Article can be accessed online at http://www.publishingindia.com

COMPUTER VIRUSES AND THEIR ROLE IN ACCOUNTING INFORMATION SYSTEMS

Ali Shirzad*, Shaban Mohammadi, Hamedesmaeili Oghaz*****

**PhD Student FerdowsiUniversity of Mashhad,Iran*
***M.A Student in Accounting, Hakim Nezami University, Quchan, Iran. Email: Shaban1362@gmail.com*
****Master Student in Faculty of Engineering, MAshhad, Imam Reza International University, Mashhad, Iran*

Abstract *Dependence on information and rapidly changing technology can be seen in many organisations,with proper security and intelligence systems to protect themselves. But success in providing security dependsonthe awareness of managers and employees. The accounting information systems in organisations are the most important element. One of the factors threatening their system is virus. Malware are computer viruses that can cause a variety of disorders, including loss of data and accounting information systems are impaired in such case. On the other hand, one of the main objectives of the viruses is to steal financial information. In this paper, one of the main factors threatening the security of accounting information systems, the viruses are described.*

Keywords: *Accounting Information Systems, Information Security, Viruses*

Introduction

One of the areas of accounting is accounting information system design. Managers need information to make strategic decisions that is generally provided by the accounting information system. Business information systems involve data processing, but it is generally not thought what happens in information systems organisations. It is presumed that only simple processing of raw data is carried out and non-financial events affect the activities of the organisation. But the reality is that different levels of managers with a variety of issues are involved at varying degrees with the terms of complexity of problem-solving strategies and systems that can help solve this diverse collection. In a range of conventional retrospective information systems to intelligent systems, an argument prospective security of the system is considerable. Management information system, especially in cases where the system does not provide sufficient safety is essential, for risks that could threaten the system, are very high. The companies and organisations where the security of information systems is very low are at risk which can manipulate huge influence and damage could be irreversible. Safety information needs require that the forecasts made by the management to system information are properly secured and contain reliable information. So far, a lot of research on the role and importance of accounting information system in decision-making and the quality of performance information in decision-making is done, considering all rational economic decision-making roles of managers in the field. Since the security of information systems processing financial information is increasing day by day, the issue of security in the accounting information system, a special place among managers, accountants and auditors, has created.

Concept System and Accounting Information Systems

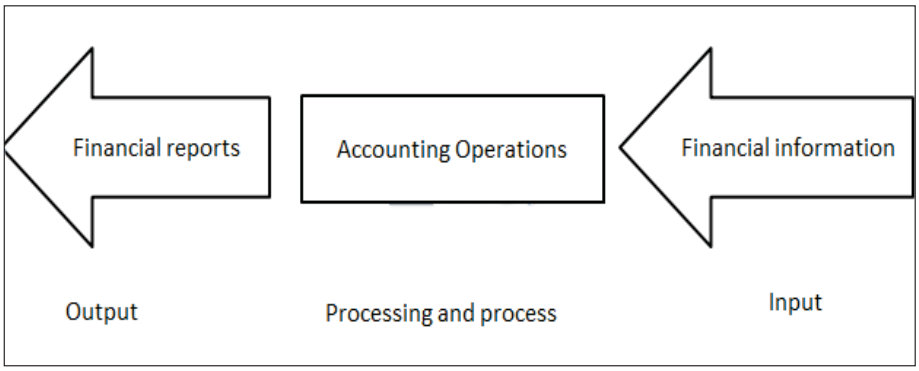
Concept system is a slang expression synonymous with the term of a technique or method that is used with various definitions provided that each system has to define certain terms. To achieve a comprehensive definition of the system, firstly some definitions expressed by experts are reviewed. Then implications of these definitions are considered, thus the definition of a system that is more complete explanation of the accounting system, will be released.The system can be used as a set of elements that interact with the relationships defined within the whole system and consist of a set (physical or idea) which is composed of interdependent components, having contiguous attachment components and behavior determined by the system (Ahlawat & Jordan, 2004). The system consists of agroup of physical or non-physical elements that constitute a set of interconnected and interdependent elements. Systems of interdependent components that make components for the achievement of certain targets are synchronised. According to the first definition, the set of elements and their relationships are mentioned as above, while in the second definition continuity and dependence on a number of elements of mind and purpose of the organisation are not considered. The

