SOCIO-ECONOMIC IMPACTS OF COMPUTER VIRUSES IN TANZANIA

M.A.M. Victor and J.L. Kamara
Department of Engineering Management and Entrepreneurship
Faculty of MECHE, UDSM P.O. Box 35131, DSM
mmvictor@uccmail.co.tz

ABSTRACT

This paper reports on a research project conducted with an objective of identifying and assessing various approaches used by different computer users (Management, System Administrators and end users) in Tanzania to combat computer viruses (CVs), and to assess users' awareness level on CVs. Specifically, the study aimed at assessing the awareness level on CVs to the Tanzanian business community; analyze the socio – economic impact caused by CVs in Tanzania and; assess existing methods, capacity and limitations on controlling CVs in Tanzania.

Data was collected using both questionnaires and interview from financial institutions such as NBC and BOT, and telecommunications sector such as TTCL and VODACOM. Other institutions where data was collected included the higher learning institutions such as UDSM, DIT & IFM, Government institutions such as the Government Chemist, and COSTECH and Non- governmental institutions such as REPOA and ESRF.

After data analysis, it was found out that majority of the surveyed organisations were aware of CVs and about half of them employ client-server technique to successfully deal with the threat. These organisations spend between US$ 12,000 to 40,000 per year to deal with CVs. This cost is mainly for paying licence fees for anti-viruses and for data back-ups. Some organisations rely on pirated anti-virus which are unreliable and in most cases lead to disasters and losses of data and production time.

It was concluded that CVs control should be given the highest priority to all ICT users. Also a policy on CVs should be well written and be instituted. Knowledge exchange on Anti-viruses' configuration should be enhanced among System Administrators within Tanzania. CVs control training should be done frequently to all workers. The use of an inert operating system such as Linux to control the spread of CVs should be promoted for use in workstations and for newly established organizations. Budget for CVs control should be considered at early stages.

Key Words: ICT, Computer viruses, Anti-viruses

INTRODUCTION

The use of Information and Communication Technology (ICT) in many Organizations and Institutions in Tanzania resulted into the spread of Computer Viruses (CVs).

Worldwide, spread of personal computers (PCs') resulted to a communication system, at that time (1980), known as computer bulletin boards. People started to communicate to each other through computer bulletin boards. Frequent uses of computer bulletin boards led to the precursor of the virus known as the Trojan horse. A Trojan horse is among the earliest strains of computer viruses. It is a computer program that when downloaded and tried to run can erase the memory disk. The earlier PCs had no hard disks, and their programs were small in such a way that the operating systems including other programs were stored in floppy diskettes. So, one could turn on the machine and load the operating system including other programs such as games or word processor. While running it, a Trojan horse could wipe out the system.

Computer Viruses can be defined as computer program that makes copies of itself whether or not the computer is in operation and infects diskettes or files available in a hard-disk (University of Washington, 2004). Therefore, CVs can only infect files and corrupt data in a particular computer. Currently, viruses can even damage the hardware.

The word **VIRUS** is used as an acronym for "**V**ital **I**nformation **R**esources **U**nder **S**iege"

(Kane, 1989). CVs are either self-distributed or sent by somebody through the e-mail system as an attachment file with extensions such as "pif", "vbs", "com", "bat", "exe", "scr", "lnk" or "js". Some actual Trojan filenames include: "dmsetup.exe", "movies.avi.pif", twice or more zipped files, and "LOVE-LETTER-FOR-YOU.TXT.vbs".

A worldwide survey done confirms areas which are highly affected with CVs to be financial services, government services, telecommunications and manufacturing processes (Townsend and Taphouse, 2002). The worldwide economic impacts caused by computer viruses reported on the website www.cybersecure.ca/q2.htm, are as shown in Table 1 (Beverly, 2001). This shows that serious negative economic impacts can be realized from CVs.

