Research Journal of Applied Sciences, Engineering and Technology 5(13): 3586-3593, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 27, 2012 Accepted: September 17, 2012 Published: April 15, 2013

Information Security Management for Microsoft Windows Enterprise Environments

[1]Yu-Chang Chang and [2]Tzong-Chen Wu
[1]Graduate Institute of Management, School of Management, National Taiwan University of Science and Technology, Taipei, Taiwan
[2]Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan

Abstract: In this study, we introduce how these new tools improved the information security of users' operating system and assisted enterprises or organizations to comply with ISMS and ISO standards; this study also used case studies to explain what improvement and advantages that these tools brought to users' information security of these enterprises or organizations.

Keywords: Information security, ISMS, ISO

INTRODUCTION

Information security of users' operating system has always been considered as the most difficult one to be managed; certainly technical problems need to be overcome, however users' behavioral models and ways of being managed are the most important factors affecting information security. Each year, hundreds of thousands of computers are lost, stolen or their tasks are removed due to a lack of appropriate protection. Ministry of Defence (2012) pointed out that cost by information security is 27 billion in 2012. Evans *et al.* (1996) have a study of the exploiting activity-based information: easy as abc. Carter (1991) have a research of the learning method to measure performance: the use of indicators in organization public administration revies. Fortuin (1988) analyze the performance indicators-why, where and how. Yin (2002) have a case study research: design and methods. Franz *et al.* (2002) study Mr. fusion: a programmable data fusion middleware subsystem with a tunable statistical profiling service. Ambareen *et al*. (2001) give a research of the fuzzy cognitive maps for decision support in an intelligent intrusion detection system. Fausi and Fredrik (2004) have a research of the deficiencies in current software protection mechanisms and alternatives for securing computer integrity. Thorsten (2005) analyze the new fields of application forhoneynets. Howard and Longstaff (1998) study the common language for computer security incidents.

In practice, the most frequently complained problem mentioned by information personnel in all information systems ranging from personal computers to ERP is the management and control of users' information security. There are numerous uncontrollable variables in this problem and its difficulty level is never lower than information security of all large-scale information systems. Microsoft had launched a series of tools since 2007; in addition to strengthening information security of itself, it also added many mechanisms to manage users and the purpose was to manage and control users' information security which was the most difficult to be managed and controlled. This study would conduct case studies on two enterprises which used Microsoft's information security tools and then use ISMS/ISO 27001 standards to examine the information security performance of these two enterprises' users.

LITERATURE REVIEW

With the ever increasing and wide application of information technology, management and control of users' information security has also become an extremely important managerial scope of enterprises. This section had an in-depth investigation on users' information security through reviewing related literature and reports from some institutes.

ISMS (Information Security Management System): Information Security Management System (ISMS) is a method of systematic analysis and management of information security risk. 100% information security is an overly high expectation; the objective of information security management is to reduce information risk to the acceptable level through means of control. Hacking or fires are both operational potential risks for enterprises. The management Guru Peter F. Drucker once mentioned

Corresponding Author: Tzong-Chen Wu, Graduate Institute of Management, School of Management, National Taiwan University of Science and Technology, Taipei, Taiwan

that it's impossible to avoid all risks in running a business and therefore reducing risks, dispersing risks and managing risks are the criteria of constructing information security management systems.
Basic structure of ISMS is as follows:

- **General security:** There must be a complete planning and policy about information security within an enterprise including personal data collection and application, authority and training and education of information security, information security operation and protection, internet security management and system access control and management
- **Procedure:** Procedures dealing with information security event, management and reporting mechanism of the amendment of information facility and system, system backup facility, routine execution of necessary data and software backup and backup operation must be clearly defined
- **Standard Operating Procedures (SOP):** According to the defined procedures, standard operating procedures must be formulated in detail and documented so that users can deal with crises according to them
- **FORMS:** All types of document should have their own standard formats and be properly managed and saved to provide evidences or references

There are also standard procedures to establish ISMS. For the system establishment, the scope of ISMS should be defined first according to the characteristics such as the type, scale, resources, business nature of an organization. After considering the requirements of laws, regulations and contracts and estimating risks and coping measures, ISMS policies getting the approval from the management level and a declaration of application are then formulated. Next, the policies should be implemented and the unit in charge should execute these controlling measures to meet the objective of control and management. Besides, training and cognition plan should be done to ensure that personnel have the ability to detect information security issues and respond to and deal with them timely. The unit should also monitor the procedures and other controlling measures of ISMS and immediately identify the occurrence, processing procedure and solution of information security events. The effectiveness of ISMS should be examined routinely and related activities and events with significant effects should be recorded. Finally, ISMS should be maintained and improved; with the approval of the management level improvement activities should be done routinely and appropriate correcting and preventive measures should be adopted and all measures should be made sure to achieve their expected goals.