third definition says, the object and purpose of the system has been emphasized while in the fourth definition system components and coordination between them and the goals of the system are located. The four defining expressions that include all the features of the system can be found in the detailed definition of the system: The system consists of a set of components interconnected in the way of achieving one or more specifically interdependent target, so that if one or more data can be entered, one or more output is obtained out of them. Accounting system consists of a set of components that work together within a financial institution to report the events of that institution and make financial statements. Accounting system like any other system is composed of interconnected components, to achieve one or more of its activities. The financial events and financial reports can be used for different groups of financial information. And with the preparation of trial balance, control accounting system provides feedback information. An accounting system, as a system, is part of the main system. All open systems interaction with environmental factors such as economic and social. The impact of environmental factors on inflation accounting system was introduced after 1970. Changes in tax laws, commercial and banking data and its impact on their processing and preparation of financial statements and reports cited by the changes. The accounting system is made up of three parts: data entry in an accounting system, records of financial events based on primary documents such as data to the system, including billing, and purchase invoice (bill of sale, receipt, and payment cash). Data processing after data entry (primary documents) is done in the following order: primary documents are seen after analysis of their impact on the assets, liabilities, costs, revenues, and equity institution, in case the debtor and creditor are in general journal. However, in some institutions, rather than financial events, entries are made directly from primary documents in their registers, to provide accounting document (draft paper) (Ray & Gupta, 1992). In large institutions, primary registration of documents relating to a group of major financial events takes place in the offices of a private newspaper. Recordings are made in public and private offices, and newspaper accounts in the general ledger are transferred.When the volume of financial events related to one or more accounts ledger is high, for more detailed product information and general ledger accounts, etc., certain agencies or cards are used. Each of the offices of cardshasa control account in the general ledger which depends on the extent and type of activity (Bae, Ruth & Gwathmay, 2004). Outputs result in a data processing system, accounting, financial statements and reports. Health records of financial events in the journal are transferred to the general ledger at the end of each month with the preparation of trial balance. Trial balance, as the output of the accounting system and the process control isused in preparing the financial statements, and some information is retrieved as feedback to improve the accounting system for the new data. The final output accounting system and financial reporting and the information is provided in them.

Security and Threats

The successful management of business units is impossible in practice without the use of tools such as reports and information obtained from accounting information systems. In order to attain success and excellence in the field of competition, information systems are required. Accounting as an information system, uses business data to identify, collect, process, and distill it. Accounting information systems processes financial data and information, and this information is provided to a broad group of decision makers. Information is the most important source for decision-making, and it must also be established in the security system. IT accounting experts at their joint meeting, "security" as the most important technology that should be considered, chosen. This selection is based on the results of the seventeenth annual Feedback by the Association of of Certified Public Accountants America Tech has been done, so that in the list of Top Technology 2006, Technology

Fig. 1: An Overview of the Accounting System



Spyware programs detection and destruction into view in there. This technology is in the form of hidden programs that collect and transmit personal information without knowledge or consent of farmers in information systems, thatis discovered and destroyed. The importance of reliability of financial information for decision-making interest groups, in today's world is clear for everyone. Information security as the most important decision-making tool, is tangible. It is safe to say that every management decision is in the wake of the financial consequences and, therefore, management is required for any decision on financial information. The task of preparing and processing information to the accounting information systems is performed, so that security is established in the system. Information security is a process of accounting systems, and procedures to maintain accounting information systems against internal and external threats areused. Information security systems and security accounting promote qualitative characteristics of financial reporting of accounting data that will come when the desired result based on accurate and reliable informationis obtained (Flott, 2000). One of the requirements of a dynamic and healthy society for financial and economic activities is a safe space. Accountants must have the knowledge and experience to create such an atmosphere. In order to provide timely and useful information to users, auditors should ensure timely financial information security, accuracy and reliability. In this regard, auditors should take risks that might lead to the distortion of information and reduce the reliability of financial information due to the lack of security in their accounting information systems. For all the cases mentioned in the previous section for security in information systems, security systems in accounting information arenecessary, especially considering the fact that authority to access any part of the definition of locks and hardware and software should be designed. Also, periodic controls for manual calculations, records and various reports should be considered. Way to ensure the absence of virus in the accounting information system.

Attack Information

Managers should always be aware that there are many ways in which mishaps to information and computer systems can occur. Some of these deliberately and consciously take place and some are random and unintentional incident (Stoner & Stagliano, 1993). Regardless of the type of event, what is important is the loss or damage to the organisation's information; thus, these events are treated as a "strike" call. An interesting feature of this type of attack is that it can copy and steal the information, original owner of the information without being aware. In other words, the attacker could access unauthorized information.

Types of Attacks

Attacks can be divided into four basic categories: Attacks can be divided into four basic categories: access, manipulate, prevent denial of service and distributed.

