companies have done their own business worldwide and in an information-rich environment. Thus, the information is equivalent to the capital and requires the proper maintenance. For proper use of benefits of information in the business, the issue of information security is raised in order to ensure the data Integrity, Confidentiality, and Availability. The electronic stock commerce is one of the areas which have changed greatly in the recent years. Initially, there were a little attention to the aspects of information security management, and the main efforts were focused on the research in general and the technical aspects of information security in particular. According to the diversity and complexity of management tasks, researchers have tried to provide the various strategies for desirable management of information security and to reduce the main vulnerability of electronic business especially in the field of information security. This research is an applied study in terms of aim and descriptive research in terms of strategy; and tries to detect the security risks of electronic stock Commerce and provide the improvement strategies for this business. For the purpose, the questionnaire has been used in order to collect and analyze the managers' views in agencies with online stock trading system. The questionnaire data which were based on the Five Point Likert scale were tested by the one-sample T-test and the Friedman test. And based on the results of research, the improvement strategies of electronic stock commerce system are offered.

**KEYWORDS:** Risk detection; electronic commerce; information security; stock.

## INTRODUCTION

The Electronic Commerce is one of the industries in which the information security and especially the online stock trading in agencies are essential. Nowadays, the agencies allow their customers to trade their shares through the internet in any place and time, so they do not need to go to current offices. The main challenge of e-trading is to reduce the risk of this type of business especially in the field of information security.

It seems that the major weakness in this type of business is not having a set of information security management practices and the lack of understanding of each of these actions. Therefore, this study seeks to assess the security actions for information security management system in the electronic stock commerce, and provide the improvement strategies.

Confidentiality, integrity and availability of information are the attributes which constitute the implementation of information security [7].

According to the various theories and models such as the Technology Acceptance Model (TAM) for accepting any technologies its users should be ensured of usefulness and easy use of that technology and in case of any inefficiency and even the threat, they will have a negative attitude towards it.

Despite the great efforts in promoting the information management level in the traditional organizations, it seem that the previous theories do not have the ability to generalize to the current organizations with new features and the Electronic Commerce is also one of the main field of this topic.

According to the theoretical view, the organizations usually use a variety of styles and frameworks for the information security management and based on this, divisions have been made and tried to determine a particular model or style for the optimal management of information security in the organizations, but as Hong believes all these comments are the pieces which are isolated from each other and they cannot be used as single view alone, so the strategy should be found in order to integrate them [12].

It is necessary and vital to assess the security actions of information security management system in the electronic stock commerce, and offer the strategies for improving the security of this kind of industry. In addition, this old and disabled thought that "The information security is the result of technologies and technical tools" should also be forgotten [5,15].

***Corresponding Author:** Amir Ghotbi, Department of Information Technology, Shahid Beheshti University, Tehran, Iran.
Email: amirghotbi@yahoo.com

## Information

### Importance of Information and its Protection

The information is one of the most important assets of each institution; therefore it should be well protected because of its high and critical value for any organization. Some writers have likened the information to the blood in the vessels of organization, and have considered them as the resuscitative factor [11] [24] and if there is a restriction or risk in this process, the organization will be faced with death [8]. However, considering the information can have numerous benefits for the organization and have the essential and necessary role in the success of organization in fields such as cash flow and market value [16]. Moreover, the information is the bonding agent of other sources of organization [6].

### Information Features of business

Information as one of the main sources of business in the organization should have a fundamental quality which IT managers should be diligent in creating and maintaining it. These features, which are in direct connection with the issue of information security in the organization, are usually divided into three main categories:

**A) Confidentiality**: It means protecting the sensitive data from unauthorized disclosure or avoiding them to be understood [13]. In the other words, the information should be available only to the authorized individuals. This is done by two ways: either through limiting the access or encrypting the sensitive information.

**B) Integrity:** contains the integrity and comprehensiveness of information. The integrity is important in the decision making. [19] If there are gaps in the integrity of information, it could be as the result of unauthorized, unexpected and unintentional changes [22] [14]. The integrity of information occurs when the accuracy, completeness, timeliness, validity, and processing methods are provided [1] [3].

