1992

An Investigation of IBM PC Computer Viruses Infection Rates and Types in a Western Australian Environment

Boon Guan Lee
Edith Cowan University

1992

An Investigation of IBM PC Computer Viruses Infection Rates and Types in a Western Australian Environment

Boon Guan Lee
Edith Cowan University

Edith Cowan University

Copyright Warning

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

An Investigation of IBM PC Computer Viruses Infection Rates and Types in a Western Australian Environment

By

LEE, Boon Guan

[redacted]

A Dissertation Submitted in Partial
Fulfilment of the Requirements for the Award of
Bachelor of Applied Science (Information Science) Honours

at the Department of Computer Science
School of Information Technology and Mathematics
Faculty of Science and Technology
Edith Cowan University
Perth, Western Australia

Supervisor:
Associate Professor Anthony C. Watson

Date of Submission: July 7, 1992

Declaration

I certify that this thesis does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.

Signature

Date July 7, 1992

Acknowledgments

Foremost, I wish to thank Associate Professor Anthony C. Watson, my supervisor, for his advice, on-going encouragement, insightful comments and suggestions, professional assistance, and for giving me access to his vast collection of computer virus papers.

I am grateful to Dr. Pender Pedler of the Department of Mathematics for his technical assistance in designing the questionnaire for the survey. I wish also to acknowledge the help of Mr. Jürgen Hinrich and Mr. Peter Austin, both from the Division of Information Technology, who went through with me patiently in field-testing the questionnaire prior to the commencement of the survey.

Special personal thanks go to the reviewers of the earlier drafts of this thesis.

And finally I am deeply grateful to my parents for giving me the opportunity to complete my education, and for their unwavering love and support.

Trademark Acknowledgments

Every reasonable attempt has been made to supply trademark information about company names, products, and services mentioned in this paper. Trademarks indicated below were derived from various sources. The accuracy of this information cannot be attested.

- 3+, 3+Open are trademarks of 3Com Corporation; 3Com is a registered trademark of 3Com Corporation.
- Apple, Apple II and Macintosh are registered trademarks of Apple Computer, Inc.
- Amiga is a registered trademark of Commodore Business Machines Inc.
- Atari, Atari ST are registered trademarks of Atari.
- LANTastic is a trademark of Artisoft, Inc.
- UNIX is a trademark and AT&T is a registered trademark of AT&T Bell Laboratories.
- DEC is a registered trademark and VAX is a trademark of Digital Equipment Corporation.
- IBM AT, IBM PC, IBM XT, IBM Personal System/2, PC DOS are trademarks of International Business Machines Corporation; IBM, IBM PC Network, LAN Manager, OS/2, PS/2 are registered trademarks of International Business Machines Corporation.
- Microsoft and Microsoft 3COM Lan Manager are registered trademarks and MS-DOS is a trademark of Microsoft Corporation.
- VINES is a registered trademark of Banyan Systems Inc.
- NetWare, and Novell are registered trademarks of Novell, Inc.

Abstract

In recent years computer viruses have become increasingly significant as a form of computer abuse. By virtue of their reproductive capability, computer viruses can have cumulative and potentially catastrophic effects to the many people who use those affected computers. There is a growing concern in the computing community about these forms of electronic vandalism. This concern arises from the possible damage to stored information on which the work depends and the ensuing disruption of the work-place.

Although the vandalism or purposeful abuse by introducing computer viruses to computer systems was originally mainly an American experience, research reports published by the Australian Computer Abuse Research Bureau (ACARB) support the claim that computer viruses have become increasingly significant as a form of computer abuse in Australia in recent years. Apart from ACARB's figures, there is minimal empirical research of a similar nature being conducted to investigate computer viruses as a form of computer abuse in Australia. In this study, an attempt has been made to investigate the problem, albeit on a limited scope.

In this study, the infection types and rates of IBM PC viruses in limited government IT organizations in Western Australia were investigated. In addition, this study has made an attempt to validate Spafford's speculation that less than 10 viruses (out of a minimum of 374) account for 90% of infections in the Western Australian environment.

This study was descriptive in nature in that a fact-finding survey based on questionnaires and standardized interviews was conducted in State Government IT organizations in Western Australia in order to obtain data on which the research

findings can be based. The data gathering instrument for this study was a standardized questionnaire which comprised limited choice questions directed at obtaining such information as infection rates of various types of computer viruses. The questionnaire was field tested to eliminate ambiguous or biased items and to improve format, both for ease of understanding and facility in analyzing results. The questionnaire was used by the interviewer as a basis for the interview so that the potential for subjectivity and bias can be reduced.

Before the commencement of this study, a letter of transmittal was sent to the prospective participants in order to request their participations. Confirmation of participation was sought through telephone calls. A very high response rate (87.5%, n = 42) for this study was achieved. This is taken as an assurance that reasonable representation of the state government sector for the study is achieved.

Prior to commencement of this study, approval was sought from the University Committee for the Conduct of Ethical Research since this study will involve human subjects. During the interview, subjects were informed of the purpose of the study, that there will be no compulsion to participate in the study and that they will be free to withdraw from further participation in the study at any time they desire.

The results of the survey and its implications are provided in chapters 5 and 6. In conclusion, the research ratifies the proposition that currently very few of the IBM PC viruses contribute to the vast majority of infections in the Western Australian work-place.

Table of Contents

Table of Contents
[cont.]

Table of Contents
[cont.]

Table of Contents
[cont.]

List of Figures

List of Tables

List of Tables
[cont.]

Page

Tables

List of Tables
[cont.]

Chapter One

Introduction

1.1 Background to the Study

1.1.1 Computer viruses as a form of computer crime[1]

Computers potentially offer a tremendous advantage in providing accurate and timely information for making decisions, but their accessibility and proliferation can

---

1 This paper commences with the proposition that deliberate development of a computer virus for *computer abuse* with malicious intent is a form of *computer crime*. Although this position is dependent upon the laws of the country in which the action takes place, it is reasonable to take the majority position which would describe the action as *criminal* since the activity is not contained within country boundaries.

It should be noted that there are subtle differences between the terms "computer crime", "computer fraud" and "computer abuse". For example, unlike *fraud* the release of a computer virus is unlikely to cause financial gain to the culprit. Indeed, there have been examples of computer viruses being released without deliberate intent to perform damage, as pointed out by Leiss (1990, p. 37). Nevertheless, the final outcome on the victim is still the same.

Notwithstanding, it is beyond the scope of this paper to made an attempt to differentiate the exact delineation between these terms. Thus, in the remaining of this paper, these terms will be used interchangeably.

pose major security problems. Since the first documented computer crime case in 1958 (Parker, 1976, p. 34), the fraudulent misuse of computers, according to Palmer & Potter (1989, p. 14), is now a major criminal activity.[2] Not only has computer fraud increased in frequency, it has increased in sophistication as well. Today, the computing community is dealing with what the *New York Times* vividly

2 For example, a "Commitment to Security" survey of 3,500 computer security professionals conducted by the National Centre for Computer Crime Data (NCCCD) in the United States in 1989 revealed that the annual cost incurred as a result of computer abuse in the U.S. is estimated at $5.5 billion, 930 person years, and 15.3 computer years ("News track", 1989, p. 657; Bloombecker, 1989; Baker, 1991, p. 4). The average annual known computer abuse losses from the assessable cases are $109,000, 365 person hours, and 26 computer hours. NCCCD data has previously noted that 45% of reported cases of computer crime in the U.S. are computer-related fraud (Bloombecker, 1988).

Statistics from the Financial Crimes Unit of the Federal Bureau of Investigation (FBI) suggest, however, a higher average cost per incident of $430,000, with annual losses in the U.S. estimated at $100 billion (Kamay & Adam, 1990, p. 10). As for Australia, data gathered from the Australian Computer Abuse Research Bureau (ACARB) indicate that from 1978 to May 1990, the average annual known computer abuse losses from 151 assessable cases in Australia is $100,749 (Kamay et al., 1990), as shown in Table 2.

A survey carried out by BIS Applied Systems Limited, a computer consultancy firm in the United Kingdom, indicated that the average amount defrauded per incident in the U.K. has increased from £31,000 in 1983 to £262,000 in 1986 and then to £483,000 in 1989 (Wong & Watt, 1990, p. 35). This represents a 15-fold increase in value over the three periods. The maximum loss recorded has also gone up from £500,000 to £10 million and then £27 million over the three periods.

calls "the letter bomb of the computer age: computer viruses"[3] ("Letter bomb", 1988). With the advent of electronic mail, computer viruses have become more than the letter bomb of the computer age, as bemoaned by Zajac (1988, p. 3), "they have become a global threat."

It seems evident (Fites, Johnston, & Kratz, 1992, p. 11; Kamay et al., 1990, p. 17; Denning, 1990, p. xiv; Leiss, 1990, p. 4) that the real reason why computer viruses are becoming a serious problem, and could be catastrophic in the future, is linked to one of the long-term trends in the development of computers: connectivity.[4]

The following well-publicized incident (Denning, 1989; Rochlis & Eichin, 1989; Spafford, 1989; Markoff, 1988; Eisenberg, Gries, Hartmanis, Holcomb,

---

3 A computer virus is generally defined as a set of instructions, usually attached to the beginning or end of a program file, that propagate themselves through computer systems and/or networks, deliberately set to do things unwanted by the legitimate owners of those systems. (See section 1.1.3 for a definition of a computer virus.)

4 The advent of networking, especially local area networks (LANs), in the second half of the 1980s had far reaching consequences. The systems software (e.g., file systems, operating systems) of PCs was basically designed with a single user in mind. As soon as PCs were connected to each other (and to minicomputer or mainframe, or both), this single-user world view was shattered; yet the operating systems of many personal work stations did not change drastically. On the one hand, networking was added to enhance the functionality of the older systems, on the other hand, even newer systems sometimes ran older systems software, usually for reasons of compatibility. "As a result," Leiss (1990, p. 7) argues, "safeguard against (accidental or malicious) undesired changes of data and software ... are substantially inadequate." Leiss (1990, p. 9) goes on to add that "many problems stemming from virus attacks can ultimately be traced back to this change in the computing milieu."

Lynn, & Santoro, 1989; Montz, 1990a; Gardner, 1989; Ferbrache, 1990) is edited from the above sources to illustrate the extent to which *connectivity* has exacerbated the computer viruses problem.

On November 2, 1988, a graduate student at Cornell University released a "worm" program[5] into ARPANET (Denning, 1989/1990; Quarterman & Hoskins, 1986/1990, p. 42), a North American academic networking system that includes electronic mail capabilities. Within hours, it had spread to several thousand computers attached to the ARPA Internet.[6] Over an eight-hour period the worm invaded between 2,500 and 3,000 Digital Equipment Corporation's VAX computers and Sun Microsystems' Sun 3 systems running the Berkeley and AT&T UNIX operating system version 4.3 at such major Internet sites as Massachusetts Institute of Technology (MIT), the University of California at Berkeley, three National Aeronautics and Space Administration (NASA) facilities, and Lawrence Livermore National Laboratory.[7] The scope of the break-ins came as a great

---

5 The program may not be a virus by the definition used in this paper, but rather a form of *worm*. The difference is academic: the program did not attach itself to any other program while spreading, it only sent copies of itself through a mail system, and is thus not a *computer virus* in the strictest sense. See the next section for the discussion of a worm.

6 The ARPA Internet (Quarterman & Hoskins, 1986/1990, p. 40) is an internetwork of several networks, of which ARPANET is the oldest. Internet exists to facilitate sharing of resources at participating organizations and free exchange of research findings among researchers through electronic mail and other services, as well as to provide a testbed for new developments in networking.

7 This machine base was a small subset of the hosts connected to the Internet. Ferbrache (1990, p. 14) argues that the diversity of Internet host platforms was a significant factor in reducing the spread of the worm. Had Morris extended his attacks to the common Sun

surprise to almost everyone, despite the fact that UNIX has long been known to have some security weaknesses, as discussed in Grampp & Morris (1984) and Reid (1987).

Computers infested with the worm were soon labouring under a huge load of programs that looked like innocuous "shell" programs (command interpreters.) The worm program expropriated the resources of each invaded computer by replicating rampantly and clogging them with many copies of itself, but did no apparent damage. Attempts to kill these programs were ineffective: new copies would appear from Internet connections as fast as old copies were deleted. Many of the computers had to be disconnected from the network until all copies of this prolific worm program could be eradicated and the security loopholes the worm used to gain entry could be plugged. The worm program had done no permanent damage to stored files or programs, but its disruptive spread had cost hundreds of hours of human effort and computer time.[8]

386i and Sun 4 systems, Ferbrache (1990, p. 14) maintains, the impact of the worm would have been far greater.

The immediacy of communication, the ability to copy source and binary files from machine to machine, and the widespread availability of both source and expertise allowed personnel throughout the U.S. to work together to solve the infection despite the widespread disconnection of parts of the network are some other factors perceived by Spafford (1989) that have helped to defeat the worm.

8 Estimated losses from individual sites are generally not available. However, NASA's Ames Research Centre and the U.S. Department of Energy's Lawrence Livermore National Laboratory estimated their dollar losses at $72,500 and $100,000, respectively (Montz, 1990b, p. 457). These losses were attributed primarily to lost staff time. Report from the NCCCD (cited in Adams, 1989, p. 10) points out that the cost of cleaning out

This incident gained much publicity[9] and reactions[10] in the computing community perhaps because it highlights the subtlety and danger of attacks by

systems in just one user organization, the Los Alamos National Laboratory, was estimated at US $250,000.

9 The worm's fast and massive infestation was so portentous that the *New York Times*, the *Wall Street Journal* and *USA Today* gave it front-page coverage. It was the subject of two articles in *Science* magazine (Marshall, 1988a, 1988b). These accounts said that over 6,000 computers were infested, but later estimates (Denning, 1989, p. 126) put the actual number between 2,500 and 3,000, about 5% of those attached to the Internet.

10 Shortly after the Internet incident, several major groups issued public statements decrying the incident, calling for more responsibility by network users and citing as unethical any disruption of the intended use of networks, wasting of resources through disruption, destruction of computer-based information, compromising of privacy (Farber, 1989; Cerf, 1989). These groups include the board of directors of the CSNET and BITNET networks, the advisory panel for the division of networking and research infrastructure at the National Science Foundation, and the Internet Activities Board. The president of the Association for Computing Machinery (ACM) at the time of the Internet incident called on the computing community to make network hygiene a standard practice (Kocher, 1989, p. 6).

In the aftermath of the Internet incident the U.S. Department of Defence (DoD) established the Computer Emergency Response Team (CERT) at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh. The CERT was established to assemble a network of experts to monitor attacks on computers, coordinate responses, and issue advisories. The CERT deals with attacks of all kinds, including intruders, worms, and viruses (Scherlis, Squires, & Pethia, 1990, p. 498). Similar organizations have been established by the U.S. Department of Energy (*Computer Incident Advisory Capability*), the U.S. Defence Data Network (security co-ordination

computer viruses and worms on computers attached to *open networks*[11]: the potential for loss of valuable information was enormous, and an actual loss may have been devastating to the many people who used those computers. The occurrence of this incident has prompted Fites et al. (1992) to assert:

> It is no longer true that computers are reasonably safe from each other. . . . Connectivity means that . . . we're all susceptible to attack. (p. 26)

The attacks on computers *not* attached to networks by viruses could prove to have equally disastrous consequences because viruses restricted to personal computers (PCs) have also infected computers on a global scale. The **Brain** virus, for example, is reported (e.g., Hafner, 1988, p. 53; Grocott, Palmer, & Travis, 1990) to have infected an untold number of PCs as it travelled throughout the world.

