Computer Viruses:
A Management Perspective

M S Olivier

PKOMP 90/4

TEGNIESE VERSLAG **TECHNICAL REPORT**
SENTRUM VIR GEVORDERDE REKEN- EN BESLUITNEMINGSONDERSTEUNING
CENTRE FOR ADVANCED COMPUTING AND DECISION SUPPORT
WNNR CSIR

PKOMP 90/4, 9p, Pretoria, March 1990.

Published by: CSIR
P O Box 395
PRETORIA
0 0 0 1
Republic of South Africa

Issued by: Centre for Advanced Computing and Decision Support
CSIR

Printed by: Scientia Printers

Preprint. Not for review.

This report is an account of work of which some or all was carried out at the Centre, but has not necessarily undergone the internal review accorded official CSIR publications.

Copies of this publication are available from:

Centre for Advanced Computing and Decision Support
CSIR
P O Box 395
PRETORIA
0001

Keywords: Computer Viruses, Computer Security, Management of computers

Computer Viruses: A Management Perspective

Martin S Olivier
Centre for Advanced Computing and Decision Support
CSIR

March 1990

Abstract

Most companies are aware of computer viruses, but many do not know which steps are appropriate to take against viruses. Criteria for such steps are effectiveness, cost-efficiency, minimum disruption of normal operations, fast response and integration with general computer security. This paper considers measures against computer viruses in a systematic way.

1 Introduction

The computer industry has by now become accustomed to the existence of computer viruses. Some companies have introduced policies to minimize the risk of infection from such viruses, while others still think that only people playing games or illegally copying software are at risk.

A variety of preventative measures may be taken—each with its associated cost. This cost can be direct, such as when anti-virus software is bought, or indirect when measures are introduced which affect the productivity of employees. In all cases this cost should be compared to the potential risk presented by viruses.

This paper adresses viruses and, in checklist form, those steps which should be considered by management when dealing with computer viruses.

2 Computer viruses and other unwelcome software

A computer virus is a section of code which, when executed, will attach itself to other programs in such a way that it will be executed when those programs are executed. This means that executing that program may spread the virus further. The virus usually also includes code to produce some unexpected behaviour such as displaying a “humorous” message, destroying data or even wearing out hardware.

Viruses are often classified by the type of program they infect; currently there are two such classes: boot sector viruses and file viruses. A boot sector virus infects the program which is executed during bootup of a computer. A file virus infects executable program files (ie COM and/or EXE files in MSDOS terminology). See [6] for details about the classification of viruses and a brief description of a few well known viruses; [9] also contains descriptions of known viruses.

Computer worms are similar to viruses but they do not use other programs as carriers—a computer worm is an independent program or set of programs. The best known computer worms use the email system to transfer a copy of themselves to other users (on the same system or at other sites via networks). The worm then uses some mechanism to activate this copy, after which the copy itself will start sending copies to all users in this user’s email address list. The Internet worm (see [10]) used a loophole in the email package to activate a program at a remote site; this loophole has probably now been closed at all sites so that a recurrence of this worm is unlikely. The Christmas tree worm activated a program at a remote site by asking the user to execute a program to see a christmas message; this program then displayed the message but also activated the worm distribution mechanism.

When discussing computer viruses reference is usually also made to trojan

horses and logic bombs. These programs can only be installed on a computer by a user with the proper access rights. Prohibiting the use of any software which was not purchased through the official channels and the proper selection of programming personnel should adequately address these issues. We do not discuss them further in this paper.

3 Risk assessment

There are three types of cost associated with viruses:

- Restoration of data destroyed by a virus, including labour and down-time
- Losses incurred because of incorrect results caused by a virus
- Loss of reputation if word of an infection gets out

The risk associated with each type depends on

- The viruses in existence
- The nature of business of the company involved

3.1 Existing viruses

In this section we consider only viruses that infect MSDOS computers.

When assessing the risk posed by viruses, a worst possible case scenario may be used. There is, however, a wide gap between this and the risk posed by existing viruses. It therefore makes sense to base calculations on the current situation although this requires a regular monitoring of the situation.

In South Africa are many cases of

- Bouncing Ball (or Italian; see [4], [5]);
- Jerusalem (or 1813, Israeli; see [7]); and
- Stoned (or Marijuana, New Zealand)

viruses.