**C) Availability:** Availability of resources means using by a related person in the correct time. This feature is important because without it the usual activities of company could not be continued and the decisions could not be taken timely [9]. Moreover, by the needs can be answered and the considerable losses can be prevented by that [14].

The aspects of information security contain the access management or access control, authentication, not denying, confidentiality, communications security, data integrity, accountability, availability and privacy, and their relationships with different types of security threats have also been identified. It seems that according to the dependency of organizations to their own information and their responsibilities about the security, the efforts to preserve these important different aspects seem to be essential.

### Information Security

This topic includes protection of confidentiality, completeness and availability of information as well as other features such as authenticity, accountability, validity, being undeniable, and reliability of data. In the terminology of International Standard Organization (ISO) for the security of computer systems, the developed and used administrative and technological safeguard has been defined as the safety for data processing in order to protect the software, hardware and data from accidental or malicious modifications, destruction or disclosures [10]. Moreover, the security has been defined as the reduction of assets and sources risk from the vulnerability and diverse threats.

Information security is an issue which threatens the organizations around the world. Since the modern economies and businesses completely depend on the information technology for survival, data should be protected more than before [15]. In our modern world, the information has been electronically and the technology has constantly been changing. Since almost all aspects of our lives are controlled by the tools, procedures, and technological processes, it is important that the effects of electronic technologies have been understood as well as their weaknesses and secret components in order to be concluded in the electronic information systems [25]. Also it can be expressed that nowadays the information of business play an important role in most of organizations, and efforts for protecting such information are so important.

The global network and Electronic Commerce are another factor in the importance of information security management. Our daily lives have been changed by the proliferation of Internet and globalization and the modern organizations have been used the Internet for their business operations, thus they are related to it. This has resulted in the e-business which has changed the business processes of organization. The dependence on the e-Business also has raised the need to protect data and created different approaches for the information security management [26].

### Aim of Information Security Management

The aim of information security management is to ensure the business continuity, customer confidence, protect the investments and opportunities of business, and reduce the business losses by preventing and minimizing the effects of security incidents [23]. In addition, it can be indicated that the main purpose of designing the information security management system is to creating the confidence for high levels of management; so the information security of company is well managed as required by the excellent management and/or regulatory requirements. [2] Furthermore, the security management of firms will reduce the resource consumption, improve the management efficiency [14], reduce the risk and protect the valuable data [15].

**Information Security Management System**

The concept of information security management system (ISMS) was first discussed during the writing and development stages of British Standard 7799 in the late 1980s. The last definition of information security management system based on the International Standard is as follows: Information Security Management System is a part of an overall management system in the organization which is based on the risky approaches of business and its goals is to establish, implement, operate, monitor, review, maintain, and improve the information security.

Information security management system is designed for ensuring the adequacy and appropriateness of security controls which protect the information assets, so the customers and other Interest groups will be ensured about the security of the information. The aim of this system is implementing a kind of security controls which ensure the information security by establishing the needed infrastructure. In fact, an information security management system provides a systematic approach for sensitive management of information with the aim to protect them, and it contains the entire staff, processes and informational systems of an organization.

**Electronic Commerce**

Electronic Commerce means doing all businesses by using the computer communication networks especially the Internet. Electronic Commerce is buying and selling and exchanging the goods, services and information via the computer networks including the Internet. This type of trade is based on the electronic data processing and transmitting including the text, audio and video. The Electronic Commerce includes various actions such as the exchanging, fast delivery of digital contents, electronic fund transfer, electronic stock exchange, electronic bill of lading, commercial and engineering projects, and after sales services.

**Importance of security in the Electronic Commerce**

Despite the fact that the information technology is the part of today business world and it will become the important factor in the future, when the organizations connect with the systems and networks for example through the electronic terminals of exchanging money in the Internet place, electronic data interchange, etc. , this raises the risk of information security. Even if the internal environment is secured, we cannot control the systems which are attached to it and we may be faced with threats. This leads to double importance of information security in the virtual organizations because these organizations are have relationships with their partners through the network and Internet and use the complex and dynamic structure which result in the numerous security challenges. Changes in order to use the distributed systems in an organization lead to security risks in the systems [21]. Protecting the privacy of confidential information has become a measuring criterion of success in the business world because it improves the reputation of organizations and attracts the individuals' validity.