Computer viruses (and related threats) are thus a form of *computer crime* that is arguably more insidious than any other because of the *sheer* number of computers and people that could be affected, the anonymity of the perpetration, and the often apparent absence of reason on the part of the perpetrator. By virtue of their reproductive capability, computer viruses can have cumulative and potentially catastrophic effects to the many people who used those affected computers.

---

centre) and by NASA (SPAN network centre), according to Ferbrache (1990, p. 17). Each co-operates closely in exchanging information on known security problems.

11 Denning (1989, p. 128) maintains that since the Internet is designed for openness, it is impossible to draw conclusions about closed networks from this incident.

1.1.2 Computer viruses and related threats

Before proceeding further, it should be noted that several other terms are often used in discussions about computer viruses. The terms include: Worm, bacteria (rabbits), Trojan horse, logic bomb, and trapdoor (backdoor). These are terms that are often used interchangeably with computer virus by the layman.[12] To the general reader the difference between these types of computer virus may be slight but to the technician they are significant and reflect a position on definition. Thus it is worth giving brief explanation of these terms.[13]

A worm[14] is a software program that can run on its own, in contrast to a virus. The worm is generally designed to search for idle computer memory; it then

---

12 For example, in the Internet incident, some of the media reports (e.g, Markoff, 1988; Jackson, 1988; Alexander, 1988) have mistakenly called the invading program a virus rather than a worm. Denning (1989, p. 127) argues that the mistaken use of terminology in this incident has "exaggerated the seriousness of what had happened" because the worm is a less insidious attack (when compared to a virus), given that "the security weaknesses in the Internet service programs have been repaired" shortly after the attack and that "it is unlikely that an attack against these specific weaknesses could be launched again."

13 The reader is referred to the papers written by Murray (1988), and Rochlis et al. (1989) which contain extensive discussions about terminology, the differentiation between terms, and the appropriateness of calling a computer virus a virus.

14 Some observers (Denning, 1990, p. 192; Shoch & Hupp, 1982, p. 172) suggest that the concept that a worm that would "invade other computers and perform acts directed by its owner" originated in John Brunner's (1975) science fiction novel, *The Shockwave Riders*, in 1975. In the computing community, the first worm programs were implemented in the network of Alto workstations at the Xerox Palo Alto Research Centre in the early 1980s (Shoch et al., 1982). Their authors, John Shoch and Jon Hupp,

rewrites itself successively through the computer's memory until the computer is exhausted and the system crashes. The worm also differs from the computer virus in that it does not insert itself into other programs. It travels over network connections to establish itself on other machines.

The Bacteria, or *rabbits*, are worms which cannot use networks to travel. They do not alter existing code but reproduce until resources are exhausted. If a system becomes clogged with a bacterium it should be closed down and restarted from known 'clean' program sets. The most common form of this problem is actually a bug which causes some program to self-propagate without limit.

A Trojan horse, like a virus, is a section of code embedded within a legitimate application that performs operations unknown to and unwanted by the user. It is a special case of a virus and possesses the same properties, except the ability to replicate itself. The unauthorized code may or may not direct the legitimate program to cause damage to the system. The Trojan horse may be activated immediately or may continue to operate as legitimate software for an extended period of time before activating itself (see logic bomb).

A logic bomb or a *time bomb* is a set of instructions that are executed in conjunction with a predetermined event. The "trigger" is often a specific date or time (e.g., April Fool's Day, Friday the 13th). The logic bomb has a legitimate use in demonstration copies of software and as a form of copy protection. A virus or Trojan horse may also contain a logic bomb.

The trapdoor, also known as the *backdoor*, is a section of code inserted into a program which allows some particular security mechanism to be avoided,

---

intended them to replicate and locate idle workstations for temporary use as computer servers; Shoch et al. saw that the worms could easily go out of control and disable the workstations and the network. Their hopes for benign uses of worm programs were not realised in the years following, as demonstrated in the Internet incident.

thus allowing unauthorized or unmonitored access. It has a legitimate use in the debugging of software. A virus or Trojan horse may implant a trapdoor in the system.

1.1.3 A matter of definition

To define a computer virus in such simple terms as "a parasitic form of computer code which has the particular characteristic of being able to reproduce itself" (al-Dossary, 1990, p. 131) is oversimplifying its attributes and "is not acceptable to the computer community," in the words of Highland (1990, p. 1). To avoid this danger this paper uses the following definitions. The reason for the inclusion of these definitions is not to be comprehensive, but to emphasize that there is not one definition of the term currently agreed upon.

> A "computer virus" is a program that can "infect" other programs by modifying them to include a possibly evolved version of itself. With this infection property, a virus can spread to the transitive closure of information flow, corrupting the integrity of information as it spreads . . . . Viruses can act as carriers of [any code the attacker wishes to use] and thus can be used to cause arbitrary [changes in programs and data.] They can carry other attacks along with them, and thus by-pass many of the mechanisms that would otherwise protect against these other attacks. (Cohen, 1984, 1988)[15]

> Virus: (1) A variation of Trojan horse. It is propagating (attaching itself to files, programs) with a triggering mechanism (event, time)

15 Dr. Frederick B. Cohen, whose research in computer viruses was first published in 1984, prepared this definition for the April 1988 issue of *Computers & Security*.

with a mission (delete files, send data). . . . (2) A section of code introduced into a disk operating system for malicious purposes. At some stage the inserted code will trigger a process that will eliminate all files from the disk. The effects of the virus can extend to many users. A disk containing the virus is loaded into a computer, and it resides in computer memory. The virus detects when a new disk is loaded into the system and then writes itself onto that disk. (Longley & Shain, 1989, p. 360)

[A computer virus is] program code, usually attached to the beginning or end of a program file, which contains the following:

(1) A part which is responsible for self-replication, i.e., which causes propagation of the virus by copying the entire virus code (or a modified version thereof) to other program files (or to some other region of a disk) at certain opportunities (usually upon execution of the already-infected program or execution of the to-be-infected program).

(2) A part which performs some action (often a destructive action on files or on entire disks) when a certain event takes place (e.g., upon execution of an infected program on a certain date or after the virus has replicated itself a certain number of times). (Radai, 1989, p. 111)[16]

A true [computer] virus is a set of instructions, programmatic or otherwise, that propagate themselves through computer systems and/or networks, deliberately set to do things unwanted by the

16 Yisrael Radai prepared this definition for the April 1989 issue of *Computers & Security*.

> legitimate owners of those systems. Key to this definition is that introduction of a virus as a deliberate act, not a technical malfunction, implying an actively hostile human intelligence behind the virus. The harm viruses [could cause] may be no more than denying use of a computer to its owners, or the complete and irretrievable loss of data and software. The potential for damage cannot be quantified, but it is unlimited in scope. (Ross, 1989)

The ability to replicate itself, the infection of other programs, the attachment to another program, the idea of a carrier and the notion of performing an unexpected function are the common functions included in these definitions.

The debate about the definition of a computer virus will probably continue. It would be difficult to express the nature of this problem more eloquently than in the words of Leiss (1990):

> It should be kept in mind ... that this area of computer security is still quite young; consequently there continue to be disagreements among researchers about the precise delineation between certain terms. (p. 29)

Dr. Harold Joseph Highland (1990, p. 27), founding editor and editor-in-chief of the international professional journal, *Computers & Security*, adds further weight to this argument by stating that currently it does not appear likely that computer scientists will agree upon an "official" definition of the term.

1.1.4 History of computer viruses

There are some who claim that the idea of a computer virus was born in the earliest days of the computer era. Elmer-DeWitt (1988, p. 65), for example, argues that it was computer pioneer John von Neumann who laid out the basic blueprint of an

electronic virus in a 1949 paper titled "Theory and organization of complicated automata." There are others (e.g., Zajac, 1990, p. 25; Fitzgerald, 1989, p. 43; Simons, 1989, p. 114) who consider computer viruses as the offspring of Frederick B. Cohen.[17] Still other people (e.g., Adams, 1989, p. 3) maintain that computer viruses have their origin in the "hacker" cultures of such premier American technological universities as MIT, Carnegie-Mellon and California Institute of Technology.[18]

---

17 For his doctoral dissertation for the University of Southern California, Cohen (1986) created a virus in an effort to find a way to defend against self-replicating programs. Cohen (1984) first made his research public at the 1984 National Computer Security Conference. He made his findings known to an international audience during his presentation that same year at the International Federation for Information Processing Computer Security Conference (IFIP/Sec'84) in Toronto, Canada in September 1984. It was established that a computer virus could infect some systems in a few minutes. A massive new computer security issue was soon apparent.

18 In his Turing Award Lecture, Thompson (1984) discusses how computer science students would amused themselves by inventing games that could reproduce an exact copy of itself. One of these was a series of games called *Core Wars* (Dewdney, 1985; 1987; 1989) that involved programs that went to war against one another - the winner being determined by the program that grew and outliving the others. What Thompson is describing is a virus, a program that can effectively reproduce itself to include possibly some evolved version of the original. To the dismay of his colleagues, Thompson (1984, p. 761) not only revealed the existence of the computer viruses in the lecture, but went on to show the audience how to make them: "If you have never done this, I urge you to try it on your own." Elmer-DeWitt (1988, p. 64) maintains that the revelation was further compounded by Dewney's landmark article in the May 1984 issue of *Scientific*

Nevertheless, it appears (Spafford, Heaphy, & Ferbrache, 1989/1990, p. 318) that computer viruses were being written by other individuals, although not named as such, as early as 1981 on early Apple II PCs. Some early Apple II viruses included the notorious **Festering Hate**, **Cyberaids**, and **Elk Cloner** strains. Spafford et al. (1989/1990, p. 318) maintain that the **Elk Cloner** virus was first reported in mid-1981.

1.1.5 The (In)famous "Trio"

It was not until the fall of 1987 that computer viruses began to command world-wide attention in the popular press as well as in the trade and technical press. Late in 1987 computer viruses struck at two universities in the U.S. and one in Israel.

The **Brain** virus first appeared on the campus of the University of Delaware in October 1987 (Webster, 1989). A few weeks later, the **Lehigh** virus

---

American, which described Core Ware and offered readers who sent U.S. $2 for postage a copy for guide-lines for creating their own viral battlefields.

In March 1985, *Scientific American* published a letter in its Computer Recreations section from two programmers that established a blueprint of a PC based computer virus. According to Dewdney (1985), Roberto Cerruti and Mario Morocutti of Brescia in Italy were inspired by the description of core wars:

> Mario thought to write a program capable of passing from one computer to the other like a virus, and 'infecting' in this way, other Apples. But we were not able to conceive it until I realised that the program had to infect floppy disks . . . . We decided that after 16 self reproducing cycles, the program should decide to re-initialize the disk immediately on bootstrap. Now, the awful evil of our idea was clear, and we decided never to carry it out, nor to speak to anybody about the idea. (p. 16)

was discovered at Lehigh University in Pennsylvania (van Wyk, 1989). In December, the Hebrew University at Jerusalem found itself attacked by a computer virus (Radai, 1989). In order to discover how the virus works and precisely what it does, a group of students in the Computer Science Department of the Hebrew University disassembled the virus code and began to study it and found the **Jerusalem** or **Friday the 13th** virus.[19]

Since the outbreak of these three incidents, the media have run numerous stories about break-ins, worms, and viruses and been somewhat sensationalised as a consequence.[20] The number of incidents has been on the rise ever since. There is a growing concern in the computer community about these forms of electronic

---

19 These three viruses can be broadly categorised into two different types. The **Brain** virus was a *boot sector* infector. The **Lehigh** virus and the **Jerusalem** viruses were *executable program* infectors. The former attached itself only to COMMAND.COM; the other two viruses infected .EXE and/or .COM programs.

The three viruses also differed in the way the media is attacked. Aside from the **Lehigh** virus that infected both floppy disks and hard disks, the others only infected floppy disks. The **Brain** sometimes destroyed several sectors of a disk but often did little more damage. The **Lehigh** virus, depending upon its host, would wipe out an entire disk after a set number of DOS operations.

The **Jerusalem** viruses were replicators, causing an increase in the size of program. Although most viruses will not reinfect a previously infected program, the coding of one of the **Jerusalem** viruses was defected. It permitted the reinfection of an infected program. Because of the viral infection some programs were unable to be executed since there was insufficient memory. In other cases there was a substantial increase in program execution time.

20 For example, it was argued (Highland, 1988; Simons, 1989, p. 115) that in a rush to get stories into print some misinformation, unfortunately, were included.

vandalism. This concern arises from the possible damage to stored information on which the work depends and the ensuing disruption of the work-place. The danger of attacks by computer viruses on computers, however, is not confined to destruction or modification of data only, as shown in section 1.1.6.

1.1.6 Risks posed by viruses

The range of threats posed by viruses is limited only by the imagination and lack of ethics of their creators. According to *The Computer Virus Handbook* (n. d.), a guide written by Price Waterhouse professionals in the U.S. and U.K., some of the risks posed by viruses include the following:

> **Loss of Life.** In a real-time system (e.g., airline traffic control system) the attack of a computer virus can be life threatening. In the case of the penetration of the Lawrence Berkeley Laboratory Computer, the intruder entered a computer used in real-time control of a medical experiment (Stoll, 1988). Had he not been detected in time, a patient might have been severely injured or even killed.

> **Destruction or Modification of Data.** In the first conviction for a virus crime, a disgruntled employee at a Texas-based securities trading and insurance firm planted a program that systematically deleted sales commission records every month (Wong & Watt, 1990, p. 63; Wilding, 1990a, p. 4; Hafner, 1988, p. 50; Elmer-DeWitt, 1988, p. 63). In this manner the *logic bomb* erased 168,000 client records. The company was fortunate in that the crime was detected after only two days. Still, the company had to spend considerable time, effort, and money rebuilding its damaged database.