Isolated cases of

- 1701 (or Cascade, Second Austrian; see [9]);
- Brain (or Pakistani; see [3], [12]); and

- Computer Ogre

viruses have also been reported.

Many more viruses have been reported worldwide but currently most problems are caused by a handful of viruses. Those viruses have all been found in South Africa except the 648 (see [1]).

Two other viruses have also been found locally. Since these viruses have not been reported elsewhere, they have been named after the cities where they have been found: Pretoria and Durban. The Pretoria Virus will change all filenames in the root directory to ZAPPED on June 16th. The Durban virus will destroy the data on disks C, B and A on any Saturday the 14th.

The viruses mentioned above will not alter data. This means that virtually no risk exist at this stage of working on incorrect data because of the presence of a virus.

Except for Computer Ogre and the Durban Virus, the viruses mentioned above do not intentionally destroy data and all can be removed fairly easily with the aid of anti-virus software packages. The number of machines, whether they are connected via networks, the number of users and the number of floppy disks all influence the cost associated with cleaning up viruses—depending on the virus, these factors can push the cost up exponentially. It is important that someone knows how to deal with viruses, because the damage caused by an incompetent person trying to remove a virus is often substantial.

3.2 The nature of business

There are a few types of business where any virus can be fatal:

- Businesses such as banks where a loss of trust by clients is a threat
- Businesses where engineers/consultants/auditors use their software on clients' machines
- Businesses which distribute software

"Open shops" like universities and bureaus where there is no control over users of a system have their own particular problems.

In other cases the importance of data to the business of the organisation determines the risk—if a computer is used only as an intelligent typewriter the potential loss is negligible; if accounting information is held on the machine, this potential is much higher; if a company's primary business depends on the information stored on a computer, this potential is extremely high.

3.3 Calculation of risk

As is the case with normal risk analysis, a "potential risk cost" can be calculated by estimating the cost associated with the different risk aspects, estimating the probability of each aspect, multiplying the costs by the probabilities and adding up. This figure represents the potential risk. The cost of any measure considered against viruses can then be compared to the decrease of the potential risk to evaluate the this measure.

The following table can be used for this calculation:

Type of risk	**Potential cost** (R)	**Probability** (%)	**Risk** (R)
Restoration Incorrect results Reputation			
Total risk			

4 Possible measures against viruses

Several measures against viruses are possible.

- Someone has to be given responsibility to deal with possible infections
- Users have to be educated about viruses
- A contingency plan should be drawn up

The responsible individual may be the system administrator in the case of a small installation or someone in the computer security section in a larger installation. In the case of a small installation this person should be aware of viruses, what the common strains do and, most importantly, know who to contact in the case of an infection. At a larger installation this individual will probably have (a selection) of anti-virus software and some experience in removing viruses. He should also know how to stop the virus from spreading. Contact with an expert on computer viruses is also recommended.

Education of users is important: users should know enough about computer viruses so that they recognise a possible infection but do not ascribe all problems to viruses. They should also know who to contact in the case of an infection and who not to contact—leaking a story to the press can be damaging.

The specifics of the contingency plan will depend on the size of the installation: In the case of a small business the following will be sufficient:

1. Contact the responsible person
2. Determine whether work may continue or should be suspended (This depends on the virus strain)
3. Decide on the disinfection plan (This may be done easily with an anti-virus software package or may require deletion of files or reformatting the disks)
4. Verify that the virus has been removed
5. Institute checks to give early warning of re-infection

A checklist for the virus section of a computer security policy is given later.

5 Viruses and the computer security policy

It is important to note that computer viruses are only one aspect of computer security. A number of the usual security measures will also help in the fight against viruses—regular backups is a case in point. The people dealing with general computer security are also the people who should deal with computer viruses.

It is important to get management's co-operation on computer security. Computer security is an overhead where benefits are not often seen; only when things go wrong is the importance noted. Managament's commitment is therefore important—it is important to budget for security; a responsible person should be appointed and it should be ensured that the policy is reviewed regularly.

6 Checklists

6.1 Contingency plan

The following serves as a checklist for the contingency plan. Not all the issues mentioned have to be included in the plan, but all have to be considered.