**Factors affecting the success of e-trading**

Moreover, other factors for the success of e-trading include the customers understanding, organizational flexibility, availability of resources, creating a brand name, having the integrated channels, specific marketing of electronic channels, systems integration, systematic changing management, excellent management support, and proper services for customers [20]. However, despite the fact that the information security is important for all financial institutions, the effective factors are different because of the different types of institutions, and they should be designed separately for each organization. In this regard, different plans, and implementing the security information separately for each specific organization can be mentioned [4].

**Stocks**

Stock is part of corporation capital which determines the contributions, benefits, and obligations of corporation owner. The Stock Sheet is a transaction document which represents the number of shares that the owner has in that corporation.

With the development of Internet security mechanisms and technologies, the growing development of e-trading and Internet users, the financial institutions should continuously improve the quality and efficiency of services provided for their own customers.

Tehran Stock Exchange is a market in which allowed brokers are buying and selling the accepted securities in the Stock Exchange on behalf of their clients. In the other words, transparent, fair and efficient market forming, organizing and managing for the securities trading is the main function of Tehran Stock Exchange.

In the recent years, the securities can be bought and sold paid via the Internet. Some brokers offer this service to customers. Customer orders will be sent to the broker and the broker will enter orders to the trading

system after reviewing and approval them. Orders entered into the system are placed in the queue of buy or sell based on price and time priorities. Based on the price priority an order of buy (sell) the securities with the highest (lowest) price will be placed at the beginning of buying (selling) queue, and based on the time priority, the order which is entered into the transactions sooner will be placed before the order which has the same price.
The transaction is done when the buy and sell orders have the same price, this mechanism is so similar to the transaction through the auction because the agents can change their place in the queue with improving the price of entered orders, or trade by providing the price equal to the proposed price by the target agent.

### Electronic Stock Exchange and On-line trading

The Electronic Commerce system aims to eliminate the middlemen and optimize the price. Each share in the market has experts who set the fluctuations in the prices based on the conventional buy and sell prices of their own shares (the difference between the market and demand price). Engaging in the price fluctuation forms the nature of an electronic stock market.

Online Trading is a term which most investors by hearing it think about the minor agencies such as E-trade, E-Schwa, and Fidelity which do the purchase and sale orders through the Internet by low fees. By benefiting from these minor agents' services rather than paying high commissions to the traditional agents, the investors can save millions of dollars. But the real power of Internet is hidden in changing the way people invest, increasing the individuals' savings, and creating a centralized automated electronic stock exchange. The electronic exchange eliminates the professional middlemen and extra payments which they create for reducing the risk and increasing the liquidity. Thus, more investors will be attracted to the market and also the transaction costs will be reduced. Eliminating the role of intermediaries such as specialists in the New York Stock Exchange (NYSE) and traditional brokers has created the major concerns about the market liquidity and efficiency which many ones are not willing to accept it. According to the most cost investors' views, the benefit from the use of online trading systems is negligible compared to the security feeling which they gain by the stock trading in the traditional markets.

### Research

### Research Questions

In order to assess the security measures of information security management systems in the electronic stock commerce, the research questions are as follows:

- How is the effect of component related to the business on the information security management system in the electronic stock commerce assessed?
- How is the effect of component related to the human management on the information security management system in the electronic stock commerce assessed?
- How is the effect of component related to the technical issues on the information security management system in the electronic stock commerce assessed?

These three types of classification into the business, human and technical factors are the background of research in the common information security management. For example, a comparison between these categories in some of the resources is shown in the Table 1.

**Table 1: Comparison of classified information security**

| **Security aspects of current study** | **Cynthi (2002)** | **NIST** | **Trček (2003)** | **Zucatto (2007)** | **Post and Kagan (2007)** | **Farn et al. (2008)** |
|---|---|---|---|---|---|---|
| Business | Operation | Operating | Legal | Business | Attributes of business | Operation |
| Human | Human | Management | Organizational | Society | Staff skills | Human |
| Technical | Technical | Technical | Technical | Technology | MIS evaluation | Technology |

## RESEARCH METHODOLOGY

In this study, the statistical population is the IT experts and senior managers in the agencies with online stock trading systems. We are faced with the limited community with 38 agencies, and the number of sample is calculated according to the below formula:

$$N.Z^{٢}_{\alpha/٢}.p.q/\left(\varepsilon^{٢}(N-١)+Z^{٢}_{\alpha/٢}.p.q\right) \qquad 1)$$

For qualitative variables and limited community the optimal number of 32 agencies was determined considering the value 0.05 for α, 0.07 for ε, and the amount of 50% for p and q, and by estimating the population which consists of 38agencies, also the experts and managers' answers have been used in this research.