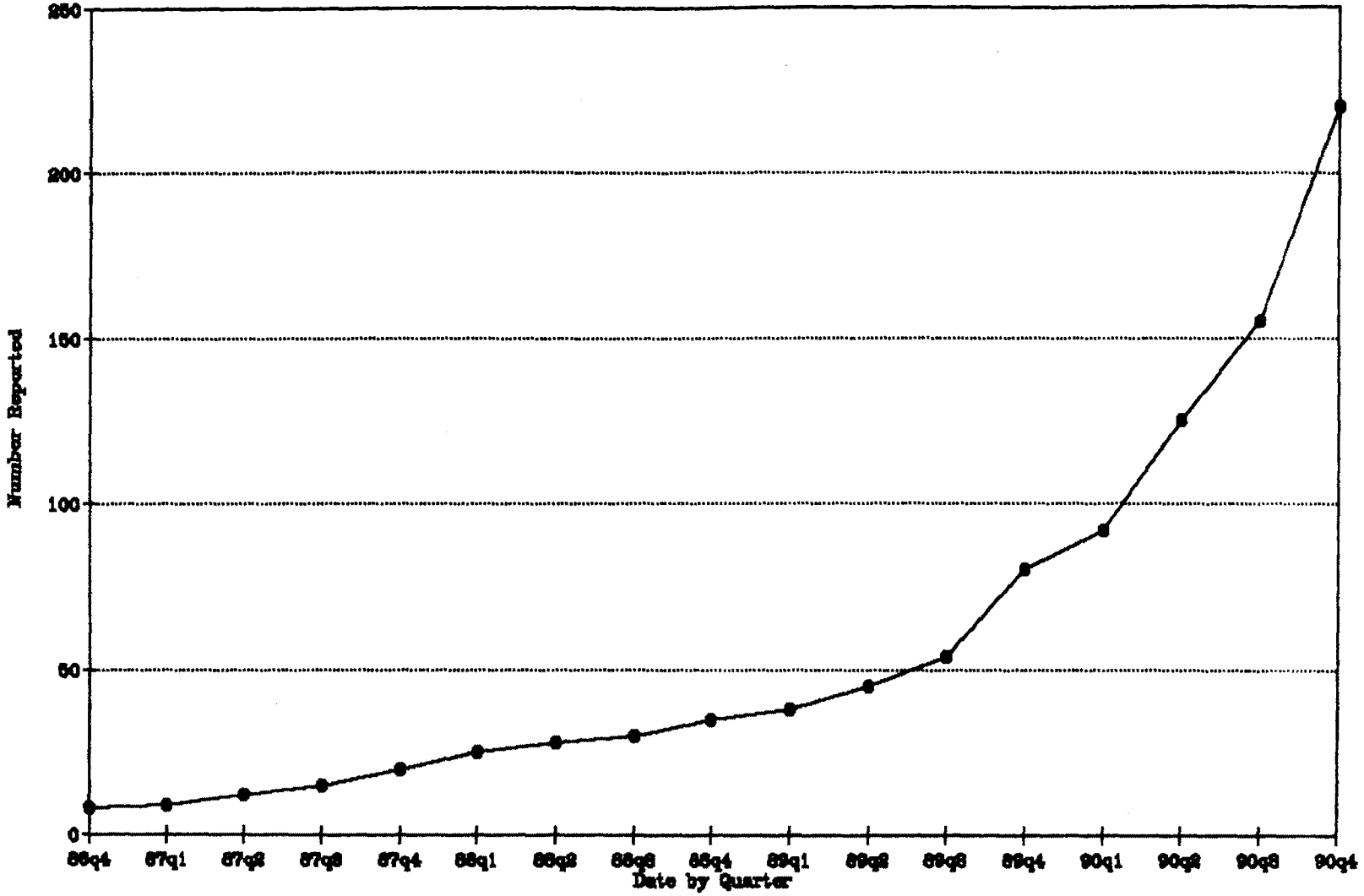
Interruption of Operations. The most significant secondary effects of a virus are those that involve lost productivity. Computer support personnel will be involved with the tasks of recovering or recreating lost files, programs, or data; removing the virus; diagnosing the problem; and developing preventive measures. Management time may be required to re-establish the confidence of customers/shareholders and to formulate procedures that will reduce the risk of future virus attack. Internal and external auditors may have to demonstrate to the audit committee and senior management that adequate audit procedures were used during the examination.

Embarrassment. Attacks of computer viruses at universities have been well documented (e.g, Grocott et al., 1990; White, 1989; Webster, 1989; van Wyk, 1989; Radai, 1989; Monk, 1990). However, the private sector has been reluctant to admit vulnerability to virus attacks due largely to their fear of adverse publicity. Details of a successful virus attack, including the losses suffered, could shake shareholder confidence in an organization's management. Many corporations are unwilling to discuss the issue for fear that any revelation might attract attention and provoke a future attack.

1.1.7 The growth of the virus problem

The problem of computer viruses has grown to significant proportions in the last few years ("News track", 1991, p. 9; Wilding, 1991a, p. 2), as shown in Figure 1. Figure 1, adapted from Fites et al. (1992, p. 53), shows that the number of new IBM PC viruses is almost growing at an exponential rate from late 1986 to January 1991.

Figure 1. Cumulative Reports of Types
by Quarter: PC Viruses



Data gathered by *Virus Bulletin*, an authoritative international publication on computer virus prevention, recognition and removal, also show a similar trend. *Virus Bulletin* publishes an update of known IBM PC viruses reported to the bulletin during the preceding month in each of its editions. In its first edition in July 1989, the bulletin listed only 14 virus patterns. Two years later, the bulletin lists a total of 374 known viruses affecting IBM PC, XT, AT, PS/2 and compatibles in its July 1991 issue.[21] (A listing of these 374 viruses is reproduced in this paper as Appendix 1 to give the reader a general feel of the name and types of the 374 unique IBM PC viruses.)

The growth of the virus problem is not restricted to the IBM PC, and now affects all popular personal computers including Macintosh, Apple II, Atari ST, and Commodore Amiga. Mainframe viruses do exist for a variety of operating systems and machines, "but all reported cases to date have been experimental in nature, written by serious academic researchers in controlled environments" (Spafford et al., 1989/1990, p. 319).

Most virus activity has involved PCs because of several factors, one of the most important being the PC software (e.g. MS-DOS) does not contain user and supervisor mode (Kamay et al., 1990, p. 16; Adams, 1989, p. 12). Thus any knowledgeable person has access to operating system level commands. In a Mainframe operating system, such access would be in privileged mode and therefore unavailable to application programs and all except systems programmers.

---

21 However, it should be noted that there are conflicting reports on the number of known viruses as of 1991 by various researchers. The number of virus samples gathered by *Virus Bulletin* is chosen for its authoritativeness. The second paragraph of section 1.4 gives a brief discussion of the reason for the disparity in the number of viruses being reported.

1.1.8 Viruses in the Australian scene

Although the vandalism or purposeful abuse by introducing computer viruses or worms to computer systems so far seems to be mainly an American experience, it has become increasingly significant as a form of computer abuse in Australia in recent years, as shown in Tables 1 & 2 on pages 31 and 32, respectively. In fact, Tables 1 & 2 show that computer virus represents the fastest growing category of abuse in terms of the frequency of occurrence during the period from February 1989 to May 1990 in Australia.

Tables 1 & 2, adapted from Kamay et al. (1989, 1990), have been updated from computer abuse cases notified to and documented by the Australian Computer Abuse Research Bureau (ACARB) during the period from February 1989 to May 1990. The ACARB's figures indicate that total number of computer virus cases increased from 12 in the period ending January 1989 to 45 in the period ending May 1990. From the 45 computer virus cases reported since 1989, the average loss to the victims is $9,310 per crime.[22] The figures indicate that computer viruses, as a type of computer abuse, represents 59% of the reported case over the period from February 1989 to May 1990.

Although ACARB's figures do not necessarily show the complete extent of computer abuse in Australia, it is important to note that the factual evidence that exists in the profile supports the claim that computer virus, as a type of computer abuse in Australia, is showing a gradual significance over this period of time.

Apart from ACARB's figures, there is minimal empirical research of a similar nature being conducted to investigate *computer viruses* as a form of computer abuse in Australia. This study was thus appropriate in that it provides current evidence as to whether there is a problem in the work environment as

22 It should be noted that this average loss is based on a small sample of 2. The real figure is likely to be much higher.

opposed to the creation and isolation of computer viruses in laboratories of computer science.

1.1.9 The present study

In the present study the extent to which the *Western Australian* environment is being infected by *IBM PC* computer viruses was examined. In particular, the study investigated the infection *types* and *rates* of IBM PC viruses in selected government organizations in Western Australia.

Although the present study was designed to investigate the government sector, it was designed to be sufficiently generalizable for use to investigate other sectors as well (e.g., small business sector, large business sector). Some future comparison study with other states and sectors would be a fruitful area for further research. (See section 7.2.1.)

The main reason why the present study focused on IBM PC computer viruses (and not other PC or Mainframe viruses) is because the vast majority of virus attacks reported to date have been against personal computers, with the attacks on IBM PCs dominating.[23] In turn this is probably because the IBM style PC is the most prolific PC throughout the world.

In addition, the present study aimed to test Spafford's (1990) speculation[24] that "less than 10 viruses account for 90% of infections." Since this study adopted

---

23 Baker (1991, p. 31) argues that more than 70% of all reported infections have involved IBM PCs and compatibles although he gives no information on how the data are gathered.

24 In his *Computer viruses: Presentation for technology training corporation*, Spafford (1990, p. 5) states that "less than 10 viruses account for 90% of infections." We have no information on how the data are gathered, although others (e.g., Borrett, 1990, p. 38) have presented similar observations. This paper treats Spafford's observation as a

the view that currently there exists a minimum of 374 viruses, Spafford's speculation really means that a very small amount of viruses actually account for a large percentage of the infections.

1.2 Purpose of the Study

The present study was *descriptive* (Isaac & Michael, 1981, p. 46; McMillan et al., 1989, p. 33) in nature in that a fact-finding survey based on questionnaires and standardized interviews was conducted in selected government organizations in Western Australia in order to obtain data on which the research findings can be based.

The data gathering instrument for the present study was a standardized questionnaire which, in large part, comprises limited choice questions directed at obtaining such information as infection rates of various types of computer viruses. The questionnaire was chosen as the data gathering instrument because it is relatively economical, has standardized questions, and questions can be tailored for specific purposes of the study (McMillan et al., 1989, p. 254; Isaac et al., 1981, p. 130).

To ensure correct interpretation of the questions - so that the potential for subjectivity and bias can be reduced - and encourage a high response rate the standardized questionnaire was administered by interview. If necessary, responses were probed, followed up, clarified, and elaborated during the interview in order to achieve specific, accurate responses (McMillan et al., 1989, p. 266).

---

speculation rather than a hypothesis because it does not meet the hypothesis criteria, as suggested by McMillan and Schumacher (1989, p. 90 ff.) and Tuckman (1988, p. 62).

The purpose of the study was:

- To collect detailed factual information of the Western Australian environment that describes existing phenomena (e.g., Is a given population being infected by IBM PC viruses? If yes, what type of virus is infecting the given population and what is the rate of infection of that particular virus for the given population? Does reinfection occur? Which categories does the virus fall into?);
- To test the validity of Spafford's speculation within the Western Australian environment (i.e. Is it true that less than 10 viruses account for 90% of infections in Western Australia?);
- To identify problems (e.g. How is the virus introduced? Who is the perpetrator?);
- To determine what other people are doing with similar problems or situations and benefit from their experience in making future plans and decisions; and
- To help determine that the problem a given population is facing is definitely caused by a virus.

1.3 Statement of Research Questions

It was the purpose of this study to investigate the infection types and rates of IBM PC viruses in selected government organizations of Western Australia. In addition, the present study aimed at testing the validity of Spafford's speculation that less than 10 viruses (out of a minimum of 374) account for 90% of all infections.

1.3.1 Subsidiary questions

1. Does reinfection of systems occur? If yes, what is the reinfection rate?
2. Which categories does the virus fall into? (i.e., is it a boot infector, system infector, application infector for PC, etc.?)
3. How is the virus introduced? Who is the perpetrator?

1.3.2 Terms

Infection types. The type of a computer virus. For example, is the virus a boot sector infector, a COM files infector, or is of any other types?

Infection rates. The rate of infection of a particular type of computer virus. For example, the infection rate of boot sector infector viruses is, say, 10%.

IBM PC. The term "IBM PC" is used here to include the IBM XT, AT, PS/2 and compatibles.

Virus. The term "virus" is used here synonymously with the term "computer virus." See section 1.1.3 for a definition of a computer virus.

1.4 Significance of the Study

The research is significant in that it focussed attention on the problem of definition and then identification of a computer virus. As noted earlier, there is no general agreement in the computer community on the definition of a computer virus. Thus, gathering and analyzing data on *computer viruses* is complicated by the fact that the definitions used by the various entities involved are ambiguous and vary widely in their specifications.

Secondly, confusion abounds in reporting regarding the number of known computer viruses. There are viruses and there are often "mutations" of these

viruses. The many ways in which a researcher can classify these mutations is the main reason for the disparity in the number of viruses being reported.[25] Also, there appears to be competition among some of the researchers working in the computer virus field to announce a greater number of known viruses than anyone else.[26] Thus, gathering and analyzing data on *computer viruses* can be complicating in that given any two viruses, one cannot always be assured that they are not the same. To resolve this problem, this study adopted the number of virus samples gathered by *Virus Bulletin* and used that classification system (see Appendix 1). In essence, this study recognized that currently there exists a minimum of 374 distinctly different viruses affecting IBM PC, XT, AT, PS/2 and compatibles.

Thirdly, it seems evident ("News track", 1991, p. 9; Wilding, 1991a, p. 2; Fites et al., 1992, p. 53) that the incidence of real world computer virus infections is increasing at an alarming rate. The growth of this problem is of limited interest if the viruses are quarantined in laboratories and unless the samples listed manifest

---

25 For example, one attribute of the **Brain** virus is to write "Brain" as the label on an infected disk. If another virus is found that writes "Hello" as the disk label but is identical in every other respect, does one count this as a *new* virus? The code of both are the same but only five ASCII characters have been changed. Some researchers have taken an easy way out. If there is any change in the critical code of a virus, no matter how slight, they count it as a new virus. Others feel that so long as any two viruses have identical code and do not behave differently, they are variants of the original virus.

Depending upon what one chooses to recognize as separate viruses the total number of separately identifiable IBM PC viruses is somewhere between 800 and 1300 as of March 1992.

26 This phenomenon is perhaps exacerbated by the myopic view that "the more computer viruses one can list, the greater an authority he [or she] is on the subject" (Highland, 1990, p. 29).

themselves in the real world there is no real problem. Unfortunately, according to Wilding (1991a, p. 2), the editor of *Virus Bulletin*, "this is exactly what is happening, with more and more different specimens being encountered." Again, gathering and analyzing data on *computer viruses* is further complicated by the fact that the number of computer viruses are increasing at a dramatic rate.

Fourthly, there is no specific study similar to the nature of the present study being conducted in Australia in general, and in Western Australia in particular. As a result, there is very limited existing data to extrapolate and build upon. The present study is thus significant in that **factual** information regarding the nature and prevalence of the IBM PC viruses problem in the Western Australia environment can be added.

In addition, an attempt has been made to link this research with Spafford's (1990) speculation so that at the end of the study, the validity of Spafford's speculation within the Western Australian environment could be verified.

1.5 Organization of the Thesis

Chapter One of this thesis gives a brief introduction to the nature of the present study and deals with the technical preliminaries of this study. This chapter will familiarize the reader with basic terminology and fundamental issues address in the present study.

Chapter Two deals with the review of relevant research and literature. This chapter contains a review of general literature on computer viruses, specific studies similar to the present study, and the research design of the present study.