Table1: Worldwide Economic Impact caused by CVs

Year	Code Name	Worldwide Economic Impact ($ U.S.)	Cyber attack Index
2001	Nimda	$ 635 Million	0.73
2001	Code Red(s)	$ 2.62 Billion	2.99
2001	SirCam	$ 1.15 Billion	1.31
2000	Love Bug	$ 8.75 Billion	10.00
1999	Melissa	$ 1.10 Billion	1.26
1999	Explore	$ 1.02 Billion	1.17

Source: (Beverly, 2001)

STATEMENT OF THE PROBLEM

As many institutions and various organizations in Tanzania are using ICT intensively in their daily activities, it is obvious that they are getting infected with various computer viruses. As a consequence some organizations experience some delays in production activities or do not achieve the set targets. CVs cause data losses and impose extra costs to replenish the defected parts as well as to pay experts. Also, the value of time lost while System Administrators work hard to eliminate CVs from the systems is not well known. Globally, such information can be obtained based on reported incidences. So far, in Tanzania, there is no data/information available regarding this issue.

Tanzania online.org websites had registered about 105 different organizations, not including all ministries and government institutions which are using ICT intensively, despite the danger of loosing their information when they get infected with CVs. It is not well known whether or not they are aware of the CVs and how they alert each other on the same. If they do so, the question that arises is, do they have any common means of defending themselves during CVs out-break? Therefore, there is a need to carry out research on some selected institutions/organizations so as to evaluate and study ways used by various System Administrators to overcome such situation and assess the socio-economic impacts.

LITERATURE REVIEW

A computer virus is a man-made computer program. A combination of three attributes to a certain program makes that program to be known as a virus. These attributes are replication, concealment and bomb (Brenton, 1999). In other words it is a section of a code of which, when executed, will attach itself to other programs in such a way that it will be executed when those programs are executed (Olivier, 1990).

Computer viruses are classified based on their targets and items they infect. That means, categorization is done based on their primary function and propagation method (Hameed, 2003).

Categorization based on what they do

This group comprises the Boot Virus, Program Virus, Multipartite Virus, Stealth Virus, Parasitic Virus, Polymorphic Virus, and Macro Virus. The Boot Virus infects the boot sector of hard-disk storage (for example, Form, Disk killer and Michelangelo). Infection is simply by accessing the disk. These viruses can "infect disks" by attaching themselves to special

programs in areas of disks called boot records and master boot records. These areas contain programs that computer uses to start up. The Program Viruses infects executable programs (for example Sunday and Cascade), such as word processing, spreadsheet, computer games or operating system programs (Hameed, 2003).

Also, the Multipartite Virus infects and spreads from both program files as well as boot records (for example Invader, Flip and Tequila). Another variety is the Stealth Virus that actively seeks to conceal itself from discovery or defends itself against any attempt to analyze or remove it (for example Frodo, Joshi and Whale). The Parasitic Virus embeds itself into another file or program such that the original file is still viable, for example Jerusalem (Norton, 1995).

The Polymorphic Virus Changes its code structure to avoid detection and removal (for example Stimulate, Cascade, Phoenix and Evil). The Macro-Virus exploits the macro-language of a program like MSWord or MS Excel for malicious purposes (for example DMV, Nuclear and Word Concept). Macro-viruses infect data files with micro capabilities. Microsoft Word document and template files are susceptible to macro attacks (Hameed, 2003).

Categorization based on Propagation method

This group is composed of Trojan horse, Worm, Bomb and Port Scanner. The Trojan horse is a computer program. The program claims to be a game, but when it is run, may erase the hard disk resulting into lose of information. Trojan horses have no way to replicate automatically (Hameed, 2003).

The Worm is also a computer software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole, and then starts replicating. It propagates on its own by a variety of means including hijacking email accounts, user identifications and file transfer programs. It replicates itself and damages data. For example, it can change passwords on existing accounts; can modify logon scripts and so on (University of Washington, 2004).

The Bomb does not propagate itself at all. It is placed by human being activities or another

program and is activated by a trigger such as time or event. It is known as social engineering virus because it wastes the bandwidth when it attaches on a message. The Port Scanner hides on a system and scans the surrounding environment for IP address and open ports such that it then makes available to other malicious codes or individuals (Brenton, 1999).

Evolution of Computer Viruses

The historical background on computer virus is as follows: CVs evolution and sequences can be traced back to the 1980's. At the beginning there were CVs with the nature of displaying a wrong computer file, inverting the video and clicking speakers as well as infecting other computer programs. These were followed by the boot sector infector (BSI) and replicating CVs. Earlier CVs could copy themselves into the floppy but not infecting it. Nowadays, they are not. As technology changed in the early 1990s, it resulted into serious complex CVs due to self-encrypting and it was very difficult to analyze them. CVs during that era were infecting all .COM and EXEC files as well as Master Boot Record (Marshall, 2005).