### Variables and indicators for measuring them

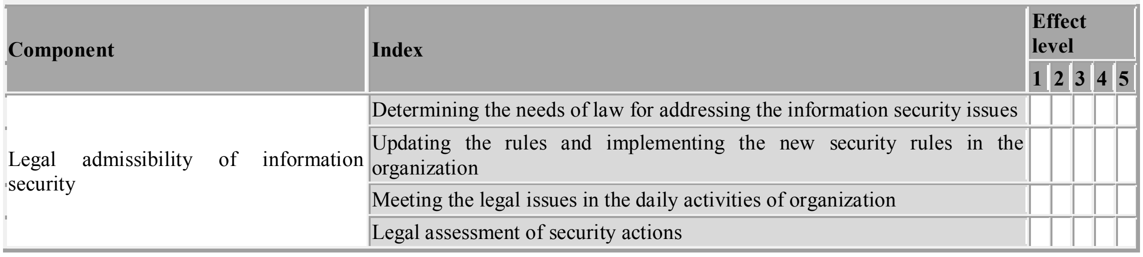
According to the conducted studies in this research about the appropriate security actions in order to implement the information security management, 63 actions (indicators) are evaluated.

### Methods and Data Collection Tools

This research has used the library technique and the basis for designing the components and indicators contained in the questionnaire has been extracted from it.

Field work is mainly based on the questionnaire. In the questionnaire which is completed by 32 managers and experts of information technology in the agencies, the effect level of each of the actions for improving the performance of information security management of agencies is measured by the Likert range.

**Table 2: A sample of survey for the importance of actions**



| Component | Index | Effect level | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Legal admissibility of information security | Determining the needs of law for addressing the information security issues | | | | | |
| | Updating the rules and implementing the new security rules in the organization | | | | | |
| | Meeting the legal issues in the daily activities of organization | | | | | |
| | Legal assessment of security actions | | | | | |

### Validity and reliability (Dependability) of measuring tool

Measuring the validity in this study was first done through the careful and extensive evaluation of background research, and then the components and indicators were discussed with several experts of information security management in order to be reformed. Therefore, the questionnaires were set based on the deep insight of the effect of information security actions on the aspects of information performance. In this study, the Cronbach's alpha coefficient has been used for the reliability. The Cronbach's alpha coefficient is one of the most widely used tools for measuring the reliability. In general, it is a steady scale and its Cronbach's alpha coefficient has the value 0.7 or greater. The Cronbach's alpha coefficient of 0.963 was calculated in a survey questionnaire and according to the statistics it indicates the reliability of questionnaire.

### Data Analysis Method

In this study, the one-sample T-test is used for data analysis and evaluation of security actions for information security management system (which were based on the range of five-scale Likert).

In the importance test for the security actions of information security management system, the analysis related to the assessment of the security actions measures was provided, and assessed by the questionnaire. Therefore, the managers determined the importance of each of 63 actions based on a range of five-scale Likert. In order to evaluate the importance of actions, the one-sample T-test with confidence interval 95% was used.

All components have the high average. One-sample t test also reveals that the importance average of each of the components at the significance level of 0.05 is greater than 3 (Test value). In the other words, all components are very important. It should be explained that because 32 people answered to all questions, degrees of freedom for all actions is 31. Thus, all measures are approved at the significance level 95%.

### Conclusion

In this study, after analyzing the questionnaires, which were determined based on the Likert range and tested by T-test with test value 3 and Friedman test, it was determined that the components of business had the greatest effect on the information security of electronic stock from the respondents' view; after the business issues, the human management components and finally the technical issues can play the most important role in the information security management of agencies.