Chapter Three provides the theoretical framework of this study: what are the variables impacting on the research questions? What are the assumptions underpinning this study?

Chapter Four describes the method of investigation for this study. This chapter contains a brief description of: the research design for this study, the instruments used, the population of this study, the ethical considerations for this study, the data analysis procedures, and the limitations of this study.

Chapter Five presents the results of the survey conducted for this study. It is divided into four sections to cover the organizational profile, the use of IBM PC in the organizations surveyed, IBM PC viruses past experience in the organizations, and the .IBM PC virus control mechanisms and procedures in place in the organizations surveyed.

Chapter Six is devoted to a discussion of the implications of the results gathered from the survey.

Chapter Seven gives a brief summary of the findings of the survey conducted for this study, provides suggestions for further research on this area of study, and concludes the thesis.

Chapter Two

Review of Literature

2.1 General Literature on Computer Viruses

There have been many newspaper and trade press articles about computer viruses - although often misleading and inaccurate (Highland, 1988a; Simons, 1989, p. 105) - but there has been little technical material published except in *Virus Bulletin* and *Computers & Security*.[27] The nature of computer security is such that published material tends to be quite limited.

2.1.1 Conceptual foundations and defence

The following are important technical research papers regarding the conceptual foundations of computer viruses, design of virus defences, and the spread of computer viruses:

- Dr. Frederick Cohen's (1984) "Computer viruses: Theory and experiments," presented at IFIP/Sec'84 in Toronto, Canada in September

27 This is a leading international journal addressing security issues, audit control, and data integrity relating to all data processing equipment: mainframe, mini and microcomputers. Each issue contains refereed articles on relevant subjects, special features, and summaries of articles published elsewhere.

1984; and his subsequent (1986) doctoral dissertation.[28] A generic example (i.e., template) for a virus, formulated in pseudo-Pascal and adapted from the one given by Cohen (1984), is given by Leiss (1990, p. 39).

- Rudiger Dierstein's (1987) "Computer viruses: A secret threat," presented at SECURICOM held in Paris, France during March 1986. This article provides an insight into the structure, propagation and function of computer viruses, and explores the systems environment in which viruses are created and proliferate.
- Dr. Ian H. Witten's (1987) "Computer (In)security: Infiltrating open systems," that appeared in the summer 1987 issue of *Abacus*. In this article, Witten describes an impressive array of methods both for securing and for attacking computers. The article also explains how viruses and worms work, and how they can be created.
- Dr. Winfried Gleissner's (1989) "A mathematical theory for the spread of computer viruses" that appeared in *Computers & Security*. This article introduces a model to treat the spread of computer viruses mathematically.

Two additional articles about computer viruses appeared during the summer of 1987, according to Highland (1990, p. 295). They were "Taxonomy of computer virus defence mechanisms" by Catherine L. Young and "Computer viruses: Myth or reality?" by Howard Israel. Both were in the Proceedings of the 10th National Computer Security Conference that was held in September 1987.

28 Cohen, generally regarded as the "father" of computer viruses, published much of the original work on computer viruses starting in 1983, which was mostly theoretical and highly mathematical based.

2.1.2 Prevention

Prevention refers to the ability to ensure that an uninfected system remains uninfected. Cohen (1984) gives a discussion of flow controls as a means of guarding against computer viruses. Some approaches based on the imperviousness of hardware to remote manipulation are given by Routh (1984) and Davis & Gantenbein (1987). Other papers of interest are provided by Highland (1988b, 1988c, 1988d), Fak (1988), Pozzo & Gray (1987), Wiseman, (1989), Zajac, (1990), Murray (1988) and Cohen (1987, 1988, 1989, 1990).

2.2 Specific Studies Similar to the Current Study

There is no doubt that there is a real threat of computer viruses but there is a dearth of information regarding the prevalence and the types of different viruses. Data exists in the U.S. in some states and periodic data comes from the U.K. but there is limited systematic data from Australia, apart from ACARB's periodic profile of computer abuse in Australia, which categorizes computer viruses as one of many forms of computer abuse.

2.2.1 ACARB's 1990 profile of computer abuse in Australia

As a non-profit public organization, ACARB sees itself in an ideal position to serve the business community "as a catalyst in the synthesis of knowledge in the [computer abuse] area, as a researcher in the evaluation and development of preventative means, and as a forum for the exchange of ideas."[29] (Kamay et al., 1990, p. 29).

29 ACARB regularly publishes a profile of the extent and nature of computer abuse in Australia in which factual information is gathered in an attempt to quantify this

2.2.1.1 Summary of ACARB's 1990 Figures

The following tables, adapted from Kamay et al. (1989, 1990) and Bright (1989), have been updated from cases notified to, and documented by, ACARB during the period from February 1989 to May 1990. The tables provided are of two types; viz., the period to date figures that represent the details of cases notified to ACARB from February 1989 to May 1990, and figures that update the total number and values of cases notified to ACARB (and prior to its formation CIT-CARB at the Caulfied Institute of Technology) since 1978.

Table 1

Type of Computer Abuse in Australia (February 1989 to May 1990)

Classification	Count	Known Value	$ Value of Loss	Percent of Value	Average $ Loss
Computer Related Fraud	2	2	1,050,000	64.30	525,000
Unauthorised Use	2	0	0		0
Hacking	3	1	5,000	0.01	5,000
Theft of Output					
Sabotage	1	1	0		0
Masterfile Destroyed					
Theft of Equipment	14	14	527,776	32.40	37,698
Electronic Funds	2	1	32,500	2.00	32,500
Virus	33	1	17,920	1.10	17,920
Total	57	20	$1,633,196	100.00%	$81,660

phenomenon, determine any trends in its development and thereby provide a biographical sketch or profile of computer abuse in Australia.

ACARB also publishes a regular Newsletter/Research Report (the *ACARB Newsletter* and the *ACARB Research Report*) which includes papers of interest and periodic statistical profiles of computer abuse in Australia in order to enable business to understand trends that are occurring. In addition, ACARB produces the *Computer Risks Update* which compiles material on current and potential risks, descriptions of viruses and other forms of attack, potential remedies, brief details of new books and other publication, new anti-viral and other security products and so forth.

Table 2
Type of Computer Abuse in Australia (as of May 1990)

Classification	Count	Known Value	$ Value of Loss	Percent of Value	Average $ Loss
Computer Related Fraud	92	63	12,052,034	79.2	191,302
Unauthorised Use	52	17	57,600	0.0	3,388
Hacking	29	4	18,300	0.0	4,575
Theft of Output	17	4	250,000	1.6	62,500
Sabotage	13	4	903,000	5.9	225,750
Masterfile Destroyed	4	2	900	0.0	450
Theft of Equipment	48	44	1,247,976	8.2	28,363
Electronic Funds	13	11	664,625	4.4	60,420
Virus	45	2	18,620	0.0	9,310
Total	313	151	$15,213,055	100.0%	$100,749

Table 2 shows that the total number of cases reported by ACARB to date is 313, resulting in a loss of $15,213,055 from 151 assessable cases. 162 cases were unassessable with an unknown loss. The average loss from the 151 assessable cases was $100,749.

Incidentally, Table 1 shows that the greatest number of reported cases over the period from February 1989 to May 1990 has involved the category of viruses. This category represents 59% of the reported cases in the period.

2.2.1.2 Types of Abuse

Tables 1 and 2 categorise computer abuse by type according to nine categories; viz., computer related fraud, unauthorised used, hacking, theft of output, sabotage, masterfile destroyed, electronic funds transfer, computer virus, and theft of equipment. The meanings of the heading in Tables 1 and 2 is as follows:

Count. Total number of incidences reported.

Known value. Total number of incidences with a known dollar loss.

Value of Loss. Total value of loss for that category.

Percent of Value. The percentage of that category against the total of all categories.

Figure 2 on page 35 shows the percentage of various types of abuse, by number of occurrences over the twelve year period (1978 - 1990) of data collection. Figure 3 on page 36 reflects the continued and stable growth of the nine categories of computer abuse over the past two years. Although ACARB's figures do not necessarily show the complete extent of computer abuse in Australia, it is important to note that the factual evidence that exists in the profile shows stable trends over this period of time.

2.2.1.3 Computer Viruses As Computer Abuse

Computer viruses are a form of computer abuse that is arguably more insidious than any other, and represents the fastest growing category of abuse in terms of the frequency of occurrence over the past two years in Australia. It amounts to 59% of the cases of computer abuse in the current period. While it amounts to only 1% of the monetary losses from computer abuse,[30] the cost of this activity may lie more with the value an organization places on data and information that may be lost on floppy and hard disk, and any subsequent loss of business opportunities and productivity. Such factors are additional to the cost of time that is often required for technicians to recover information or rebuild a hard disk. Hence, it is hard to quantify the value of losses associated with viruses.

It is evident (Kamay et al., 1990, p. 16) from the documented cases by ACARB of known viruses that they utilise relatively few methods of operation with the most likely outcome being the destruction of information on a floppy or hard

30 It should be noted that the 1% is based on a small sample of 1 (see Table 1) and is therefore not a good indicator of cost.

disk. A notable change in the character of viruses has occurred over the period from February 1989 to May 1990, as Kamay et al. (1990, p. 16) observed, "has been their increasing level of sophistication which has led to greater difficulty in their detection and removal, and their greater virulence and destructive impact." This observation is in general agreement with Wilding's (1991a, p. 2) findings.

Figure 2. Type of Computer Abuse In Australia (as of May 1990)

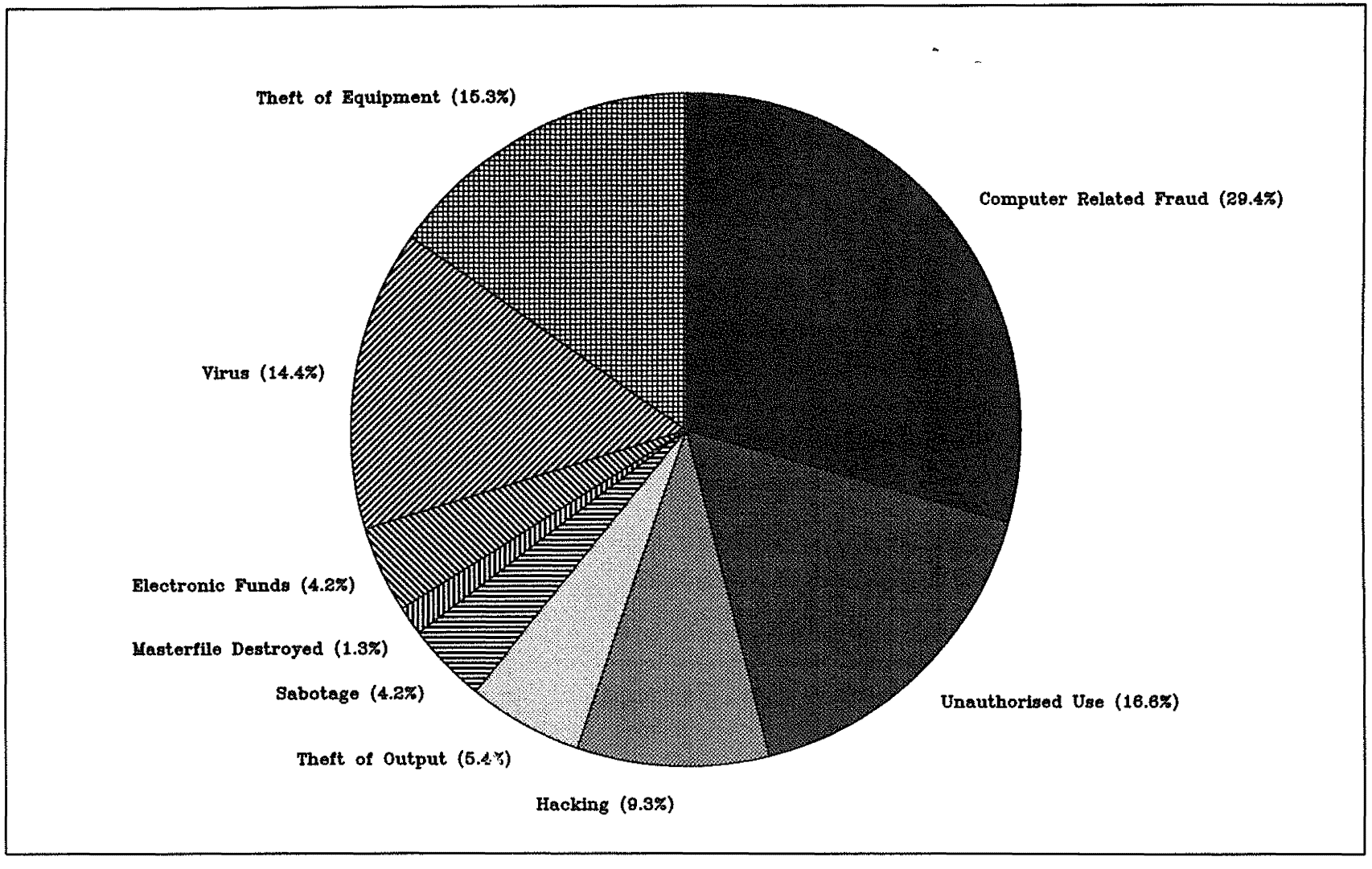
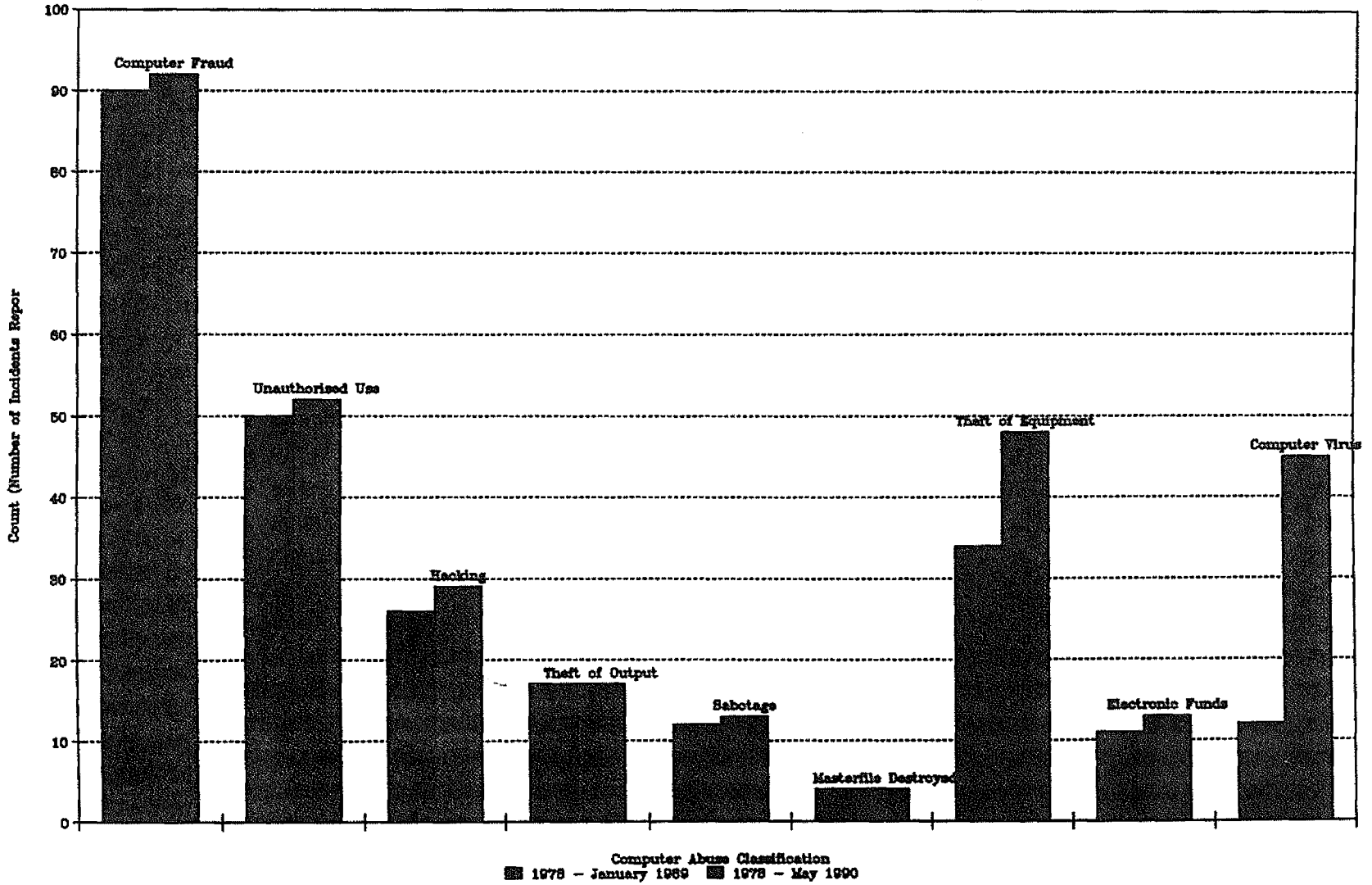


