The Impact of Computer Viruses on Society

Dr. Jimming Lin
Faculty of Administration
University of Ottawa
Ottawa, Ontario K1N 6N5, Canada

Dr. Chia-Hao Chang
Department of Industrial and System Engineering
University of Michigan-Dearborn
Dearborn, MI, USA 48128

Computer viruses have recently drawn a lot of attention because of some spectacular examples of their power of disruption. This paper discusses the impact of computer viruses on different sectors of the society. Four important perspectives of society will be discussed here:

1. The managerial perspective
2. The users' perspective
3. The manufacturers' perspective
4. The security specialists' perspective

Brief Overview

A virus is a program that can infect other programs by modifying them to include a possibly evolved copy of itself. With its infection property, a virus can spread throughout a computer system or network using the authorization of every user to inflict his/her own programs. Every program that gets infected may in turn act as a virus and thus start an endless cycle. This ability to reproduce itself combined with the numerous points of interconnection in today's computer systems makes it spread like AIDS.

Managerial Perspective

The implications of the computer virus growth are especially important for management information systems (MIS). Management is becoming more aware of the security considerations and internal policies of the firm. In order to prevent system contamination, employees should be warned not to use any unchecked programs. The MIS management should set more straightforward policies and the repercussions of not abiding by them. Similarly, any software used in the office should remain there and no place else. This is to safeguard against possible infections that could occur outside of the office environment. The focus of most policies will be on preventing external intrusions rather than internal threats simply for the sake of reducing external dangers.

Management should also emphasize better education and training of its workers. It might be worthwhile to expose them to virus attack simulations during their training period. This

will dramatize the importance of security issues by showing how all the valuable data, programs and even hardware of the users can be tapped by a virus. The computer virus, as a training tool, would help users understand the dangers inherent in program and data exchange.

Although the control mechanisms are important, management should not overreact to the virus threat and thus suffocate end users' innovations. The manager must strike a balance between the benefits of information exchange and the isolation of computer systems.

Users' Perspective

The impact of computer viruses upon the users could be severe. The initial impact may be a trend towards software development that is bulletproof rather than user friendly. With more complex software, the result could be a longer learning curve for new users.

The interchange of programs on "Bulletin Boards" is also affected by the virus epidemic. This cheap source of new programs has dried up as more and more people become concerned with potential contamination. A similar decline has taken place in second-hand or borrowed software as the "fortress mentality" sets in.

With the decline of borrowed or pirated software, there is a sign of growth in the sales of programs at some reputable, safe retail outlets. People seem to be willing to trade some cost for an increased sense of security with their programs.

Users may protect themselves by fully understanding their equipment and the process by which computer viruses operate. The best way for users to protect against viruses and other personal computing hazards is through education. Users require good knowledge of DOS to realize the seriousness of the problem and to understand the risk involved when those DOS-related problems arise. Common sense and a healthy dose of caution will go a long way towards protection against viruses.

The immediate effect on users of the new cautious environment is putting an end to the uninhibited program swapping that made the early days of the computer revolution so exciting. Just as the threat of AIDS has made people become cautious of casual sexual behavior, the computer virus may also restrain the development of software pirating.

Manufacturers' Perspective

Besides the development of vaccines and antidotes, the software manufacturers may see the computer virus as a potential marketing tool. By providing warranties or guarantees to the purchaser against the existence of viruses in their software, they believe that they can eradicate the pirates and copycat vendors who are cannibalizing their markets.

Vicious software developers may use viruses as a selective predator, targeting only software or hardware sold by specific vendors. With the rapid spread of PC-to-mainframe linkages, those malicious developers may use viruses to attack competitors without leaving a trace.

As manufacturers grapple with the threats and opportunities posed by computer viruses, they must also deal with the plethora of legal ramifications that will eventually follow.

Computer Security Specialists' Perspective

The growing need for computer security specialists is predictable. Consultants may earn enviable income by telling corporate computer users how to protect their machines from catastrophic failure and how to use antidote and vaccine products.

The computer specialists will be in a never ending game with each other. As they develop preventive vaccines and administer the viral antidotes, the viral breeders will also be developing new viruses to overcome the new security measures. The phenomenon will be exactly the same as the situation in disk copy and protection in the past few years.

The problems of computer security specialists are compounded by the existence of fake antidotes. These antidotes appear to cure the program but in fact implant a new virus. Recently, a more dangerous retrovirus has emerged to give security personnel real headaches. The retrovirus remains even after the computer memory has been erased.

Rather than contracting a Germany company to build a gas plant, it is much easire for terrorist groups to hire a computer specialist to build virus programs that will attack airplanes, banks and national defense. Computer specialists, especially those who develop the military system, should be very carefully screened.

Some terrorists blackmail victims by inserting a "time bomb" virus into a system and then demand payment. The emergence of virus hoaxes should appear shortly, as malicious pranksters phone in with threats of viruses. Since the use of viruses is difficult to prove, this opens up a new field of legal repercussions and costs for the company.

Conclusion

This paper has considered each stakeholder in the computer industry who may have an interest in the activities of computer viruses. Managers will have to compromise between innovation and control. Users may have to be more cautious of software pirating. Manufacturers must recognize the opportunities and threats of computer viruses as a marketing weapon. Security specialists face a never ending battle against virus creators trying to overcome their security measures, antidotes and vaccines. These are just a few of the impacts that can be expected on the computer industry. For the computer society, the computer virus has become a fact of life.

References

Cohen, F., 1984, "Computer Viruses: Theory and Experiment", University of Southern California, July.

Elmer-Dewitt, Philip, 1988, "Computer Viruses", *Time Magazine*, September 26.

Dvorak, J.C., 1988, "Virus Wars Ahead", *PC Magazine*, November 15, 1988, p. 71.

Finch, J.H. and Dougall, E.G., 1984. *Computer Security: A Global Challenge*, Elsevier Science Publishers, Amsterdam.

Hadler, E., 1982. *Computer Security Handbook*, Brandon Publishing, New York, New York.

King, S., 1988, "Computer Viruses: Detection and Vaccination", *CGA Magazine*, October.

Ludlow, R., 1988, "Electronic Epidemic: Computer Viruses Can Put Whole Networks Under the Weather", *The Ottawa Citizen*, November 5, p. 1-2.