This result shows that our managers usually care about the business issues and they consider the human issues less, so this causes poor human management of information security in the Electronic Commerce of our country.

About ranking the business components of Friedman test, it was observed that the component of legal admissibility of information security has been at the rank first and then the aligned components of information security management with business goals and IT, implementing the information security management and of technical standards, developing the policies and objectives of information security, and designing the information security structure have been at the next rank, respectively. Fortunately, agency managers have paid special attention to their business legal issues; these results also confirmed that the senior managers in agencies do not consider the information security management essential and do not think that it is necessary to create or modify the processes and procedures of information security of organization.

In the case components of human management, it was identified that the component of relations management with customer about the information security is in the last importance level of human management issues of organization and it indicates the customers' view of participation in the organization about the information security.

About the technical components, according to the results of Friedman test, the physical security component is ranked at the latest level and this indicates the lack of management approach of organization to the security of physical locations of agency.

**Improving Strategies**

This section has been compiled by the interviews with agencies managers:

- The company which designs the buy and sell software system should increase its online sales and after sales service, and periodically ask about its agencies and customers' problems and eliminate the defects of this software according to feedbacks and improve it continuously.
- The time difference between the original transaction and the information board on the websites about the price and the amount of supplied stock cause doubt and reduce the customer confidence to the agency and it is necessary to provide updated information for customers.
- People who demand for the electronic stock commerce services should be trained by the stock market.
- The agencies websites should be upgraded in order to train customers in the field of information security, and the electronic stock commerce system should be used by putting the e-learning contents on these websites.

**Suggestions**

According to this subject that the discussion of information security in the electronic stock commerce is so important and the shareholders concern about the financial transactions to protect their confidential information about the trading, and with regard to the results of questionnaires and ISO 27001 standard, the suggestions and measures are listed in order to improve the areas of information security in the electronic stock commerce:

- The first part of suggestions is about the businesses issues:

- The Security management standards which are valid and updated should be got and all the facilities should be used in order to match the security management function of organization with the world standards.
- The security policy of organization should be prepared and notified to all staff by mentioning the long and short term goals and responsibilities of each organizational unit in achieving the goals, and the staff should be aware of their own tasks to perform the policy document by holding the training courses.
- The appropriate rules and regulations should be defined and implemented, and there should be formulated and adopted laws of Electronic Commerce and other legal issues.

- The second of suggestions is related to the human management issues:

- The information technology unit should educate the staff about the security features of services used by the organization so they will protect the equipment without the security guards.
- The individuals' responsibilities should be developed towards the protection of information, and the responsibilities should be reviewed and clarified in the job descriptions for staff.
- Culture making has a special place in making the stakeholders familiar with the methods of Electronic Commerce; in addition, the culture of e-business should be expanded, and the investors should be assured about the information security and their properties. Moreover, for culture making in the field of electronic stock commerce, it is proper and effective to create a unit named the Notification about the Electronic Stock Commerce in order to provide the right, accurate and updated information in this field for investors in the Stock Exchange.
- Managers should provide necessary trainings in the functional fields for their clients and audiences, and also hold the training classes or publish the brochures, pamphlets and educational CDs for users.
- The individual rights should be defined about the confidentiality of customers' personal information, and the trust should be made in them.

- The third section suggests the technical issues:

- The policy of table and display without the documents should be made in order to enhance the system security.
- The information and assets of organization should be classified, and the procedures be established in order to control and protect them.

- The appropriate protocol should be used for creating the security and information confidentiality in a way that this protocol supports the authentication of server and client and protects the security and completeness of transmission channel by using encryption, authentication and message authentication codes.
- The stakeholders should be ensured in the field of compliance with the current standards, information security, and also the buyers' identity and specifications should be kept and the security systems used in the trading system be described.
- In order to assure the customers, agents need to ensure the shareholders that about the communication infrastructure the security devices such as updated firewalls, detection system, and intrusion prevention are used.

**Research Limitations**

There are limitations and problems in conducting any study and research. The above study is not also excluded from this and has problems which are briefly described:

- Lack of attitude for gaining the competitive advantage from the information security in the agencies;
- Lack of reliable competent authority in the information security in our country;
- Lack of IT experts and information security specialists in the agencies;
- Low development of agencies about applying the e-commerce as their primary process and not participate the customers in the information security.