Figure 3. Accumulated Growth of Types
of Computer Abuse in Australia



2.2.2 Dataquest's 1991 computer virus market survey

One of the most revealing sessions of the 1991 NCSA (National Computer Security Association) Anti-Virus Product Developers Conference in Washington, D.C. was the publication of a Computer Virus Market Survey undertaken by *Dataquest (*Hruska, 1992; Monk, 1992). The survey aims to identify the nature and the extent of computer virus problem on PCs in the U.S. During October 1991, 602 corporate end-users were interviewed by telephone during October 1991. All interviews were conducted on sites with 300 or more PCs and the majority of respondents were responsible for controlling the virus problem on all the PCs. The findings of the survey, adapted from Hruska (1992, p. 7) and Monk (1992, p. 5), are summarized below:

- 63% of respondents reported at least one encounter with a virus over the past year, and 9% had more than 25 PCs infected in the process;
- **New Zealand** (or **Stoned** or **Marijuana**) was responsible for 48% of the attacks, **Jerusalem** (or **Friday the 13th**) for 37% and **Joshi** for 8%;
- The major entry points of viruses into the organizations surveyed were disks brought from home PCs (43%), followed by the virus-infected programs pulled down from bulletin boards (7%) and demonstration disks and service engineers (6%). Only 1% of infections came with the PC from the dealer or the factory;
- When asked to estimate the cost of each virus infection, 31% of organizations spent less than $2,000, 29% between $2,000 and $10,000, while 7% spent more than a staggering $100,000.

A comparison between the findings of Dataquest's 1991 survey in the U.S. and the findings of this study is provided in section 6.3.5 of this paper.

2.2.3 Virus Bulletin's February 1992 virus prevalence table

A Virus Prevalence Table, produced from statistics collated by *Virus Bulletin*, is featured in each edition of the bulletin showing the prevalence of different viruses in the U.K. during the preceding month.

The following Virus Prevalence Table, adapted from Wilding (1992, p. 6), shows recorded virus infections reported to *Virus Bulletin* in the U.K. during February 1992. However, it should be noted that Wilding (1991) maintains that:

> the figures shown in these tables do not accurately portray the *full* extent of the problem in the U.K. as they do not include statistics from the myriad of other agencies involved in combating computer viruses. (p. 4)

Table 3

Virus Bulletin's February 1992 Virus Prevalence Table

Virus	Incidents	Total Reports
New Zealand II	11	20.3%
Form	11	20.3%
Tequila	7	12.9%
Michelangelo	4	7.4%
Spanish Telecom	3	5.5%
Cascade	2	3.7%
Vacsina	2	3.7%
Maltese Amoeba	2	3.7%
Flip	2	3.7%
Brain	2	3.7%
1575	1	1.8%
DIR II	1	1.8%
Liberty	1	1.8%
Anticad 2576	1	1.8%
Joshi	1	1.8%
Total	54	100%

2.3 Literature on Methodology

The present study was descriptive in nature in that a survey based on questionnaires and interviews was conducted. The literature of surveys design and techniques (Fink & Kosecoff, 1985; Fowler, 1984; Isaac et al., 1981; Borg & Gall, 1979; Campbell & Katona, 1953), of questionnaire design (Borg, 1963; Oppenheim, 1966), and of interview techniques (Borg, 1963; Kerlinger, 1973) were therefore expected to be relevant.

Research papers of interest and periodic statistical profiles of computer abuse in Australia that ACARB publishes regularly was also consulted as appropriate during the design of the questionnaire.

Chapter Three

Theoretical Framework

3.1 Variables Impacting on the Research Questions

Since the research was *descriptive* in nature, no "independent", "dependent" variable need be identified because "[descriptive research] does not involve manipulation of independent variables" (McMillan et al., 1989, p. 282). The purpose and the logic of this study determined that there was only one variable of interest to the present study; viz., the infection rates and types of different IBM PC viruses. All of the state government organizations of Western Australia comprised the designated population of the study. (See Appendix 6 for a list of the surveyed organizations.)

The 374 known IBM PC viruses (as of July 1991) gathered by the *Virus Bulletin* (Wilding, 1991b) are categorised into the following seven types:

- The COM files infector;
- The EXE files infector;
- The DOS boot sector[31] infector;
- The master boot sector[32] infector;
- Not memory-resident after infection virus;

31 This is logical sector 0 in each DOS partition.

32 This is the sector stored at absolute track 0, head 0, sector 1.

- Memory-resident[33] after infection virus; and
- Companion virus.[34]

A somewhat similar classification method is provided in *Virus Characteristics List V89B*, a software documentation that comes with the 1992 version of McAfee Associates' antiviral software, *VIRUSCAN Version 8.4B89* (1992). All unique IBM PC viruses are categorised into the following ten types:

- Virus uses Stealth Techniques;
- Virus uses self-encryption;
- Virus installs itself in memory (i.e., memory-resident);
- Virus infects COMMAND.COM;
- Virus infects COM files;
- Virus infects EXE files;
- Virus infects Overlay files;
- Virus infects floppy diskette boot;
- Virus infects fixed disk boot sector; and
- Virus infects fixed disk partition table.[35]

---

33 This implies that, once a single infected program has been run, the virus potentially can spread to any or all programs in the system. This spreading occurs during the entire work session (until the system is rebooted to clear the virus from memory), rather than during a small period of time when the infected program is executing viral code.

34 The term "companion virus" describes any computer virus which locates an EXE file and then creates a new program in the same directory with a COM extension (Wilding, 1990b, p. 3). This bogus COM file contains the virus code and is invoked before the legitimate EXE file executes.

35 Fixed (or hard) disk partition table (or record) (aka master boot record) is the 64-byte table contained at the end of the master boot sector.

For the present study, it was determined that the classification method used by VIRUSCAN Version 8.4B89 (1992) is more appropriate since it covered a wider range and is somewhat more updated. Thus, all unique IBM PC viruses that are known to infect the responding organizations would be categorised into the 10 infection types advocated by VIRUSCAN Version 8.4B89 (1992).

3.2 Assumptions Underpinning the Study

The present study assumed that:

1. IBM PC viruses do exist and pose a form of computer abuse in the Western Australian environment.
2. information about IBM PC viruses within selected organizations can be obtained during the interview.
3. the respondents realise that the problem of IBM PC virus infection does exist in their respective organizations and recognise the types of infecting viruses.
4. the respondents have reliable information with regards to their organization's IBM PC viruses infection rates.
5. no one guesses or presents an uninformed answer when answering the questionnaire during the interview.
6. the respondents will be cooperative and that they will produce unbiased and truthful responses during the interview.

Chapter Four

Method of Investigation

4.1 Design of the Study

As stated, the research was *descriptive* in nature in that a survey based on questionnaires and interviews was conducted for the study. The study was initiated with the view that it will stand or fall on the extent to which it can add convincingly to knowledge about the present status of the IBM PC viruses problem in the Western Australian environment. In addition, the study has made an attempt to investigate Spafford's speculation within the Western Australian environment.

4.2 Description of Instruments Used

Data on which the research findings will be based were obtained from a survey of selected state government organizations. The data gathering instrument was a locally developed questionnaire which, in large part, comprises limited choice questions directed at obtaining such information as type of virus and infection rates. (The questionnaire is appended as Appendix 2). The questionnaire was standardized so that information from each respondent is gathered in the same manner. The standardized questionnaire was used by the interviewer as a basis for the interview so that the potential for subjectivity and bias can be reduced. The

participants were assisted by the interviewer in identifying the types of infecting viruses when the need arise.

As with other descriptive research, there is no assurance that all questions in the questionnaire will be understood. In the present study, this problem was recognised and to this end it was intended that the questionnaire was carefully field tested to eliminate ambiguous or biased items and to improve format, both for ease of understanding and facility in analyzing results. Furthermore, any inquiries the respondents might have regarding the questionnaire during the interview have been answered by the interviewer.

4.3 Population of the Study

Before the commencement of the study, the official list of the address of all the state government organizations and the name of a contact person was sought from State I.T. Division, Department of State Services. Since the population of the study was not sufficiently large (n = 48), a letter of transmittal was sent to all of the 48 prospective participants to request their participations in the survey. (A sample letter of transmittal is included in Appendix 3.) Confirmation of participation was sought through telephone calls.

4.4 Survey Response Rate

A very high response rate (87.5%, n = 42) for the study has been achieved. This is taken as an assurance that adequate representation of the state government sector for the study is achieved and that the survey results is truly representative of the state government sector. (See Appendix 6 for a list of the organizations.)

Of the six (12.5%) organizations that refused to participate in the study:

- 3 (50%) of them declined to give any reason of their refusal to participate;
- 2 (33.33%) of them said they were too busy with their work to be able to participate; and
- 1 (16.67%) of them cited the organization has a written policy never to participate in any study of this nature.

4.5 Ethical Considerations

Prior to commencement of the study, approval was sought from the University Committee for the Conduct of Ethical Research since the study involves human subjects. (The approval letter is included in Appendix 4.)

Participation in the study was entirely voluntary and subjects were free to withdraw their consent at any stage of the study. During the interview, subjects were informed of the purpose of the study, that there will be no compulsion to participate in the study and that they will be free to withdraw from further participation in the study at any time.

In keeping with the policies of the university's Committee for the Conduct of Ethical Research, a copy of the Form of Disclosure and Informed Consent was made available to participants for their records. (The written statement is included in Appendix 5.)

Although number identification on the questionnaires was used to allow easy recording of data, participants were not identified by name. Completed questionnaires were seen only by this researcher, usef for the purpose of this study only and were destroyed at the end of the study.

4.6 Data Analysis Procedures

When the data on which the research findings will be based were gathered from the survey, the infection rate of each of the individual infecting viruses were then tabulated. Once the infection rate of each of the infecting viruses was tabulated, it was relatively easy to validate whether Spafford's speculation that less than 10 viruses account for 90% of infections was applicable in this environment. The reinfection rate of the infecting viruses were then determined from the available data gathered from the survey.

4.7 Limitations of the Study

Isaac (1981) argues that, with the exception of surveys based on a search of records:

> surveys are dependent on direct communication with persons having characteristics, behaviours, attitudes, and other relevant information appropriate for a specific investigation. (p. 128)

This, Isaac (1981, p. 128) contends, "make them *reactive* in nature; i.e., they directly involve the respondent in the assessment process by eliciting a reaction." It should be noted that reactive methods run many risks of generating misleading information although they are often the most cost-effective, efficient, and credible means of collecting data. These risks, adapted from Isaac (1981), include:

- Surveys only tap respondents who are accessible and cooperative;
- Surveys often make the respondent feel special or unnatural and thus produce responses that are artificial or slanted;
- Surveys arouse "response sets" such as acquiescence or a proneness to agree with positive statements or questions;

- Surveys are vulnerable to over-rater or under-rater bias - the tendency for some respondents to give consistently high or low ratings; and
- In the case of interviews, biased reactions can be elicited because of the characteristics of the interviewer or respondent, or the combination, that elicit an unduly favourable or unfavourable pattern of responses (p. 128).

The present study is thus delimited by these risks.

Chapter Five

Results of the Survey

5.1 Organization Profiles

The first section of the questionnaire was designed to obtain information regarding the number of PC users, the volume and the size of each organization surveyed.

5.1.1 Industrial groupings

In terms of industrial groupings, all the respondents of the survey were from W.A. State Government departments and organizations. The high response rate (87.5%, $n = 42$) for the survey assures reasonble representation.

5.1.2 Size of the organizations

It is difficult to determine the size and in turn the computer activity in a particular organization and one of the criteria used was to examine the expenditure of the organization. The size of the organizations in terms of gross annual budget in $A is set out in Table 4.

Table 4 reveals that half of the organizations (50%) have a budget of under $100 million. In terms of gross annual budget, the organizations have an average of $121.08 million with a standard deviation (S.D.) of $244.51 million. However, it should be noted that one organization has a very large budget (over $1000

million). If this organization were excluded from the calculation, the average gross annual budget of the organizations will be $81.12 million, with a S.D. of $125.12 million. These figures, ignoring the exceptional case, are believed to be more representative.

Table 4 also shows that a significant number, approximately one third (33.33%) of the respondents could not, or chose not, to answer this question. This can be attributed to the fact that many respondents of the survey are technical personnel who can answer questions pertinent to the virus infection in their respective organizations but who may not have the necessary information regarding the financial status of their organizations.

Table 4

Size of Organizations In Terms of Gross Annual Budget

Budget ($ Millions)	Number of Respondents	Percentage
Not Available	14	33.33
Under 50	17	40.48
51 - 100	4	9.52
101 - 200	2	4.76
201 - 300	1	2.38
301 - 400	2	4.76
401 - 500	1	2.38
Over 1000	1	2.38
Total	42	100.00

Mean = $121.08 million

Standard Deviation = $244.51 million

5.1.3 Number of staff

Another indicator of size of the organization is the number of staff employed which also represents an indication of the likely computer activity. The number of full-time staff in each organization is shown in Table 5.

Table 5 shows that the majority of the organizations (52.38%) employed between 51 and 300 employees. The average number of staff in the organizations is 839 (round off to the next digit).