- Responsible person appointed
  - Budget approved to support contingency plan
  - Power delegated to enforce contingency plan
  - Person to handle problems in absence of responsible person
- Review date specified

- Action plan in case of infection
  - Users aware of reporting procedure
  - Users aware of their responsibilities (especially regarding talking about the case, continued use of machines, handling possible infections of personal computers at home, etc.)
  - Information on virus available or obtainable from an identified source
  - Anti-virus software available or obtainable from an identified source
- Risk-reducing steps
  - Applicable prevention steps selected (see following section)
  - Users educated about these steps
- Early detection of viruses possible
  - Virus scanning software available
  - Scanning policy introduced and enforced for all software entering the company
  - Users educated

6.2 Possible risk-reducing steps

- Make regular backups.
- Use write-protect labels on all diskettes that are not to be written to. (Also test all disc drives to ensure that their write-protect mechanisms work.)
- Ensure that all personnel who work on computers in other departments or organisations are informed about viruses. All diskettes that could be written to, should be tested for the presence of viruses prior to use on other computers.
- Copy programs from the original distribution diskettes only. (These original diskettes should be fitted with write-protect labels immediately after purchase.)
- If at all possible, do not allow anyone else to use your computer or to use your diskettes on other computers.

- Do not boot a computer from a diskette without good reason. (Should a computer be switched on with a diskette in the drive, resulting in the message *Not a system disk, replace and strike any key*, remove the diskette and reboot with *Ctrl-Alt-Del*.)
- Keep records of dates and sizes of a few *.COM and *.EXE files that are used regularly and check that this information remains unchanged.
- Be careful of public-domain programs and diskettes from universities and colleges.
- Do not attribute all unexpected computer behaviour to viruses—in most cases the problem is the result of a program or user error.
- Install a dual-floppy machine which may be used to scan for viruses. This machine should not be connected to any networks and the boot floppy and anti-virus software sould be write-protected and used only on this machine.

6.3 In the event of a virus attack

The following should be kept in mind by the general computer user in the event of a virus attack.

- Do not panic or take any rash action.
- Do not continue to use your computer, if at all possible, so as to provide a better opportunity for detecting the origin of the virus.
- Contact an expert—people that do not have experience of viruses can often do more harm than good.
- Notify senior management in the event of a virus attack and let them assume responsibility as to whether the attack should be publicised or not. (The news that even a harmless virus has entered an organisation can prove detrimental to business.)
- Do not make unfounded allegations concerning the origins of the virus. (It is seldom possible to identify the person responsible.)

7 Conclusion

Viruses are a fact of life. It is impossible to prevent viruses but the chances of an infection can be reduced by suitable policy. Costs incurred should be in line with the reduction in risk they offer. Viruses should be addressed formally as part of the computer security policy.

References

[1] Burger, R, “Computer Viruses—A High-tech Disease”, Abacus, 1988

[2] Glath, R M, “The Case of the “Gerbil Virus” that wasn’t”, Computers & Security, **7** (1988), 451–453

[3] Highland, H J, “The BRAIN Virus: Fact and Fantasy”, Computers & Security, **7** (1988), 367–370

[4] Highland, H J, “The Italian Virus”, Computer Fraud & Security Bulletin, **11**, 7 (1989), 7–8

[5] Olivier, M S and Teitge, H W, “Analysis of the Bouncing Ball Virus”, Technical report PKOMP 89/5, Centre for Advanced Computing and Decision Support, CSIR, July 1989

[6] Olivier, M S “Rekenaarvirusse: ’n Suid-Afrikaanse Perspektief”, Technical report PKOMP 90/1, Centre for Advanced Computing and Decision Support, CSIR, January 1990

[7] Radai, Y, “The Israeli PC Virus”, Computers & Security, **8** (1989), 111–113

[8] Rubenking, N J, “Infection Protection”, PC Magazine, April 25 1989, 193–228

[9] Solomon, A, “Dr Solomon’s Anti-Virus Toolkit”, S&S Enterprises, Amersham, 1989

[10] Spafford, E H, “Crisis and Aftermath”, Communications of the ACM, **32**, 6 (1989), 678–687

[11] Thompson, K, “Reflections on Trusting Trust”, Communications of the ACM, **27**, 8 (1984), 761–763

[12] Webster, A E, “University of Delaware and the Pakistani Computer Virus”, Computers & Security, **8** (1989), 103–105