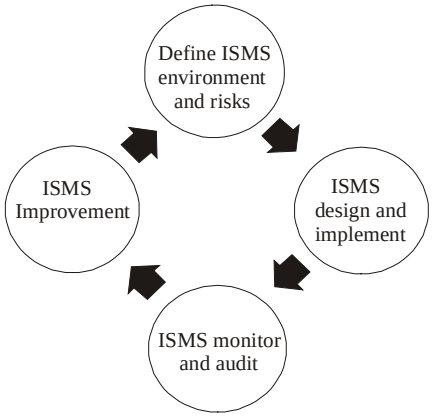

Fig. 1: ISMS Cycle

PDCA is also a method to measure the improvement of ISMS indexes; it can be used to constantly improve and construct information security management system so that flaws can be found out in planning and execution and they can be improved and processes can be amended effectively to improve the indexes. Figure 1 shows the ISMS Cycle.

ISMS cycle: The development of enterprises' information system is dynamic and the management method of ISMS can control the variables of the dynamic growth and allow enterprises to fully control information security. The design of Vista conforms to ISMS regulations and it has functions and designs corresponding to the general security, procedure, standard operating procedures and forms of IT information security; moreover, it can be customized according to enterprises' needs to achieve the purpose of managing and controlling information security.

ISO27001: What is the certification of information security management? ISO 27001, BS 7799 or ISO 17799? Many people probably have this question. In fact, BS 7799 is the information security management standard of England and its international version is ISO 27001. The confusion was caused because ISO first turned BS 7799 code of practice into the international standard ISO 17799 in 2000; however, the information security management standard BS 7799 didn't become the international standard ISO 27001 until 2005. The time difference caused that ISO 27001 and ISO 17799 seemed to be totally different.

This slight confusion has been improved; ISO had decided to integrate information security management standards as ISO 27000 and changed the name of the

code of practice ISO 17799 of ISO 27001 to ISO 27001 so that the certification of information security management ISO 27001 and its code of practice ISO 17799 could use the title of ISO 27000 series. The whole ISO 27000 series still has room for development and improvement. The number and outlines of ISO 27003, 27004, 27005 and 27007 had been established and after the contents are fully developed they will be released.

ISO 27006 specifies requirements and provides guidance for bodies offering audit and certification. The standards of ISO 17021 have been included in the series of information security management standard ISO 27000. This series will make codes of practice on the businesses to which information security management is applicable; for instance, ISO 27799 is the best practice guidelines of introducing the information security certification on the healthcare industry. Currently, the international standard number for the code of practice of introducing the information security has reached ISO 27058.

The ISMS systems which had obtained the certificate and passed through the certification will reach the goal of governance and good governance only after having an effective metrics system of performance measurement. For most organizations, governance and good governance is a hot topic and also a challenge facing them because it will affect not only the industry but also all managers of any organization. The certification of Information Security Management System still is the major task to achieve the goal of strengthening the ability to protect information security.

In 2007, ISO issued ISO/IEC 27006:2007(E) specifying requirements for bodies offering audit and certification of an ISMS and it provided the foundation for investigating requisite abilities to audit ISMS that the information industry expected certification bodies to have according to the requirements. As the environment gets more complicated and organizations grow larger, the extent to which managers depend on information will be higher day by day. A digital society is an environment with rich information and because people do not have the sufficient ability to process information and managers' time is limited, we had better build up an effective metrics system of performance measurement to provide managers with timely precautionary information of ISMS.

In 2005, based on "Federal Information Security Management Act" the U.S. issued the scoring and rating metrics system of ISMS that it has been following since 2000. In the section of the implementation of CNS (ISO/IEC 27001:2005) and ISO/IEC 27006:2007, the requirements of "effective measurement of ISMS and information security controls" has become an issue that ISMS governance must face so that the flaw of lacking ISMS policies of former ISMS documents can be improved and ISO/IEC 27006 can be gradually implemented.