Table 5

Number of Staff in the Organizations

Number of Staff	Number of Respondents	Percentage
Not Available	1	2.38
Under 50	2	4.76
51 - 100	8	19.05
101 - 200	9	21.43
201 - 300	5	11.90
301 - 400	1	2.38
401 - 500	2	4.76
501 - 750	3	7.14
751 - 1000	4	9.52
Over 1000	7	16.67
	42	100.00

Mean = 838.22 ≅ 839

Standard Deviation = 1357.93 ≅ 1358

5.1.4 Computing (or computer services or IT) section

A separate computing (or computer services or IT) section is maintained in 38 (90.48%) of the 42 organizations. The size of computing sections in terms of staffing is set out in Table 6. The majority of the organizations (66.67%) employed between 1 and 30 staff in their respective computing sections. On average, the number of staff employed in each computing section is 25.

Table 6

Number of Staff in Computing Section of the Organizations

Number of Staff	Number of Respondents	Percentage
1 - 10	22	57.89
11 - 20	2	5.26
21 - 30	4	10.53
31 - 40	1	2.63
41 - 50	1	2.63
51 - 60	2	5.26
61 - 70	3	7.89
71 - 80	1	2.63
81 - 90	1	2.63
91 - 100	1	2.63
	38	100.00

Mean = 24.34 ≅ 25

Standard Deviation = 28.19 ≅ 29

5.2 Profile of the IBM PC Use

To understand the computer virus infection incidents it was necessary to obtain information regarding the profile of PC use within an organisation. Such relevant information would include the number of PCs in use and the number of users. It is also to determine whether the systems are nertworked or operated on a standalone basis.

5.2.1 Number of IBM PC

The number of IBM PC each of the organizations possessed is listed in Table 7, which shows that the majority of them (59.52%) have between 1 and 100 PCs. On average, the number of IBM PC each organization owns is 170 with a S.D. of 208. The large standard deviation can be attributed to the fact that the data are "positively skewed" (i.e., organizations tend to have small number of PCs) and not spread in a normal distribution.

Table 7
Number of IBM PC in the Organizations

Number of IBM PC	Number of Respondents	Percentage
1 - 25	10	23.81
25 - 50	7	16.67
51 - 100	8	19.05
101 - 150	4	9.52
151 - 200	3	7.14
201 - 300	2	4.76
301 - 400	1	2.38
401 - 500	2	4.76
Over 500	5	11.90
	42	100.00

Mean = 169.57 ≅ 170
Standard Deviation = 207.51 ≅ 208

5.2.2 Number of Apple Macintosh

Although this survey was not examining computer viruses associated with Apple Macintosh PCs it was considered worthwhile to gain an understanding of the penetration of Apple Macintosh computers compared to IBM PCs in this particular environment to consider whether research into Apple Macintosh viruses could be justified.

As it transpired, 24 (57.14%) of the 42 surveyed organizations own one or more Apple Macintosh computers. For those organizations that possess at least one Apple Macintosh, the number of Apple Macintosh each of them owned is set out in Table 8.

The majority of the organizations (54.17%) have between 1 and 5 Apple Macintoshs computers. On average, the number of Apple Macintosh computers the organizations own is 59. However, it should be noted that there is an organization which has a very large number of Apple Macintosh (approximately 1000). If this organization were excluded from the calculation, the number of Apple Macintosh in each organization, on average, will be 18, with a S.D. of 37. These figures are believed to be more reflective of the existing situation.

Table 8

Number of Apple Macintosh in the Organizations

Number of Apple Macintosh	Number of Respondents	Percentage
1 - 5	13	54.17
6 - 10	3	12.50
11 - 15	3	12.50
16 - 20	1	4.17
21 - 25	0	0.00
26 - 50	1	4.17
51 - 100	1	4.17
Over 100	2	8.33
	24	100.00

Mean = 58.21 ≅ 59

Standard Deviation = 203.68 ≅ 204

5.2.3 Number of IBM PC users

The number of staff that are IBM PC users on a regular basis in the organizations is shown in Table 9. The majority of the organizations (54.76%) have between 1 and 100 staff that are regular IBM PC users. On average, the number of staff that are regular IBM PC users in the organizations is 215.

Table 9

Number of Staff That Use IBM PC Regularly In the Organizations

Number of IBM PC User	Number of Respondents	Percentage
1 - 25	10	23.81
25 - 50	5	11.90
51 - 100	8	19.05
101 - 150	4	9.52
151 - 200	2	4.76
201 - 300	2	4.76
301 - 400	3	7.14
401 - 500	2	4.76
Over 500	6	14.29
	42	100.00

Mean = 214.19 ≅ 215

Standard Deviation = 276.40 ≅ 277

5.2.4 Number of Apple Macintosh users

Twenty two (52.38%) of the 42 surveyed organizations have one or more staff that are regular Apple Macintosh users. For those organizations that possess at least one Apple Macintosh, the number of staff that are regular Apple Macintosh users is set out in Table 10. The majority of the organizations (72.73%) have between 1 and 15 staff that are regular Apple Macintosh users. On average, the number of staff that are regular Apple Macintosh users in the organizations is 75. However, it should be noted that there is an organization which has a very large number of staff that are regular Apple Macintosh user (approximately 1200). If this organization were excluded from the calculation, the number of staff that are regular Apple Macintosh users in the organizations, on average, will be 22, with a S.D. of 38.

Table 10

Number of Staff That Use Apple Macintosh Regularly In the Organizations

Number of Apple Macintosh User	Number of Respondents	Percentage
1 - 5	7	31.82
6 - 10	5	22.73
11 - 15	4	18.18
16 - 20	2	9.09
21 - 25	0	0.00
26 - 50	1	4.55
51 - 100	1	4.55
Over 100	2	9.09
	22	100.00

Mean = 74.64 ≅ 75

Standard Deviation = 253.94 ≅ 254

5.2.5 Time for which the organizations have been using IBM PC

The length of time for which the organizations have been using IBM PCs is summarised in Table 11, which shows that the majority of the organizations have been using IBM PCs for between 6 and 8 years.

Table 11

Years For Which the Organizations Have Been Using IBM PC

Years	Number of Respondents	Percentage
Not Available	2	4.76
Under 3 years	1	2.38
3 - 5 years	9	21.43
6 - 8 years	19	45.24
Over 8 years	11	26.19
	42	100.00

5.2.6 Network connections

In 28 (66.67%) of the 42 organizations, at least one networking system is in place. The number of separate networking systems in use in the organizations is summarised in Table 12. There are a total of 63 separate networking systems in used in the 28 organizations.

Table 12

Number of Separate Networking Systems In Use in the Organizations

Number of Separate Networking Systems	Number of Respondents	Percentage	Total Number of Networking Systems
1	15	53.57	15
2	7	25.00	14
3	3	10.71	9
4	1	3.57	4
9	1	3.57	9
12	1	3.57	12
	28	100.00	63

5.2.7 Number of IBM PC in each of the networks in the organizations

The number of IBM PCs in each of the 63 networking systems in the organizations is summarised in Table 13. The majority of the networking systems (72.13%) have between 1 and 30 IBM PCs linked to it. On average, the number of IBM PCs that are linked to the networks in the organizations is 50.

Table 13

Number of IBM PC in the Networking Systems of the Organizations

Number of IBM PC	Number of Respondents	Percentage
Not Available	2	3.17
1 - 10	11	17.46
11 - 20	14	22.22
21 - 30	19	30.16
31 - 50	7	11.11
51 - 100	4	6.35
101 - 200	4	6.35
Over 200	2	3.17
	63	100.00

Mean = 49.51 ≅ 50

Standard Deviation = 97.81 ≅ 98

5.2.8 Use of network operating systems in the organizations

The network operating system (NOS) of the 63 networking systems in the organizations is set out in Table 14.

Table 14

Network Operating System of the Networking Systems in the Organizations

Network Operating System	Number of Respondents	Percentage
Not Available	8	12.70
Novell NetWare	26	41.27
3Com 3+ Open	11	17.46
IBM OS/2 LAN Server	7	11.11
PC NFS	4	6.35
IBM LAN Manager	3	4.76
LANTastic	1	1.59
Banyan VINES	1	1.59
Microsoft LAN Manager	1	1.59
Pathwork	1	1.59
	63	100.00

5.2.9 Effect of non-availability of networks in the organizations

The effect of non-availability of each networking system in the organizations is summarised in Table 15.

Table 15

Effect of Non-availability of Networks in the Organizations

Effect	Number of Respondents	Percentage
Minimal	14	22.22
Inconvenience	7	11.11
Major	42	66.67
	63	100.00

5.2.10 External connections

In 15 (35.71%) of the 42 organizations, external dial-in capabilities are allowed. Only 4 (26.67%) of the 15 organizations use a dial-back system to allow only access from an approved list of numbers. Nine (81.82%) out of the 11 organizations that do not use the dial-back system are relying on the password mechanism to prevent unauthorised access. In addition to password protection, three (27.27%) other organizations disclosed that the use of a dial-back system is unnecessary because all external person can only dial into a single stand-alone

personal computer within the organization. One (9.09%) other organization revealed that the use of dial-back system is unnecessary because the dial-in capabilities are normally disabled and are not used very frequently.

5.3 IBM PC Virus Problem Experience

5.3.1 Seriousness of the IBM PC viruses problem in the organizations

The following table summarises the perceived seriousness of the IBM PC viruses problem in the organizations. Of particular note is that the majority of the respondents (57.14%) believe that IBM PC viruses only pose a minor problem in their respective organizations.

Table 16
Perceived Seriousness of the IBM PC Viruses Problem in the Organizations

Seriousness of the problem	Number of Respondents	Percentage
No problem	15	35.71
Only a minor problem	24	57.14
A reasonable serious problem	2	4.76
A major problem	1	2.38
	42	100.00

5.3.2 Number of organizations that had IBM PC viruses infection

There were a total of 27 (64.29%) organizations reported to have at least one IBM PC virus infection over the years. The following table summarises the number of times the 27 organizations have had an IBM PC virus infection. It reveals that the majority of the organizations (55.56%) have between 1 and 4 infections over the years.

In terms of number of separate incidents, the organizations have an average of 15 incidents with a S.D. of 39. However, it should be noted that there is an

organization which has a very large number of occurrences (200 times). If this organization were excluded from the calculation, the number of separate incidents of the organizations, on average, will be 8, with a S.D. of 10. These figures are believed to be more representative than the previous figures since it is rather unusual to have this large number of infections.

Table 17

Number of IBM PC Virus Infection in the Organizations

Number of Infections	Number of Respondents	Percentage	Total Infections
1	4	14.81	4
2	5	18.52	10
3	2	7.41	6
4	4	14.81	16
5	1	3.70	5
6	2	7.41	12
7	1	3.70	7
9	1	3.70	9
12	1	3.70	12
16	1	3.70	16
20	1	3.70	20
26	1	3.70	26
30	1	3.70	30
31	1	3.70	31
200	1	3.70	200
	27	100.00	404

Mean = 14.96 ≅ 15

Standard Deviation = 38.04 ≅ 39

5.3.3 Types of PC virus infections

The number of incident of IBM PC viruses by types in the organizations in the periods prior to 1991, during 1991, and as of April 1992 is summarised in Table 18.

Table 18

Number of IBM PC Viruses by Types in the Organizations

Types	Prior to 1991[36]		During 1991		As of April 1992		Total	
	No	%	No	%	No	%	No	%
New Zealand (Stoned, Marijuana)	83	20.54	99	24.50	7	1.73	189	46.78
Michelangelo	-	-	132	32.67	6	1.49	138	34.16
Liberty (Magic, Mystic)	3	0.74	28	6.93	1	0.25	32	7.92
Jerusalem (Jerusalem B)	2	0.50	5	1.24	1	0.25	8	1.98
Den Zuk (Search)	-	-	6	1.49	-	-	6	1.49
Ohio (Hacker)	-	-	5	1.24	-	-	5	1.24
Keypress (Turku, Twins)	-	-	3	0.74	1	0.25	4	0.99
Dark Avenger	-	-	3	0.74	-	-	3	0.74
Italian (Pingpong, Friday the 15th, Israel)	-	-	3	0.74	-	-	3	0.74
No-Int[37]	-	-	2	0.50	1	0.25	3	0.74
Flip	-	-	2	0.50	-	-	2	0.50
1559	-	-	-	-	1	0.25	1	0.25
1575	-	-	-	-	1	0.25	1	0.25
Form	-	-	-	-	1	0.25	1	0.25
Slow	-	-	1	0.25	-	-	1	0.25
Unknown	1	0.25	6	1.49	-	-	7	1.73
Total	89	22.03	295	73.02	20	4.95	404	100.00

36 The data from the survey show that the first incidents of IBM PC virus attacks among the respondents occurred in 1989.

37 **No-Int** is a variant of **New Zealand**.

5.3.4 Number of PC infected during each infection in the organizations

The number of IBM PC infected during each of the IBM PC Viruses infections in the organizations is shown in Table 19.

Table 19 reveals that there were a total of 6490 PCs (including reinfection) infected as a result of the 404 incidents. On average, this gives rise to an average of 16.06 PCs being infected in each of the incidents. However, it should be noted that there is an organization which has a very large number of occurrences (200 times), with 30 PCs infected during each of the 200 infections. If this organization were excluded from the calculation, there were a total of 460 PCs being infected in 204 separate incidents, with an average of 2.25 PCs being infected per incident. These figures are believed to be more representative than the previous figures because the very large number of infections in the particular organization is really a unique case and should not be treated as the same with the other cases.

Table 19

Number of IBM PC Infected During Each Infection in the Organizations

Number of PC Infected	Number of Respondents	Percentage	Total PC Infected
0	3	0.74	0
1	127	31.44	127
2	50	12.38	100
3	3	0.74	9
4	2	0.50	8
5	3	0.74	15
6	1	0.25	6
10	3	0.74	30
13	10	2.48	130
30	201	49.75	6030
35	1	0.25	35
	404	100.00	6490

5.3.5 Time taken for the eradication of each incident in the organizations

The following table summarises the time taken for each of the viruses to be cleaned or removed from PC. In 2 separate incidents, the viruses, contained in floppy disks, were detected before any PC was infected. Therefore, there was no need to eradicate the viruses from PC for these 2 incidents.

Table 20 shows that more than 84% of the organizations took less than 10 minutes to perform the clean-up procedures in the event of an IBM PC virus attack. However, in 5 separate incidents, the clean-up took between 1 and 3 days.

Table 20

Time Taken to Clean the Virus in Each Incident in the Organizations

Time Taken	Number of Respondents	Percentage
Not Applicable	2	0.50
1 - 10 minutes	340	84.16
20 minutes	8	1.98
30 minutes	19	4.70
1 - 2 hours	12	2.97
2 - 3 hours	15	3.71
3 - 5 hours	3	0.74
1 1/2 day	2	0.50
2 - 3 days	3	0.74
	404	100.00

5.3.6 Additional costs associated with each infection in the organizations

Of the 27 organizations that have at least one encounter with an IBM PC viruses, only 2 (7.41%) reported to have additional costs associated with each clean-up of the infecting viruses. On one occasion, external contractor had to be asked to solve the problem, twice, which cost approximately a total of $300. In the other incident, hard disks drives had to be purchased as a result of the incident, which eventually cost the organization a total of $500.