(A) An attacker attempts to strike and obtain information that he should not see. This type of attack is to obtain confidential information.

(B) The attacker attacks to manipulate information and tries to change the information, thus the accuracy and integrity of information are destroyed. In this attack, an attacker can exchange and delete the information.

(C) Attacker tries to attack to stop services for an authorised user so that he can not use resources in the system or the system can not use data or functionality. Here an attacker does not attack to access or change the information, however, he preventstheauthorised users to use services. He is motivated to attack to stop the service, but usually not to sabotage the data. Its variants can be as follows: denial of access to information, stopping of catering to software applications, preventing access to the system, and blocking access to communications.

Fig 2: A Sample Demonstration of Security

(D) The other type of attack allows the information to be false or that of a real event or transaction that has taken place, be denied.

Such attacks can be as follows:

(i) Mask: In this attack, the attacker tries to falsify the identity of the person or another system.

(ii) Denies an event: In this attack, the attacker tries to propose the denial of doing something that has been recorded. Suppose a user uses credit card at somestore. But when the credit card company sends her shopping bills, it strongly denies that any such purchase from the stores.

Types of Threats

Managers to meet their information needs have been increasingly dependent on information systems. Accounting and accounting information systems are widely spread and complex. Along with increasing complexity of information systems, organisations are faced with threats.Threats that organisations face, are as follows: create, modify and manipulate the data, unauthorised copying or theft of information, release of information, destroy databases, and threats related to computer databases in the financial and economic affairs.Threats to the economic systems on line include the following: enter and penetrate into banking systems and unauthorised financial withdrawals from accounts with turnovers, and structuring transactions electronically unrealistic to obtain credit, open bank accounts,. changes in the financial and banking documents and forgery, and misuse of credit cards and shopping and virtual sales.

Viruses, Types and Potential Damage

Hidden Virus

Virus changes the file or record startup doing clandestine work. It changes the files creating a natural look and displaying it for others to read. As a result, the user will not notice a change (Krogstad, Ridley, & Rotenberg, 1999). The virus isalso somewhat deceiving.There should be a virus to protect against other virus while searching memory. The first record of this type of virus, Brain, is a DOS virus. It acts to control the input and output of DOS and every time a request comes to the area of the disc that has already been stored in the boot, it gives a healthy lead. From a programming standpoint, the virus is interrupted 21H subdued and results from DOS commands are directed to the area of user'schoice.

The Virus

Virusis hard to identify, because itinfects files used by the operating system. In other words, the virus only infects files that are currently in use. For example, a virus may be on a floppy boot area and infect a command such as FORMAT or SYS. One of the most common viruses, Darth-Vader infects only the files of the COM in writing by the operating system.

Viruses Backward

A virus after a direct attack tries to reveal their operations pass. Professionals from the virus are called backward as anti-virus detection. Making such ananti-virus is difficult because virus designers have access to virus detection software prevailing in the market (Robbins, 1993). The only thing that should be done is to study all the capabilities and features of the virus and find its weakness. The most common way is backward function of a virus that the data contained in the anti-virus program is not exceeded and by storing the virus signature file is deleted. The anti-virus is not able to identify the specific virus.

Viruses Multispectral

The virus also infects executable files and boot sectors. When you run a program infected with avirus, boot sector of computer's hard disk also gets infected. So each time you

Fig 3: A Sample Demonstration of Trojan

run a program, the infection is spread. One of the group's most famous viruses is One-Half.

Virus Armor

Virus's armor are armed with pieces of a program that operate by tracking, identification and destruction of the virus body. Armored virus may use the "dress code" senses observer the virus body throws. Then make their camouflage. Virus Wall is one of the most viruses. Wall is one of the most famous viruses of this type.

Virus's Exchange

Viruses exchange with a copy of an executable work. For example, a virus may become as winword.com. Thus, every time the operating system comes to winword.com, the virus is run to infect the system.

Phage Virus

It is the virus applications or databases in unauthorised manner causing destruction and change. The professionals have names these viruesPhage virus after virus in medicine domain. In such case, a virus infects a cell, and replaces the genetic code (in medicine). Similarly Phage virus isan executable program in the computer with ability to cause body changes.