Take the evaluation of information security policies as an example: we should establish quantitative management methods so that the goal of governance and good governance of ISMS can be achieved step by step. In the 1990s, the global civilization had gone through significant changes; the management of quality, environment and safety and hygiene increasingly tended to become unified and standardized and related international standards also affected the ways of economic development and organizational management and operation in many countries; the obedience to ISO 9000 quality management and ISO 14000 environmental management was the best manifestation.

DIMENSIONS OF USER INFORMATION SECURITY MANAGEMENT STRATEGY

Users' information security management included the following 4 categories:

- **Anti-virus:** After the first virus was created, people started to pay attention to data backup and look for coping strategies. At the beginning, viruses were created by software composers to protect their intelligent works and punish those who embezzle the software copyrights as a self-defense precaution. However, it was spread and created maliciously and thus produced unavoidable nightmares for computer users and hence data backup became the only passive self-protection method and users didn't have active defensive weapons until the launch of the first generation anti-virus program. Nevertheless, the production of viruses and renewal of anti-virus software had become an endless competition and information systems had turned into their arenas.
- **Anti-hack:** With the widespread usage of information system, internet and communication are widely set up and used and hence the first hacker was born. At first, he/she just sat in your living room for a while and left a sign telling you about its existence; later, systems were destroyed (intentionally or unintentionally) and even data were stolen. As a consequence, systemsecurity planning such as password, ID verification, dial-back and the construction of firewall had started to

be widely used and people expected that these could avoid hackers' invasion. Until then, users of computer systems thought that they could finally relax but no one knew that 921 big earthquake event and the terrorists' attack in New York on Sep. 11 had shocked them and made them be aware that it wasn't good enough to use anti-virus and anti-hack for information security and there were still many tasks needed to be done.

- **Anti-disaster:** In fact, anti-disaster design wasn't started from 921 big earthquake or 911 events. After these events, users began to create a more complete anti-disaster plan more seriously. In the past, efforts and budgets were only put in matters related to the environment (such as air, temperature, humidity and electricity etc.) and system fault tolerance (highly usable planning such as disk array, fault tolerant component and cluster server); however, after the events of 921 and 911, offsite backup, only used in data and systems of government or national defense institutes earlier, has been extensively applied in enterprises' systems. Even the mechanism of "setting up sub-office" was used by many organizations and enterprises in SARS period.
- **Anti-theft:** The popularization of information system has almost enabled each person to have one computer and the overflow and improper usage of information has become a serious problem. It's easy to prevent external thieves but it's hard to prevent internal ones; therefore, data security within organizations has become a new challenge for information security. Previously, bosses thought that employees couldn't steal companies' data if they removed floppy disks and it seemed that they couldn't do anything about the loss of confidential data with the prevalence and necessity of email and the launch of removable storage devices (such as flash disk). Therefore, encryption of data which could avoid improper stealing had become a wonder drug and data encryption management system (such as Microsoft's EFS or RMS/IRM) also turned into a new topic of information security.

With the above 4 major systems, it's still not good enough because many users have plenty of blind spots about correct construction, usage and maintenance. For these 4 major issues, the management strategies are set as the following:

- **The occurrence and solution of problems:** Users often complained that their computers still had virus attacks after installing anti-virus software and they even argued with the supplier; some users complained that hackers still invaded their systems after using firewalls; moreover, some users set up expensive data and system backup and auto-reply system but they found out that the function didn't work well. What are the causes of these unexpected events? What can we do about them?
- **Having good concepts:** Good tools are prerequisites to successfully execute jobs. All preventive systems are no more than tools and people using them must be equipped with sufficient knowledge and professional skills to be able to use and manage them properly and then we can expect them to have good performances.
- **Good planning, construction and maintenance:** As far as anti-virus is concerned, nowadays viruses have numerous types and their spreading approaches are highly multiple. After installing any anti-virus software, we must routinely update virus pattern and engines, as for operating systems and application systems we must pay more attention to patches provided by suppliers at any time to avoid the invasion and destruction of worms and Trojan. Do not open and even execute unidentified emails or programs out of curiosity and get used to do virus scanning on the files that we receive or download. In so doing, the chance to get viruses will be greatly lower (no guarantee that there won't be any virus).

The improvement of the functions of users' information security management of Microsoft's information security tools.