In the late 1990s the first Windows 95 and Macintosh CVs infectors were released. Again, CVs started to attempt to write the flash BIOS. At that time the creation of the macro/worm hiked the industry. For example, Melissa and Christma.EXE spread quickly infecting a specific subset of users. Distributed Denial of Services (DDoS) package and Explorer zip CVs were circulated. In the year 2000, there came Visual Basic Script (VBScript) viruses / worms which were sent through email or sometimes they appeared as attachments with two extensions. The trick of giving an attachment with two extensions has grown to be very common with the following meaning: The first extension suggests a harmless, non-executable text file, while the second extension indicates that the victim would not see the real nature of the file. In the year 2000 viruses caused servers to melt. Servers are said to melt due to the BIOS program being corrupted with CVs. Nowadays, there are files infecting viruses compatible with both Microsoft windows and

LINUX executable file types (Harley, et. *al*., 2001).

Various approaches to combat computer viruses

Computer viruses can be prevented by using network security measures as outlined here into four 'A's (Townsend and Taphouse, 2002):

- Authorise (Secrecy). Firewalls authorise only certain visitors to access the computer or servers they protect.
- Authentications. Tools such as public key infrastructure (PKI) validate or authenticate identity of participants in electronic conversations or transactions.
- Administer (Non-repudiation). Privilege Management Infrastructure (PMI) tools help to administer company policies laying down who is authorised to see or modify certain data.
- Audit (Integrity control). Forensic tools audit or dissect an electronic crime scene, uncovering who broke in and what was done while behind an electronic company's walls.

According to Harley and colleagues (2001) writing a virus is not illegal. But legal actions are active to those who may be guilty of causing the following during use of their programmes:

- Damaging or destroying property;
- Rendering property dangerous or impairing its ability to function; and
- Obstructing the lawful use of property.

Regarding regular CVs threats, some International standards were established to control them. For example, the BS 7799, British Standard Code of Practice for information security management is used to virus controls. The standard emphasizes the following points:

- The need to educate users in virus control and, in particular, the need for a proactive virus strategy;
- The need to encourage general security awareness; and
- The need to implement appropriate system controls.

CVs have raised the key questions being asked today by frequent computer users, "…how can I protect myself or organization? And what are the cost of being hit and recovering from it…?" It was pointed out that the network security attacks are increasing in number and sophistication. New evolving attacks are capable of spreading faster than any possible human response efforts (Greek, 2004).

RESEARCH OBJECTIVES AND METHODOLOGY

The general objective of this research was to identify and assess awareness level, socio-economic impacts as well as various approaches used by different computer users (Management, System Administrators and end users) in Tanzania to combat computer viruses.

The research started by identifying vulnerable areas with CVs. Various institutions were sampled and visited. The surveyed areas included the following: financial institutions such as NBC and BOT. Telecommunications sector included TTCL and VODACOM. Higher learning institutions included UDSM, DIT & IFM. Government institutions included Government Chemist, and COSTECH. Non-governmental institution included REPOA and ESRF.

These institutions were purposefully selected to include those with extensive use of computers in their operations. Various interviews with different System Administrators, computer users as well as management team were conducted. All visited institutions filled the distributed questionnaires and some observations were made while at their work place. The researchers used SPSS software plus MS Excel software to analyse collected data.

RESULTS AND ANALYSIS

Analysis of CVs awareness level

Users' awareness on the CVs was tested on various aspects to check their attitudes. Such aspects includes: frequency of updating the AV software, reasons to keep CVs attack records, and users' level on understanding organization policy on CVs.

Frequency of updating the anti virus software
Respondents revealed the frequency of updating the anti-virus software as shown in Figure 1. Those updating the anti-virus software on a daily basis are (36%), followed by weekly updates (29%). Other respondents undertake updates whenever an update is released (21%). Also there are those who update monthly (14%).