Macro Viruses

At present, the growth of these viruses is more impressive than other viruses. These viruses can be developed on the network in addition to personal computers. The greatest danger macro viruses is that these are independent of hardware and operating system. In addition, the macro virus infects an executable file, but do not directly attack the data. The variety and species of macro virus rapidly increase. Till October 1996 only 100 registered viruses of this type were identified. In May 1997 the number rose to 700 and at present this figure is not comparable to earlier data. These viruses are written with a local language and within the applications. Examples of such programs include: recruitment programs, spreadsheet, and graphical virus writers to infect files that are created by this type of program. Thus, the exchange of infected files to other computers infect other computers' files, too. Any system that is able to read this type of files gets infected with this virus which will invade local language programs, often with great powers and can perform functions like deletion and renaming of files and folders to change the contents of a file. Many macro viruses are written using Word and Visual Basic. A macro virus written in VBA is able to infect a file in Excel, Access database or a PowerPoint project.

Some of the Known Macro Viruses

Word Prank Macro virus is a macro written with MS Word 6.0 macro language. Several macro viruses are formed like

Table 1: Overview of Computer Viruses

Virus Type	What it Does	How it Affects Our PC	Example of Virus
Resident Viruses	Lives as a resident in the RAM memory	Interrupts all of the operations executed by the system	Randex, CMJ, Meve, and MrKlunky
Program or File Virus	Infects executable such as EXE, BIN, COM, SYS	Destroys or alters programs and data	Sunday and Cascade
Boot sector Virus	Infects boot sectors on hard and floppy disks	Destroys or alters programs and data	Disk Killer, Stone virus
Multipartite Virus	A hybrid of a program and boot sector virus	Destroys or alters programs and data	Invader, Flip, and Tequila
Macro Virus	Triggers on a command in Microsoft Office	Commonly affects Word & Excel	DMV, Nuclear, Word Concept
Stealth Virus	Uses various tactics to avoid detection	Destroys or alters programs and data.	Frodo, Joshi, Whale
Polymorphic Virus	Uses encryption to foil detection, so that it appears differently in each infection.	Destroys or alters programs and data.	Voluntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101
Email Virus	If the recipient opens the email attachment, the word macro is activated	spreads only with the opening of the attachment in the email	Melissa, ILOVEYOU, Love Bug
Spyware	It makes unnecessary alterations to your PC & Changes your experience of it.	a computer system is causing it to slow down	7FaSSt, Elf Bowling

Trojan Horses	Programs that do things that are not described in their specifications	It allows other computer users to take control of your PC over theInternet	A2KM.Nitrogen , 91Cast, 8sec!Trojan
Worms	Negativelyaffects your system, they aredetected and eliminated by antivirus	It replicates as standalone programs	Lovgate.F, Trile.C, Sobig.D, Mapson.
Directory Virus	It inserts a malicious code into a cluster and marks it as allocated in the FAT	It prevents FAT allocation from being allocated in the future	Spam Laws, DIR IIvirus

Payload, File saveAs, AutoOpen, AAAZFS, AAAZAO. The virus tries to infect <normal.dot >file that is Word basic page. If at the time of infection <normal.dot>, are macros Payload or File Save As on the confirmation screen, the virus's assume that the page is infected and that takes work. Once the page is infected, key files that are stored by the Save As option, will be infected. By selecting Tools> Macro, one can discover the presence of the virus.Ifin the list of macros AAAZFS name is seen, concept virus has probably infected your systemby creating macros that contain any grammatical form called Payload. This macro will overwrite the virus, and the virus is believed to infect the system and will continue to work. Creating macros Payload is a temporary solution. May be someone else no matter whether the file <normal.dot> contains macros or Payload File SaveAs using other viral Concept body design. Another famous macro viruses are WordMacro / Nuclear, WordMacro / DMDA, WordMacro / Hot, WordMacro / Colors, WordMacro / Bandung, WordMacro / Atom, and WordMacro / Wzzu. The best solution to deal with macro virusesof MS Word 97 is to open the file containing the virus after a message is displayed. In addition, it is better that all Word files as email attachment are downloaded from the Internet or stored on the disc. In addition, in the new version of VBA, the security mechanism is intended that the survey method can make all macro viruses ineffective. VBA language within many applications such as AutoCAD, Photoshop, and Chameleon is used.

Security Policy and Proposed Ways to Prevent the Risk of Viruses

If the software to protect a computer from known viruses are used, the user need not worry about viruses. New viruses are produced daily and distributed, thus anti-virus software to detect and eliminate them should be updated on a regular basis. To do this, you can visit the website of the manufacturer of anti-virus and receive information about how to update the software.

Do not Open Email from Unknown Sources

Follow this simple rule, "If you do not know the sender, follow the letter and attachments very carefully." If you receive a suspicious e-mail attachment, the best practice is to remove the entire email. For added security, even if the sender is familiar, such mails should be treated with caution. Your friend may have randomly sent you a virus. I Love You virus did exactly the same for millions of computers worldwide which got infected. Do not hesitate to delete suspicious emails. Anyone who uses a computer must have sufficient information about the security, Likehow to use and update their antivirus software, security patches, how to install them, and how to choose the method of getting the proper password, among other things.