- In the past, the security of personal information system use didn't receive much attention and most IT personnel focused on the security of large servers or database systems. After personal viruses became prevalent, users' information system security gradually got attention. Nowadays, most of them only use anti-virus systems to deal with this problem; however, anti-virus is just a part of personal information system security. Anti-hack system is a new emerging subject and anti-disaster and anti-theft haven't been included in the tasks of information system security management by common IT personnel. The new-generation Microsoft's information security tools have included these 4 major functions. All enterprises using modern IT technologies face the most serious challenge- security threats that important information faces.

The designing idea of Microsoft's information security tools was to utilize highly stable platforms to provide the highest security and assist organizations to overcome risks. These tools applied whole new security certification needs and standards and therefore the platforms with more protection enhanced the security threshold. The tools are briefly introduced as follows:

- **Windows security center:** "Windows Security Center" is a single administrative site of computer security need and it supports anti-spyware monitoring (Windows Defender and cooperative supplier's application program), anti-virus software monitoring (cooperative supplier's application program), enhanced firewalls and other security setup etc. Users don't have to check many locations of their computers in order to check whether the firewall is open or anti-virus software is on or not. "Windows Security Center" even can apply cooperative suppliers' software to remind users of protecting files, folders and setup to avoid virus attacks.
- **Bitlocker:** BitLocke Drive Encryption technology. When a computer is lost or stolen, this new technology can prevent the confidential data and intellectual properties in it from being used by lawless people. Windows BitLocker adopted hardware data encryption technology. Besides, Windows BitLocker can encrypt the whole hard disk and therefore it can reduce the cost of buying new computers.
- **ASLR (Address Space Load Randomization):** The function of address space load randomization had come to exist in Unix system; when people booted a computer, they could download some important system files in different memory addresses. For operating systems of different languages, the corresponding memory addresses were all the same and there was only a little difference of corresponding memory address among operating systems of simplified Chinese, traditional Chinese and English versions. Hence, formerly hackers could attack computers of the same language or even of different languages after they compose an attack program of operating system of a certain language. However, the emergence of ASLR function enables address space to be loaded randomly in each operating system and even if there are worms it will be harder to cause a large-scale virus spreading. Moreover, as for the vulnerability of buffer overflow it will be harder for them to use the method of inferring memory address to attack successfully.
- **Patch guard:** Patch guard can execute the function similar to HIPS (Host Intrusion Prevent System) and it can prevent the amendment on core objects and then enhance the protection of the core layer.

Moreover, Microsoft' s information security tools have the following functions and effects as Table 1 shows.

Table 1: Effects of microsoft's information security tools

Function title	Effect
Browser protection mode	Limiting browsers' abilities to amend files and setup of users and systems to prevent users from the intrusions and attacks from malicious websites
Defender	Routinely scanning users' computers and suggesting users to remove any spyware or other hazardous software it finds to protect enterprises' computers
Advanced firewall	Offering new advanced functions to prevent users' internet and computers from malicious attacks more effectively
User account control	Allowing users to have the same level of productivity without working under the mode of system administrator and further improving security and total cost of ownership
New login structure	Providing improved verification infrastructure and allowing independent software vendors and organizations to execute their own verification approaches by composing credential provider such as identification or credential of biological characteristics
New infrastructure of smart card	Including a disk drive of general smart card reading device and improving infrastructure flexibility of smart card by Cryptographic Service Provider (CSP) module update obtained through Windows Update
Windows BitLocker™ drive encryption	Providing whole disk encryption and boot integrity check to assist enterprises to ensure that data in computers will be kept confidential even if they are lost, stolen or obsoleted
Encrypting file system	Encrypting every user's files, and data in public computers will be more secure
Group policy of device installation	Blocking the installation of removable devices such as USB flash disk and portable hard disk; this is helpful in preventing enterprises' intellectual properties or confidential data from leaking out or being stolen

CASE STUDY

Case profile: Case A focuses on the design, manufacture and sales of hardware and it has sales sites in the U.S., Europe, Japan, China and Taiwan. Case B develops wide-ranging investment projects including traditional, electronics, semi-conductor, telecommunication and bio-technology industries.

CASE ANALYSIS AND DISCUSSION

Case A: Case A indicated that Windows' new information security protection technology made its information security management more efficient. A's information security management had always been strict controls such as forbidding using removable storage devices and installing unapproved software; however, this type of management was slightly inconvenient for some departments because they needed to use them. "For IT department, it was difficult to manage particular when IT staff had to open some colleagues' authority to use USB at certain points in some projects." Case A also indicated that "In the past, when we used Group Policy to do management and control using USB was not allowed at all and if there were special business needs, we needed other solutions. Then, we could only buy software from the third party. Buying extra software was a cost and inter-system maintenance also needed personnel expense. Now, we use Group Policy of Microsoft's information security tools and because there are more than 500 new policies that we can set the auto-management ones according to our needs so that these policies will be more precise. Moreover, to enhance the convenience, group policy provides the approaches of searching, filtering and annotation etc. to make information security management more convenient.