5.3.7 Major perpetrators classification

Table 21 compares reported occurrences of IBM PC virus incidents according to the broad classifications of user staff, computer staff, external personnel, software vendor, and those unable to be identified

The table indicates that approximately 80% of the perpetrations can be attributed to the user staff of the organizations with those unable to be identified make up the other 20% of the perpetrations.

Table 21
Person Responsible for Introducing the Virus to the Organizations

Perpetrator	Number of Respondents	Percentage
User staff	315	77.97
Computer staff	6	1.49
External personnel	2	0.50
Software vendor	1	0.25
Unknown	80	19.80
	404	100.00

5.3.8 Actions taken as a result of each infection in the organizations

The following table summarises the action (or actions) taken as a result of each of the IBM PC virus incidents in the organizations. Of particular note is that in the aftermath of 65.84% of the incidents no action whatsoever was taken by the victimised organizations.

Table 22
Actions Taken in Each of the Incidents in the Organizations

Action Taken	Number of Respondents	Percentage
None	266	65.84
Formal Enquiry	2	0.50
Informal Enquiry	45	11.14
Educate User (Awareness Campaign)	91	22.52
	404	100.00

5.4 IBM PC Virus Controls

This section is devoted to a review of the control mechanisms and procedures in relation to IBM PC viruses that are used in the organizations surveyed.

5.4.1 Formal reporting and recording of IBM PC viruses procedures in the organizations

In 17 (40.48%) of the 42 organizations formal reporting and recording of IBM PC viruses procedures are employed. Of those who do not keep a log of the incidents (n = 25), 44% (n = 11) cited IBM PC viruses, as a form of computer abuse, is a relatively minor problem in their organization and therefore, recording of the incidents is not necessary. Another 28% (n = 7) claimed that a log is unnecessary because they have never had any infection before.

5.4.2 Formal IBM PC viruses clean-up procedures in the organizations

In this paper, *formal clean-up procedures* is taken to mean that in the event of a virus attack, an organization has some means to eradicate the infecting viruses. Anti-viral software are usually used to perform the clean-up procedures.

The survey has found that in 39 (92.86%) of the 42 organizations formal clean-up procedures of IBM PC viruses are employed. Of those who have no formal clean-up of IBM PC viruses procedures, 100% (n = 3) cited because they have never had any encounter with any IBM PC viruses before, therefore the clean-up procedures are not necessary.

5.4.3 Formal Contingency (or Disaster Recovery) Plan in the organizations

In 11 (26.19%) of the 42 organizations a formal Contingency plan in relation to IBM PC viruses is adopted to ensure minimal interruption to normal business operations to the organization's IBM PCs in the event of an IBM PC virus attack.

5.4.4 Storing of back-up copies of original software in the organizations

In 26 (92.86%) of the 28 organizations that have networking systems, there is a policy that prescribes storing back-up copies of original software for IBM PCs that are linked to the networks as soon as the package is open. However, only 4 (14.29%) out of the 26 organizations store back-up copies of original software at the *offsite* location. In 39 (92.86%) of the 42 organizations, back-up copies of original software used in stand-alone IBM PCs are stored as soon as the package is open. However, only 8 (19.05%) out of the 39 organizations store the back-up copies at the offsite location, as illustrated in Table 23.

Table 23

Storing of Back-up Copies of Original Software in the Organizations

	Back-up				*No Back-up*		*Total*	
	Onsite		Offsite					
	No	%	No	%	No	%	No	%
Software In Networked PCs	22	78.57	4	14.29	2	7.14	28	100
Software In Stand-alone PCs	31	73.81	8	19.05	3	7.14	42	100

5.4.5 Creating of back-up copies of all applications and data in the organizations

In all (100%, $n = 28$) organizations that have networking systems, there is a policy that prescribes creating back-up copies of all applications and associated data for

IBM PCs that are linked to the networks on a regular basis. Seventeen (60.71%) of the 28 organizations create back-ups on a daily basis; two (7.14%) create back-ups once a week; and nine (32.14%) do not have a fixed date to create back-ups.

For stand-alone IBM PCs, a policy that prescribes creating back-up copies of all applications and data are found in only 3 (7.14%) out of the 42 organizations. In other words, in 92.86% of organizations, the onus is on the users of the stand-alone PCs to create their own back-up regularly. This is understandable because it is generally not economically feasible to perform back-up on behalf of all of the users of stand-alone PCs within an organization.

Table 24

Creating of Back-up Copies of All Applications and Data in the Organizations

	Creating Back-up		*No Back-up*		*Total*	
	No	%	No	%	No	%
Software In Networked PCs	28	100.00	0	0.00	28	100.00
Software In Stand-alone PCs	3	7.14	39	92.86	42	100.00

5.4.6 Testing of back-up and recovery procedures in the organizations

There is a policy that prescribes testing standard procedures for back-up and recoveries for IBM PCs that are linked to the networks in 21 (75%) of the 28 organizations that have networking systems. However, for stand-alone IBM PCs, a policy that prescribes testing standard procedures for back-up and recoveries for IBM PCs is found in only 4 (9.52%) out of the 42 organizations. Table 25 depicts the frequency with which the organizations carry out the testing of the back-up and recovery procedures. Table 26 depicts the last time with which the organizations test the back-up and recovery procedures.

Table 25

Frequency with Which the Organizations Carry Out the Testing of the Back-up and Recovery Procedures

	Number of Respondents	Percentage
When Changes Are Introduced	14	56.00
Daily	1	4.00
Once A Week	2	8.00
Once a Month	2	8.00
Twice A Year	3	12.00
Once a Year	3	12.00
	25	100.00

Table 26

The Last Time the Testing of the Back-up and Recovery Procedures was Carried Out in the Organizations

	Number of Respondents	Percentage
Within The Last Two Weeks	4	16.00
Four Weeks Ago	3	12.00
Two Months Ago	3	12.00
Six Months Ago	7	28.00
Nine Months Ago	1	4.00
One Year Ago	6	24.00
Two Years Ago	1	4.00
	25	100.00

5.4.7 Assigning personnel to specific responsibilities regarding back-up procedures in the organizations

In 24 (85.71%) of the 28 organizations that have networking systems, personnel is assigned to specific responsibilities regarding back-up procedures for IBM PCs that are linked to the networks. However, all 42 organizations (100%) do not see a need to assign personnel to specific responsibilities regarding back-up procedures for all stand-alone IBM PCs, as shown in Table 27.

Table 27

Assigning Personnel to Specific Responsibilities Regarding Back-up Procedures in the Organizations

	Assign Personnel		*No Personnel Assigned*		*Total*	
	No	%	No	%	No	%
Software In Networked PCs	24	85.71	4	14.29	28	100
Software In Stand-alone PCs	0	0.00	32	100.00	32	100

5.4.8 Antiviral software used in the organizations

In 37 (88.10%) of the organizations, at least one antiviral software package or system is used to ensure minimal interruption to normal business operations to the organization's IBM PCs in the event of an IBM PC virus attack. The number of antiviral software used in the organizations is set out in Table 28. The types of the individual antiviral software used in the organizations is listed in Table 29.

Table 28

Number of Antiviral Software Used in the Organizations

Number of Antiviral Software Used	Number of Respondents	Percentage	Total Number of A. Software
1	27	72.97	27
2	8	21.62	16
3	1	2.70	3
4	1	2.70	4
	37	100.00	50

Table 29
Antiviral Software Used in the Organizations

Antiviral Software	Number of Respondents	Percentage
Scan	22	44.00
Virus Buster	6	12.00
Doctor Solomon's Toolkit	5	10.00
Norton AntiVirus	5	10.00
IBM Virus Scan	3	6.00
Virucide	2	4.00
Central Point Software	1	2.00
F_Prot	1	2.00
Flu_Shot Plus	1	2.00
Victor Charlie	1	2.00
ViruSafe	1	2.00
Virustop	1	2.00
Virusfix	1	2.00
	50	100.00

5.4.9 Software acquisition policy in the organizations

In 35 (83.33%) of organizations, a Software Acquisition policy is maintained to control and inspect all software brought into the organization's IBM PCs. For those who have a Software Acquisition policy (n = 35):

- 97.14% (n = 34) of respondents prescribe purchasing software only from reputable vendors and accepting only software received in original sealed packaging;
- 74.29% (n = 26) of respondents prescribe reviewing, inspecting and testing new software as well as upgrades to existing software before installation; and
- 74.29% (n = 26) of respondents accept shareware or freeware into their organizations' IBM PCs. Twenty four (92.31%) of the 26 organizations that accept shareware or freeware into their organizations' IBM PCs will test any shareware or freeware prior to use in production.

Chapter Six

Discussion of the Survey

6.1 Organization Profiles

The data in Tables 4, 5 and 6 indicate the sizes of the organizations included in the survey. The organizations surveyed are generally large, with over 52% of them having between 51 and 300 staff and approximately 90% of them having a *computing* (or *computer services* or *IT) section.* However, these sections are, in general, small with 58% of them having less than 10 staff.

6.2 Profile of the IBM PC Use

6.2.1 IBM PC

The data in Table 7 confirms the view that IBM PCs are in wide spread use with approximately 12% of those surveyed having more than 500 IBM PCs in their organization and that on average, the number of IBM PCs each organization owns is 170.

The data in Table 9 suggests that there is almost a one for one correspondence between the number of IBM PCs and the number of IBM PC users. This is significant from a computer virus research perspective because it implies that there is unlikely to be a large population using the one machine or

several machines and sharing disks. Thus, the likelihood of transmitting viruses through sharing disks may be reduced.

The data in Table 11 show that the organizations surveyed are *experienced* with more than 71% of them having over 6 years of experience with IBM PC (and clones) environment, given that IBM PC (and clones) has been available in Australia for approximately a decade. Again this is significant from a computer virus research perspective as experienced users are more likely to be aware of the problems and transfer mechanisms associated with computer viruses.

6.2.2 Apple Macintosh

Although this survey was not examining computer viruses associated with Apple Macintosh PCs, data was gathered on these PCs because it was considered worthwhile to establish the penetration of these systems into the PC market in the State Government sector to consider whether research into Apple Macintosh viruses could be justified. If these Macintosh systems represented a significantly high proportion of investment then more attention could be devoted to addressing virus problems in this environment.

As it transpired, the data in Table 8 show that approximately 80% of the organizations surveyed had less than 15 Macintoshs and 43% had none at all. In fact, Table 10 shows that 75% of the organizations had less than 10 staff who regularly used Macintosh computers. These data suggest that the most common businness PC in use in this sector was the IBM style machine. This area would then be most likely to be require more attention for support in virus research.

6.2.3 Network connections

The transfer of computer viruses across networks has been seen as a major threat and the data in Tables 12 show that the use of IBM PC style networks is

reasonably common with two third of the organisations surveyed having at least one newtork of this type. Table 13 shows that 15% of these networks have more than 50 PCs linked to them.

The types of network operating system (NOS) environments are listed in Table 14 and the implications for virus security differs in each case. Table 14 shows that the two most popular NOSs are Novell's NetWare and 3COM's 3+ Open. This is in accordance with Christianson, King, & Munger's (1990, p. 6) claim that "the most popular NOS is NetWare, . . . which has an estimated 65% of market share" and that "3+ Open . . . is probably the second most popular system, with about a 10-15% market share."

The data in Table 15 show that in two third of the cases, if the network in use in the organizations were put out of action, it would have major effects on company operation. This suggests that organizations have increasingly come to reply on the use of network systems and that the non-availability of these systems would have far reaching consequences to the affected organizations. Therefore, from the standpoint of computer virus reseach, network security is a worth-while effort.

6.2.4 External connections

It is also argued that the use of dial-in/out connections has the potential to transfer viruses in much the same way as a network but is even more dangerous in that external intrusion may occur. In only 35% of the organizations surveyed was external dial-in capability allowed. However, only 26% of these organizations use a dial-back system to allow only access from an approved list of numbers. Most of the 11 organizations that do not use the dial back system are relying on stand-alone systems and the password mechanism to prevent unauthorised access.

6.3 IBM PC Virus Problem Experience

6.3.1 Perceived seriousness

With regard to the perceived seriousness of computer virus infections, Table 16 shows that more than one third (35%) of the respondents did not see any problem. Another 58% claim it was only a minor problem. In fact only 7% of the respondents regard computer virus infections as reasonably serious or as a major problem.

This is a surprising result and may reflect the mechanisms and procedures which have been established effectively to prevent computer viruses becoming a problem. For example, Table 28 shows that more than 88% of the organizations have at least one antiviral software and that more than 84% of the organizations (from Table 20) claimed that it took them less than 10 minutes to perform the clean-up procedures in the event of an IBM PC virus attack.

It may even be that the use of anti-viral software has lulled users into a false sense of security thinking they are "protected" against viruses (Zajac, 1992, p. 225). However, it should be noted that anti-viral software is not a panacea because it will not protect against all viruses but only the known ones. Furthermore, it is possible that even with an anti-viral program in place, an organization could still be a victim of an attack because the virus had a new twist to beat the anti-viral software. To quote Zajac (1992, p. 225), "anti-viral software is only a treatment, not a cure or vaccine to the viral problem."

6.3.2 Infection type

The main purpose of this study was to investigate and quantify the infection types and rates of IBM PC viruses in the Western Australian State Government

organizations. Table 18 shows that there were a total of 15 unique IBM PC viruses that were known to infect the responding organizations.

The following table shows the *types* of each of the 15 unique IBM PC viruses that are known to have infected the responding organizations, and the *damage done* by these viruses. As mentioned, this classification method is based on the one used by VIRUSCAN Version 8.4B89 (1992).

Table 30

Infection Types of the 15 Known IBM PC Viruses in the Organizations and the Damage Done by These Viruses

Name of Virus	Type*	Damage Done**
1559	2,3,4,5,6	O,P,L
1575	3,4,5,6	O,P,L
Dark Avenger	3,4,5,6,7	O,P,L
Den Zuk	3,8	O,B
(Search)		
Flip	2,3,4,5,6,7	O,P,D,L
Form	3,8,9	B,O,D
Italian	3,8,9	O,B
(Pingpong, Friday the 15th, Israel)		
Jerusalem	3,5,6,7	O,P
(Jerusalem B)		
Keypress	3,4,5,6	O,P,D
(Turku, Twins)		
Liberty	3,4,5,6,7	O,P
(Magic, Mystic)		
Michelangelo	3,8,9,A	B,O
New Zealand	3,8,A	O,B,L
(Stoned, Marijuana)		
No-Int	3,8,A	O,B,L
(New Zealand, Stoned, Marijuana)		
Ohio	3,8	B,O
(Hacker)		
Slow	2,3,5,6,7	O,P,L

* *Type Codes*

1 = Virus uses Stealth Techniques
2 = Virus uses self-encryption
3 = Virus install self in memory
4 = Infects COMMAND.COM
5 = Infects COM files
6 = Infects EXE files
7 = Infects Overlay files
8 = Infects floppy diskette boot
9 = Infects fixed disk boot sector
A = Infects fixed disk partition table

```
**      Damage Fields
        B = Corrupts or overwrites the boot sector
        D = Corrupts data files
        F = Formats or overwrites all/part of disk
        L = Directly or indirectly corrupts file linkage
        O = Affects system run-time operation
        P = Corrupts program or overlay files
```

From Table 30, it is apparent that of the 15 known viruses that are known to have infected the respondents:

- none (0%) of them uses Stealth techniques;
- 3 (20%) of them use self-encryption techniques;
- all 15 (100%) of them are memory-resident after infection;
- 6 (40%) of them infect COMMAND.COM file;
- 8 (53.33%) of them infect COM files;
- 8 (53.33%) of them infect EXE files;
- 5 (33.33%) of them infect overlay files;
- 7 (46.67%) of them infect floppy diskette boot;
- 3 (20%) of them infect fixed disk boot sector; and
- 3 (20%) of them infect fixed disk partition table (aka master boot record).