Fig 4: A Sample Demonstration of Deciphering Password

Use Strong Passwords

Password-only access to resources limits strangers from guessing it simply. Do not share your password with anyone and do not use the same password at more than one place. In such case, if one of your passwords is compromised, all the resources at your disposal will be at risk.Golden rules for choosing passwords include the following: the password must contain at least 8 characters, possibly meaningless words, for example if you choose a combination of lowercase and uppercase letters and numbers as xk27D5Gu, safety will be higher. Change your passwords on a regular basis.

Protect your Computer from Intrusion by Using Firewall

Firewall provides virtual buffer between a computer system and the outside world. This product is produced in two forms, software and hardware to protect PCs and networks. Firewall prevents illegal data or data that are potentially dangerous to cross the filter and other information. Moreover it also acts as a shield when the computer is connected to the Internet, preventing unauthorised access to the computer. For the benefit of firewall use antivirus Internet Security.

Lack of Computer Resource Sharing With Strangers

Operating system makes it possible to provide users with the purpose of sharing files, access others' files via local network or the Internet. This feature provides the possibility of transmission through the network. On the other hand if the user is careful not to act in the share files, it allows you to share your files to others.So the real need is to have the ability to stop files sharing.

Disconnect the Internet Connection When not in use

Remember that the digital highway is a two-way where data can be sent and received. Disconnect the computer from the Internet when not needed. There is no possibility that someone has access to your device and destroy the data.

Backing up Data

Always be prepared for the loss of data saved on your device memory. Today, a variety of hardware and software are available to have backup copies according to the type of data Care must be taken depending on the policy.In this process, the appropriate equipment and time are specified for backup. In addition, this should always be available to the Start Up disk so that in the case of adverse events, the system can restore as quickly as possible.

Getting Regular Security Patches

Manycompanies producing software offer updates and security patches from time to time .Over time, new problems are identified in the software that make it possible for hackers to take advantage. Having identified the problem, the product manufacturer releases patches for enhanced security and destroys the way of penetration into the system. These patches are available on the corporate website and users need to secure their systems with this. Always have the latest version of the patch installed on your system. For the convenience of users, tools have been developed to automatically connect to the sites of companies producing products and receive a list of the latest patches. Then review the current system and identify its weaknesses. Thus the user becomes aware of the latest version and update.

Regular Review of Computer Security

Review computer securityat regular intervals to evaluate the security situation. Doing this at least twice a year is recommended. Reviewing and configuring security software, including browsers and ensuring appropriate security level settings are performed in the process. Proposal for the security of your system will benefit from OPSWAT Security Score tool.

Conclusion

Nowadays, computer viruses are a major cause of damage to security. Meanwhile stealing financial information is one of the main goals of viruses. Lack of attention to the potential risks of viruses and lack of being proactive on this issue may cause irreparable problems. Another aspect that should be considered, is subject to audit. The assurance auditors must examine the accounting information systems security. Auditors are aware that without the security of information systems and accounting, managers will not be able to provide accurate and reliable information. This increases the importance of security. The proposals must be noted that as a user, we comply with laws governing the Internet. Anti-viruses are used to avoid getting infected computer, delete anonymous emails. We should have a good firewall to prevent intruders from accessing the systems. For periodic backup of data we should update our information systems. Computer security examines situation periodically. At time when we do not need an Internet connection, it should be cut off. For proper use of memory stick, security experts also take advantage of the comments.

References

Ahlawat, S. S., & Jordan, L. D. (2004). Anexamination of internal auditor objectivity: In-house versus outsourcing, auditing. *A Journal of Practice & Theory,*147-158.

Bae, B., Ruth, E., & Gwathmay, S. S.(2005). Internal Control Issues. *Information System Control Journal,* 4.

Flott, L. W. (2000).Quality Control. *Internal Auditor Journal.*

Krogstad, J. L., Ridley, & Rotenberg, L. E. (1999). Where we are going? *Internal Auditor Journal,* 27-33.

Ray, M. R., & Gupta, P. P. (1992). Activity Based Costing. *Internal Auditor Journal,* 45-51.

Robbins, S. P. (1993). *Organizational behavior.* NewJersey, p. 45.

Stoner, E., & Stagliano, A. J. (1997). A survey of US manufacturers on implementation of ABC. *Journal of Cost Management,*39-41.