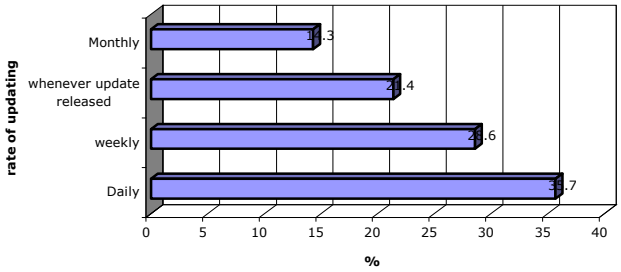

Figure 1: Frequency of updating the anti-virus software

Reasons to keep CV attack records
The tendency to keep CV attacks experienced by various organizations was indicated by respondents. That most of the organizations (35.7%) use attack records for various purposes, including doing analysis and finding solution for the affected areas. Some organizations (21.4%) need to look for more effective anti-virus software, while others (7.1%) want to know who are trying to penetrate their system. The study revealed that others (7.1%) just wanted to know the frequently attacking virus and get appropriate anti-virus software. Some organizations (28.6%) revealed that they do not keep records or they keep for a short period before they rewrite the back-ups.

Availability and Knowledge on Organization's Computer Virus policy
Respondents' knowledge on CVs was tested to know users' awareness on any existing CVs policy. Results revealed that about 57% of the organizations had ICT policy (which includes CVs issues) already known by users. Thus, additional efforts/ campaigns are required to change the understanding of various organizations on the need to have such a policy in place.

Socio –Economic impact

The respondents were required to indicate the socio-economic impacts that have occurred in organizations as a result of CVs attacks. In order to analyze the socio-economic impacts, various incidences caused by CVs were analyzed. In the analysis, all costs as a result of CVs attacks were investigated. Such costs included costs incurred to replenish the defective software/ hardware, costs to secure anti-viruses; costs of securing back-ups; the time value wasted while a System Administrator resets the system.

Majority feelings on disconnection from the Internet
Respondents were asked to indicate their feelings on the situation of staying without Internet services. Their views were analyzed. The respondents indicated that to stay without Internet connections due to the CVs 35.7% were getting hard time, 21.4% were annoyed, 21.4% were bored, 14.3% were frustrated and some users 7.1% felt embarrassed.

Cost to replenish the affected software / hardware
The respondents were asked to indicate the amount of cash spent on securing new items after being affected with CVs. It was found out that organizations dealing with highly valuable and sensitive data systems were investing highly on controlling CVs. Every organization has its plan to replenish the defective items. About 57.1% of the surveyed organizations do not replenish the defective items. The rest of the organizations replenish the affected systems by spending between US$ 400 and US$10,000.

Cost to secure an anti-virus software per year
The respondents were asked to indicate the amount of money used to buy effective anti-virus software. Some organizations are highly committed to eradicate CVs. Hence they invest a lot to harness the situation. Other organizations dealing with sensitive and valuable information are well protected. The range was found to be between US$ 200 – US$12,000.

Costs for securing back-ups
The respondents indicated the amount of money spent on buying back-ups to make sure that valuable data are not lost. By so doing, organizations avoid data loss due to CVs infections. Some organizations (50%) were found not to have estimation for costs to secure back-ups. Organizations that spent U$100 were about 43%, while about 7% spent between US$2,000 and US$3,000.

Value of time wasted
The respondents were asked to indicate the value of time wasted while the System Administrator resets the system. The value of wasted time ranged between US$ 10 and US$ 100 for 14.3% of the System Administrator. For 28.6% it ranged between US$ 100- US$ 500, others (14.3%) valued the wasted time to be between US$ 500 – US$ 1000. Only 7% of the respondents valued time wasted to be above US$1000. Some respondents (36%) did not estimate the value or did not respond to the question.

Assessing the existing methods, capacities and limitation of controlling CVs
Assessing the existing methods, capacities and limitations on controlling CVs was done by looking at how computers are protected from CVs. Also the study sought to know various procedures used by different organizations in CVs control. Finally, organizations capacities to fight against CVs were investigated.