## REFERENCES

1. Boritz, JE., (2004), Managing enterprise information integrity: security, control and audit issues, USA: IT Governance Institute.
2. Broderick, J. S., (2006), ISMS, security standards and security regulations, Information security technical report, 11, 26-31 .
3. Carlson, T., Information security management: understanding ISO 17799, Lucent Technologies Worldwide Services, Available from: http://www.netbotz.com/library/ISO_17799.pdf; 2001 [retrieved February 1, 2004.[
4. Chang, I., Hwang, H., David C., Huang, H., (2006), An empirical study of the factors affecting Internet security for the financial industry in Taiwan, Telematics and Informatics, 23 343–364.
5. Chang, S.E, Minkin, B., (2006), The implementation of a secure and pervasive multimodal Web system architecture, Information and Software Technology, 48, 424–432.
6. Eloff, M.M., Von Solms, S.H., (2000), Information security management: A hierarchical framework for various approaches, Computer &security, 19 243-256.
7. Farn, K., Fung, A., Lin, S., (2004), A study on information security management system evaluation—assets, threat and vulnerability, Computer Standards & Interfaces, 26, 501–513.
8. Fulford, H., Doherty, N.F., (2003), The application of information security policies in large UK-based organizations: an exploratory investigation, Information management & computer security, 11/3, 106-114.
9. Gerber, M., Von Solms, R., (2001), From risk analysis to security requirements, Computers and Security, 20(7):577e84.
10. Haj Bakry, S., (2003), Development of security policies for private Networks, International Journal of Network, 13: 203–210.
11. Halliday, S., Badenhorst, K., Von Solms, R., (1996), A business approach to effective information technology risk analysis and management, Information Management and Computer Security, 4(1),19-31.
12. Hong, K., Chi, Y., Chao, L.R., Tang, J., (2003), An integrated system theory of information security management, Information management & computer security, 11/5 243-248.
13. Humphreys, EJ, Moses, RH, Plate, EA., (1998), Guide to BS7799 risk assessment and management, British Standards Institution.
14. Kim, S., Kim, S., Lee, G., (2006), Structure design and test of enterprise security management system with advanced internal security, Future Generation Computer Systems, April .
15. Knapp, K.J., (2005), A model of managerial effectiveness in information security: From grounded theory to empirical test, A Dissertation Submitted to the Graduate, Faculty of Auburn University for the Degree of Doctor of Philosophy Auburn, Alabama December 16 .
16. McPherson, PK., (1996), The inclusive value of information, International Federation for Information and Documentation – 48th congress, p. 41–60.
17. NIST 800-12 Handbook, An introduction to computer security, National Institute of Standards and Technology, US Department of Commerce. Available from: http://www.csrc.nist. gov/publications/nistpubs/index.html; 1995.
18. Posta, G.V., Kagan, A., (2007), Evaluating information security tradeoffs: Restricting access can interfere with user tasks, computers & security, 26, 229 – 237.

19. Ritchie, B., Brindley, C., (2001), The information-risk conundrum, Marketing Intelligence and Planning, 19(1):29e37.
20. Shah, M., Siddiqui,Feroz A.; (2006) Organisational critical success factors in adoption of e-banking at the Woolwich bank; International Journal of Information Management 26, 442–456.
21. Smith, A.D., (2004), E-security issues and policy development in an information-sharing and networked environment, Aslib Proceedings: New Information Perspectives, 56, 5, pp. 272-285.
22. Thompson, K., Von Solms, R., (2003), Integrating information security into corporate culture, Masters Dissertation, Port Elizabeth Technikon.
23. Vermeulen, C., Von Solms, R., (2002), The information security management toolbox-taking the pain out of security management, Information management & computer security, 10/3 119-125.
24. Von Solms, R., Von Solms, S.H., (2006), Information security governance: Due care, computers & security, 25, 494 – 497 .
25. Wolfe-Wilson, J., Wolfe, Henry B., (2003), Management strategies for implementing forensic security measures, Information Security Technical Report. Vol. 8, No. 2, 55-64.
26. Zuccato, A., (2007), Holistic security management framework applied in electronic commerce, Computers and Security, 26, 256–265.