Besides, when we open special project authority we can use the function of Event Log to do the double management of making operators' log and reviewing the log when needed." Group Policy is the foundation of Windows platform management and the mode of the central management of Group Policy helps Case A to implement its power management policy; even if employees do not shut down their computers, Group Policy still can make them turn into sleep mode and the business philosophy of diligence and simplicity can be truly achieved. Figure 2 gives the cost down of security problem loss in case A company.

Case B: For Case B, in order to improve the operational efficiency their employees are allowed to use USB and DVD/CDR; however, confidential data might leak out from the channels of these devices. From the perspective of information management, it's necessary to make a log about employees' data access behaviors and build up a mechanism of post examination. Event Log function of Windows Vista provides B with a strengthened guard of information security. Event Log has the function of making a log of users' access behavior and therefore it can record who accesses what data through what means in detail. TI

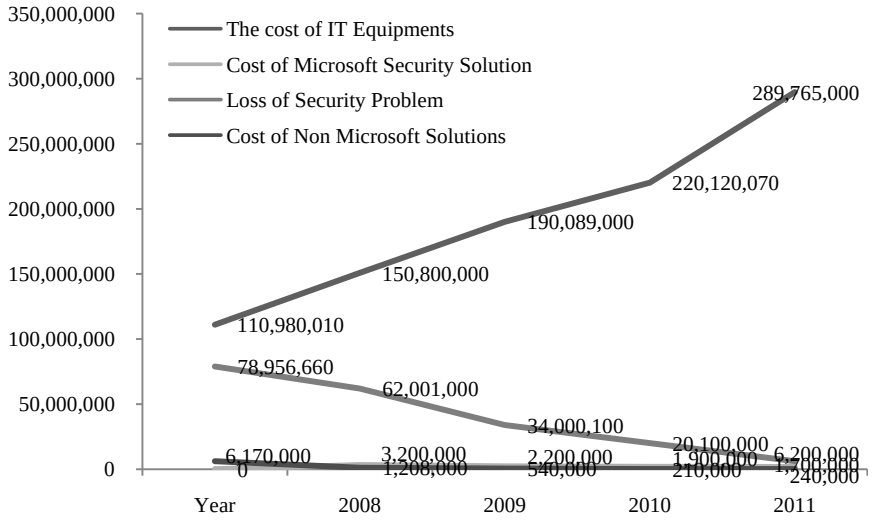

Fig. 2: The cost down of security problem loss in case "A" company

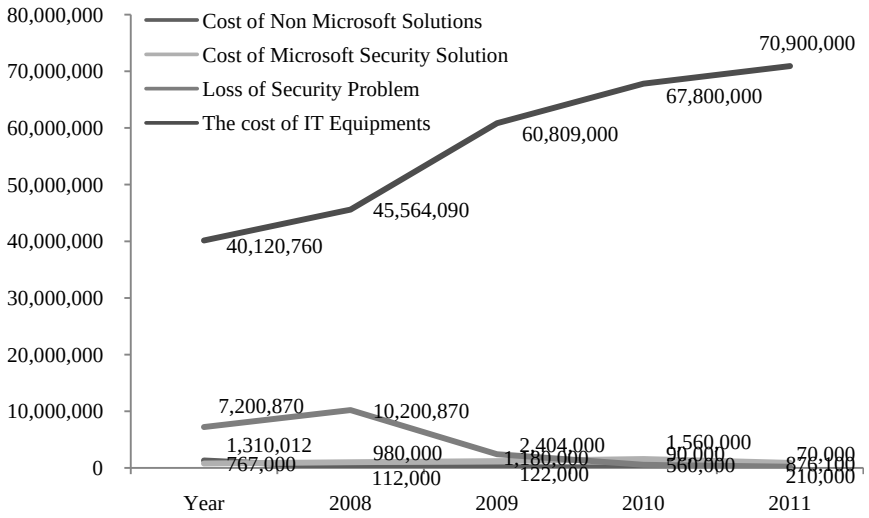

Fig. 3: The cost down of security problem loss in case "B" company

staff can also program that a notice email will be sent or certain programs will be executed immediately when some access behaviors which might violate information security policies happen. As for policies, informing users that their operation behaviors will be recorded can prevent them from violating information security policies. Event Viewer of Vista can make a log for future review and tracking and can be used as a tool of policy promotion; all these can build up a control and audit mechanism of information security for B.