Protection of Computer from CVs
Respondents indicated methods of which computers at various organizations are protected against CVs. Most organizations (50%) use anti-virus software to protect theirs computers. Other organizations (28.6%) prohibit files sharing and use anti-viruses. Some organizations (7.1%) control CVs by controlling file sharing. The study revealed that sometimes, organizations (7.1%) disconnect from the Internet in order to control the same. Lastly, the study found out that some organizations (7.1%) use anti-virus and control file sharing as well as using firewall.

Procedures to tackle CVs
Respondents were asked to indicate procedures followed to deal with CVs when their LANs are affected with CVs. It was observed that procedures used by various organizations to deal with CVs differ from each other. But, the basic point is that experts are called to deal with CVs whereby they update, repair damage and delete unsuccessful files (35.5%). Others (21.3%) disconnect from Internet, follow instructions on how to remove them, then undertake updates and scan PCs. Some (7.1%) install anti-virus software to the background in such a way that it is activated as one starts to use the computer. It was found out that other organizations (7.1%) monitor ports that are frequently attacked by hackers. Other organizations (28.4%) not responded as to which procedure they use to tackle computer viruses.

Organization capacities to fight against CVs
The respondents also reflected on organization capacities by indicating means of securing anti-viruses software. Other organizations (28.6%) were found operating their systems by using pirated anti-virus software as shown in the Figure 2. Only 14.3% organizations buy anti-virus software from software manufacturers while 57.1% buy from reliable local agents.

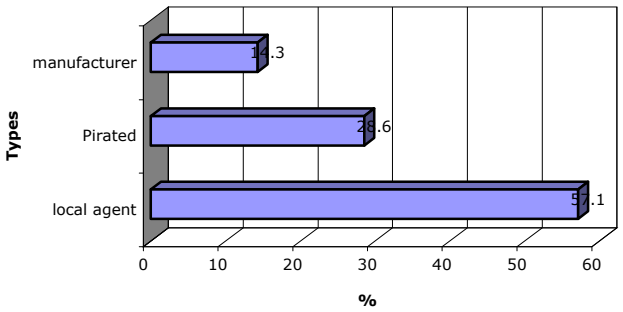

Figure 2: How an Anti-Virus on use was secured

CHALLENGES FOR CONTROLLING CVs IN TANZANIA

Shortage of funds
The total costs to deal with CVs are very high due to prior requirements needed to be in place. All computer facilities, both hardware and software, are procured from abroad. Therefore, any item required for controlling CVs means that responsible organizations should have foreign currency to be able to

purchase them. Most of the organizations in Tanzania, especially higher learning institutions do not have enough funds to deal with CVs, taking into consideration that the anti virus (AV) software are produced to last for a year. Most of the higher learning institutions in Tanzania, taken here as an example because of their intensive use of ICT, cannot manage to renew their AV software for each year. There is an alternative option of using an open source for AV software, but is not reliable.

CVs awareness

CVs awareness to other organizations is at a minimum level such that the efforts of dealing with CVs are affected by that reason of not knowing their side effects. This was reflected during this research because it was found out that some organizations do not keep records about CVs including having no staff dealing with CVs. Other organizations allow use of pirated AV software in their systems. The company policy on CVs sometimes is unclear to the users. At the same time some Systems Administrators do not have time to educate users on side effects.

Availability of the Technology

During the research, it was observed that most of the software in Tanzania environment is purchased from abroad. There are no local experts who can make/ produce AV software in Tanzania. That results in high spending of foreign currency. Also, this is another factor, which causes some organizations in Tanzania to use pirated software.

SUMMARY OF THE RESULTS

Research findings were analyzed and discussed. Mainly, the analysis aimed to know the users' awareness level on CVs; socio-economic impacts caused by CVs; assessing the existing methods and capacities and limitations on controlling CVs. The users' awareness level on CVs was tested and found higher in two areas which are, educating users and the rate of users' to understand organization policy.

To analyze the socio-impacts, the research focused on psychological factors that result from disconnecting affected LANs from the Internet. These included causing hard time to users, users getting annoyed, users getting bored, others getting frustrated, and sometimes feeling embarrassed. On socio-economic impacts, analysis revealed that various costs incurred by different organizations per year were found to be high. For example costs to replenish the affected software / hardware range between US$ 400 and US$ 10,000, costs to secure an anti-virus software range from $ 200 to US$ 12,000 and costs to secure back-ups range from US$ 100 to US$14,000. The time wasted by System Administrators for resetting systems each time of CVs attack was valued between US$ 10 and US$ 1000. Also the value of lost files due to CVs ranges from US$ 50 to US$ 500.