Share Folder Tracking can effectively manage data access behaviors. In Case B, there are many cross-departmental projects and members of the same project will use a folder to be their public data-sharing space. Nevertheless, sometimes operation mistakes may cause that files are lost or overwritten and then it's easy to have disputes. Case B mentioned that "Through the function of Share Folder Tracking, Windows Vista can record employees' operation details in Event Log and whenever there are disputes we can review the log and this helps us find out the real problem and reduce careless harms to the minimum." Figure 3 shows the cost down of security problem loss in case B company.

DISCUSSION

There are ever-increasingly more and more new emerging internet attaching approaches challenging users' information security and it seems that this situation will never end and this challenge will become more difficult. It's an important issue to reach a balance between users' convenience and security; we can neither cause users' inconvenience nor let enterprises be exposed in risky environments of information security. This study will assist in constantly improving the experiences in introducing Microsoft's information security tools. Future researches will do further investigations and studies about the influences of the updated version and new functions of these tools on enterprises.

CONCLUSION

Microsoft's information security tools of new version are more secure than those of the past versions. Within half a year after Case A introduced these tools, the percentage of computers that were detected by Windows Defender as being affected by malicious software or spyware greatly reduced 60%. Within half a year after Case B introduced these tools, the percentage of computers that were detected by Windows Defender as being affected by malicious software or spyware greatly reduced 40%. The reduce curve is shown as Fig. 4.

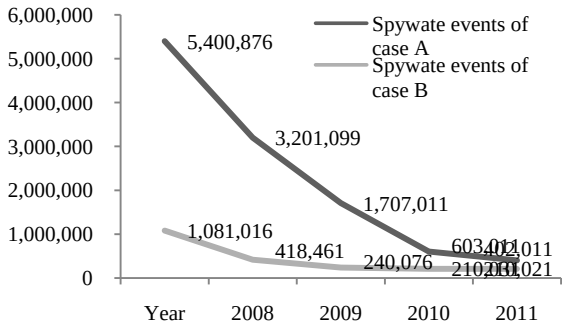

Fig. 4: The reduce of spyware events

Table 2: Compare table of before and after using MS security solutions

	Before using MS security solution		After using MS security solutions	
Item	Case A	Case B	Case A	Case B
ISMS Procedures	□	□	☑	☑
SOP	☑	□	☑	☑
Forms	☑	☑	☑	☑
ISO 27001	□	□	☑	☑

Table 2 shows the compare table of before and after using MS security solutions. After using MS information security solutions, Case A and case B are all fit the standard of ISMS and ISO 27001. The compare table of after and before using MS security solutions is as Table 2.

REFERENCES

Ambareen, S., M.B. Susan and B.V. Rayford, 2001. Fuzzy cognitive maps for decision support in an intelligent intrusion detection system. Joint 9th IFSA World Congress and 20th NAFIPS International Conference, 25-28 July, Mississippi State Univ., MS, 4: 2165-2170.

Carter, N., 1991. Learning to measure performance: The use of indicators in Org. Pub. Adminis., Rev., 12: 85-101.

Evans, H., G. Ashwort, M. Chellew, A. Davidson and D. Towers, 1996. Exploiting activity-based information: Easy as ABC. Manage. Account., 74(7): 24-31.

Fausi, Q. and T. Fredrik, 2004. Deficiencies in Current Software Protection Mechanisms and Alternatives for Securing Computer Integrity, pp: 66-88.

Fortuin, L., 1988. Performance indicators-why where and how? Eur. J. Operat. Res., 34(1): 1-9.

Franz, A., R. Mista, D. Bakken, C. Dyreson and M. Medidi, 2002. Mr. Fusion: A Programmable Data Fusion Middleware Subsystem with a Tunable Statistical Profiling Service. pp: 273-278, ISBN: 0-7695-1101-5.

Howard J.D. and T.A. Longstaff, 1998. A Common Language for Computer Security Incidents. pp: 23-25.

Thorsten, H., 2005. New Fields of Application for Honeynets. pp: 54-59.

Yin, R.K., 2002. Case Study Research: Design and Methods. Sage Publications, Thousand Oaks, Calif.