On assessing the existing methods, capacities and limitations on controlling CVs, the analysis focused on how computers are protected from CVs. It was found out that for half of the surveyed organizations, their PCs are protected with anti- virus. The regularly used AV software was found to be Norton and McAfee.

For procedures to tackle CVs, the research revealed that nearly half of surveyed organizations call experts, update software, repair damaged files and delete the unsuccessfully repaired files.

There were over three quarter of studied establishments that employ various methods for getting information on new CVs such as through AV magazines, mailing list, searching through the Internet sites such as www.nai.com, and others hearing from colleagues. Other organizations use pirated software to protect their system. It was found out that some of the sampled organizations buy AV software from local agents.

CONCLUSION

From the results, it can be concluded that in some organizations, CVs controls were successful since training of computer users on that aspect was emphasized. Also, use of client – server architecture to configure computer systems enabled some of the organizations to control CVs. Uses of client–server architecture enable automatic scanning of system for CVs

and hence, reduce the probability of CVs attacks. This is only possible for the organizations with licensed, corporate software. The use of pirated software caused CVs control to be ineffective. This was so because the pirated software can manage to scan only signatures of CVs available at that particular time the software was produced. That means, use of pirated software do not receive updates from the manufacturer. Thus, they fail to control more current CVs.

Other areas found not satisfactory in the process of CVs control include users' awareness. These include encouraging users to have tendencies of frequently updating the anti-virus software, letting users know reasons for keeping CVs attack records and that users should understand impacts caused by CV attacks. The use of automatic updating software such as service update software (SUS), zero - effort network and E-directory software can improve efficiency to fight against CVs.

RECOMMENDATIONS

Based on the research findings, the following are recommended in order to minimize or manage and be able to control CVs in computer systems.

- The use of client – server architecture to operate the computer systems is highly effective in CVs control. The use of this kind of architecture can successfully improve the CVs fight in Tanzania.
- Raising users' awareness on CVs can be achieved through training of users on all ICT policies, AV configuration, and CVs side effects (in case they attack).
- The use of pirated software should be discouraged in computer systems anywhere in Tanzania. Thus, use of licensed, corporate and effective AV software should be encouraged.
- Before establishment of any ICT systems by an organization, costs for CVs control should be considered at early stages.

REFERENCES

Beverly W., (2001) Economic Impact of malicious code attacks http://www.cybersecure.ca/q2.htm, Visited on 20-06-2004.

Brenton C., (1999) Mastering Network Security, Sybex Inc., Alameda, USA Pg. 355- 368.

Greek D., (2004) The real impacts of viruses: Part 1, Personal Computer World, http://www.pcw.co.uk/features/1151775, visited on 29-12-2004.

Hameed I., (2003) Common Computer Virus types, http://www.faqs.org/qa/qa-500.html, visited on 18–6-2004.

Harley D., Slade R. and Gattiker E., (2001) Viruses revealed understand and counter malicious software. Osborne / McGraw-Hill, New York, USA. Pg. xxi, 22-43, 492-518.

Hofstetetter F. T., (1998) Internet Literacy. Irwin McGraw Hill. Pg. 12, Upper Saddle River, New Jersey.

Kane P., (1989) V. I. R. U. S Protection, Vital Information Resources Under Siege, Micro Text Productions. Pg xxi. New York USA.

Marshall B., (2005) How Computer Viruses Work http://www.computer.howstuffworks.com visited on 04-01-2005.

Norton P., (1995) Norton AntiVirus TM for Windows 95 User's Guide, Systemic Corporation.

O'brien J. A., (2002) Management Information systems Fifth edition. McGraw- Hill Irwin

Olivier M. S., (1990) Computer Viruses: A Management Perspective http://Mo.co.za/open/infosec.pdf, visited on 07-01-2005.

Townsend & Taphouse, (2002) A 3i white paper in association with the economist intelligence Unit. http:// www.3i.com, visited on 24-06-2004

University Of Washington, (2004) Protect your computer from viruses http://www.washington.edu/computing/virus.html, visited on 18-06-2004.