Table 30 also shows that of the 15 known viruses that are known to have infected the respondents:

- all 15 (100%) of them affect system run-time operation;
- 8 (53.33%) of them corrupt program or overlay files;
- 7 (46.67%) of them directly or indirectly corrupt file linkage
- 7 (46.67%) of them corrupt or overwrite the boot sector;
- 3 (20%) of them corrupt data files; and
- none (0%) of them formats or overwrites all or part of disk.

6.3.3 Reinfection rate

In this paper, *reinfection* is taken to mean that a particular computer virus reinfects an organization's PC (or PCs) after the first infection of the *same* virus has been eradicated.

Reinfection occurred in 18 (66.67%) of the 27 organizations that had at least one encounter with an IBM PC virus over the years. Table 31 shows the number of times the reinfection of the viruses in the organizations had occurred.

From Table 31, it is evident that over 47% of the time reinfection is occurred only once and that there were a total of 333 reinfections out of a total of 404 separate incidents, which makes the reinfection rate stands at 82.43%.

Table 31
Number of Reinfections of Viruses in the Organizations

Number of Times Reinfected	Number of Respondents	Percentage	Total Number of Reinfections
1	16	47.06	16
2	1	2.94	2
4	4	11.76	16
5	2	5.88	10
7	1	2.94	7
9	2	5.88	18
11	1	2.94	11
14	3	8.82	42
19	1	2.94	19
26	1	2.94	26
67	1	2.94	67
99	1	2.94	99
	34	100.00	333

6.3.4 Spafford's (1990) speculation

The data in Table 18 show that 4 IBM PC viruses (i.e., **New Zealand**, **Michelangelo**, **Liberty**, and **Jerusalem**) account for 367 out of the 404 incidents in the responding organizations, or an equivalent of 90.84% of all infections.

Thus, Spafford's speculation that less than 10 viruses account for 90% of all infections holds true in the Western Australian State Government organizations environment.

6.3.5 Comparison with the 1991 Dataquest survey

A comparison of the known infecting viruses with Dataquest's 1991 Computer Virus Market Survey is tabulated in Table 32.

Table 32

A Western Australia - U.S. Computer Viruses by Types Comparison of Infections

Computer Virus	United States	Western Australia
New Zealand	48%	46.78%
Jerusalem	37%	1.98%
Joshi	8%	-
Michelangelo	-	34.16%
Liberty	-	7.92%
	93%	90.84%

The most striking aspect of Table 32 is that Spafford's (1990) speculation that less than 10 viruses account for 90% of infections holds true for both surveys.

Dataquest's survey reveals that 63% of respondents reported at least one encounter with a virus in 1991 whereas the present study's survey shows that 64.29% of the responding organizations reported at least one IBM PC virus infection over the years.

6.3.6 Major perpetrators classification

The data from Table 21 indicates that the user staff of the organizations account for approximately 80% of the perpetrations with those unable to be identified nearly make up the other 20% of the perpetrations. Clearly, this is an area where effective control can be applied. The user staff of the organizations have to be

educated to be aware of the viruses problem, and means by which viruses can be transmitted. By doing so, the threat of the viruses may be reduced since collectively, the user staff of the organizations account for 8 out of 10 perpetrations.

6.4 IBM PC Virus Controls

Prior to the commencement of this study it had been assumed that there would be difficulty in both detecting whether particular problems had been caused by viruses and secondly if a particular problem had been encountered had the virus been identified. As it transpired, the interview situation in which the questionnaire was administered provided an indication that the anticipated virus identification problems did not arise in that the organizations surveyed appeared to be well informed and have the tools to identify viruses infecting them. Of all the viruses detected only seven incidents (1.73%) could not be identified positively.

A close examination of the data showed that the control mechanisms and procedures of the organizations surveyed, in general, are adequate. For example:

- formal clean-up of IBM PC viruses procedures are in place in over 92% of the organizations;
- over 92% of the organizations prescibe storing, mostly onsite, back-up copies of original software that are used in both networked and stand-alone PCs;[38]
- all organizations (100%) prescribe creating back-up copies of all applications and associated data for networked PCs on a regular basis;

38 This is to allow restoration of a system that has been contaminated by a time-released virus.

- the standard procedures for back-up and recoveries for the networked IBM PCs are tested and reviewed regularly in 75% of the organizations that have networking system;
- personnel are assigned specific responsibilities regarding back-up procedures in over 85% of the organizations that have networking systems;
- over 88% of the organizations use at least one anti-viral software package to ensure minimal interruption to normal business operations to their IBM PCs in the event of an IBM PC virus attack;
- a Software Acquisition policy is maintained in over 83% of the organizations to control and inspect all software brought into their IBM PCs; and
- no fewer than 74% of the organizations that have the Software Acquisition policy realise the importance of:
  - purchasing software only from reputable vendor and accepting only software received in original sealed packaging;
  - reviewing, inspecting and testing new software as well as upgrades to existing software before installation; and
  - testing any shareware, freeware in quarantine (e.g., test or development machine or stand-alone PCs) prior to use in production.

Nevertheless, there are two aspects of the virus control mechanisms and procedures in the organizations that are found to be inadequate: only approximately 40% of the organizations keep a formal reporting and recording of the virus incidents in their organizations; and a Contingency (or Disaster Recovery) plan in relation to IBM PC viruses are in place in only 26% of the organizations.

To effectively control the virus problem, the importance of having a Contingency plan and keeping a log of all virus incidents cannot be stressed enough.

Given that the organizations surveyed are, in general, large with many staff (as shown in Tables 4, 5, and 6) and that the user organizations are *experienced* with more than 70% having more than 5 years experience with the IBM PC (and compatibles) environment, one would assume that these two aspects of virus controls would not be overlooked. One clue to this phenomenon may be that over 92% of the respondents regard computer virus infections as a relatively minor problem. Nevertheless, regardless of the reasons, these two aspects of virus controls are very important and should receive increased consideration.

Chapter Seven

Conclusion

7.1 Summary of the Survey Findings

The major findings from an analysis of this survey are that:

- With regard to the perceived seriousness of computer virus infections, over 92% of the respondents regard computer virus infections as a relatively minor problem.
- 64.29% of respondents reported at least one encounter with an IBM PC virus during the period from 1989 to April 1992;
- Over 55% of the organizations surveyed have between 1 and 4 infections during the period from 1989 to April 1992; the average number of incidents per organization is 8;
- With the exception of one organization, 2.25 PCs, on average, were infected in each incidents, which is negligible when compared to an average of 170 PCs each organization owns;
- **New Zealand** (or **Stoned** or **Marijuana**) was responsible for 46.78% of all attacks, **Michelangelo** for 34.16%, **Liberty** (or **Mystic** or **Magic**) for 7.92% and **Jerusalem** (or **Jerusalem B**) for 1.98%; together these 4 viruses account for over 90% of all infections;
- Over 84% of respondents reported that the clean-up procedures of the infecting viruses took less than 10 minutes;

- Apart from interruption of business operations and loss of productivity, additional costs associated with each clean-up of the infecting viruses is reported in approximately 7% of cases;
- In 78% of cases, the infecting viruses were introduced by the user staff of the organizations;
- No action (other than clean-up) was taken in the aftermath of 66% of the incidents;
- Over 59% of the organizations do not have a formal reporting and recording of viruses procedures;
- Formal clean-up of IBM PC viruses procedures are in place in over 92% of the organizations;
- Over 73% of the organizations do not have a formal Contingency (or disaster recovery) plan in relation to computer viruses;
- Over 92% of the organizations prescibe storing, mostly onsite, back-up copies of original software that are used in both networked and stand-alone PCs;
- All organizations (100%) prescribe creating back-up copies of all applications and associated data for networked PCs on a regular basis;
- The standard procedures for back-up and recoveries for the networked IBM PCs are tested and reviewed regularly in 75% of the organizations that have networking system;
- Personnel are assigned specific responsibilities regarding back-up procedures in over 85% of the organizations that have networking systems;
- Over 88% of the organizations use at least one anti-viral software package to ensure minimal interruption to normal business operations to their IBM PCs in the event of an IBM PC virus attack; and

- A Software Acquisition policy is maintained in over 83% of the organizations to control and inspect all software brought into their IBM PCs.

7.2 Future Research Directions

7.2.1 Comparison study with other states and sectors

The present study was designed to investigate the State Government IT sector of Western Australia. Clearly this study was based on assumptions of homogeneity across Australia and other sectors which may not hold. Some future comparison study with other states and sectors would be a fruitful area for further research to test this assumption.

7.2.2 Follow up study

A follow up study to examine trends in frequency and type of virus is worthy of some future study as it is expected further viruses of the current types in addition to new types will become manifest for some time yet.

7.2.3 Detailed analysis

A detailed analysis of the relationships between the number and type of computer viruses and other factors (e.g., size of organization, size of network) to examine whether a different scale of operation and infrastructure may affect outcomes in this field is another area worthy of some further study.

7.2.4 Taxonomy of viruses by types

As mentioned in section 1.4, there is general disagreement among researchers regarding the classification of the various viruses by types and this debate is likely to continue. Nevertheless, perhaps clarification could be achieved in the concepts of "generic viruses" which could be categorised in a taxonomy. This would be a fruitful area for further research although the changing nature of viruses must leave this open to continual adjustment.

7.2.5 Universal Virus Detector (UVD)

A UVD is a program which can perform static or dynamic analysis of programs and determine with 100% certainty whether the programs contain a virus or not. The most difficult task would be for the UVD to determine *when* a virus infection had actually occurred. This is partially because of the lack of a precise definition of the term "virus". One solution is to develop "generic viruses" which will be of great help in developing a generic virus defence or collection of generic strategies.

7.2.6 Stealth Viruses Detection

Another area worthy of further research is to propose mechanisms and techniques for the detection of the so-called "Stealth" viruses. This area is rather specific in that the research will only concentrate on the detection methods of one of many types of viruses. This area also represents specific leading area research in the computer virus field.

7.3 Conclusion

This paper presents the results of an extensive survey undertaken in a number of government based user environments in Western Australia. The study has accomplished several objectives:

- It provides *factual* information regarding the nature and prevalence of the virus infections in the Western Australian environment, in particular, the infection types and rates of IBM PC viruses in the W.A. State Government sector;
- It sets a base line of viruses information for government organizations in W.A. and provides a comparison with overseas findings;
- It provides current evidence that there is a problem in the work environment in W.A. as opposed to the creation and isolation of computer viruses in laboratories of computer science;
- It identifies what other people are doing with similar problems or situations and benefit from their experience in making future plans and decisions;
- It ratifies the propositions that currently very few of the viruses contribute to the vast majority of infections in the Western Australian workplace.

Bibliography

Adams, T. (1989). A plague of viruses and other vermin: Working paper no. 1. Melbourne, Australia: Royal Melbourne Institute of Technology (RMIT) Ltd.

Alexander, M. (1988, November 7). Virus [sic] ravages thousands of systems. Computerworld, pp. 1, 157.

Baker, R. H. (1991). Computer security handbook. (2nd ed.). Blue Ridge Summit, PA: TAB Professional and Reference Books.

Bloombecker, J. J. (1988, Winter). Measuring the byte of computer crime. Computer Control Quarterly, 6-8.

Bloombecker, J. J. (1989, October 1). Short-circuiting computer crime. Datamation, 71-72.

Borg, W. R. (1963). Educational research. New York: David McKay Company, Inc.

Borg, W. R., & Gall, M. D. (1979). Educational research: An introduction. (3rd ed.). New York: Longman.

Borrett, L. (1990). Virus attacks should be planned for. Computer control quarterly, 8 (2), 37-39.

Bright, G. (1989, June). Computers need better security. Security Australia, 9 (5), 23-30.

Brunner, J. (1975). The shockwave rider. New York: Ballantine.

Campbell, A. A., & Katona, G. (1953). The sample survey: A technique for social science research. In L. Festinger and D. Katz (Eds.), Research methods in the behavioural sciences (pp. 15-55). New York: Dryden Press.

Cerf, V. (1989, June). Statements of ethics: Ethics and the Internet. Communications of the ACM, 32 (6), p. 710.

Christianson, P., King, S., & Munger, M. (1990). Networking with Novell® NetWare®: A LAN manager's handbook. Blue Ridge Summit, Pitsburgh: Windcrest Books.

Cohen, F. (1984). Computer viruses - Theory and experiments. DOD/NBS 7th National Conference on Computer Security. (Originally appearing in IFIP-Sec'84, also appearing in Computers & Security, 6, 22-35 and several other publications in several languages.)

Cohen, F. B. (1986). Computer viruses. (Doctoral dissertation, University of Southern California.) Pittsburgh, Pennsylvania: ASP Press.

Cohen, F. (1987, December). A Cryptographic checksum for integrity protection. Computers & Security, 6 (6), 505-510.

Cohen, F. (1988, April). On the implications of computer viruses and methods of defense. Computers & Security, 7 (4), 167-184.

Cohen, F. (1989). Models of practical defenses against computer viruses. Computers & Security, 8, 149-160.

Cohen, F. (1990). Implications of computer viruses and current methods of defense. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 381-406). Reading, Massachusetts: Addison-Wesley Publishing Company. (This is an updated version of a paper that first appeared in Computers & Security, 7 (4), pp. 167-184 in April 1988.)

Davis, F. G. F., & Gantenbein, R. E. (1987). Recovering from a computer virus attack. Systems and Software, 7, 253-258.

Denning, P. J. (1989, March-April). The Internet worm. American Scientist, 77 (2), 126-128.

Denning, P. J. (1990). The ARPANET after twenty years. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 11-19). Reading, Massachusetts: Addison-Wesley Publishing Company. (Reprinted from American Scientist, November-December 1989, pp. 530-534.)

Denning, P. J. (Ed.). (1990). Computers under attack: Intruders, worms, and viruses. Reading, Massachusetts: Addison-Wesley Publishing Company.

Dewdney, A. (1985, March). Computer Recreations: A Core War bestiary of viruses, worms and other threats to computer memories. Scientific American, 14-18.

Dewdney, A. (1987, January). Computer Recreations: A program called Mice nibbles its way to victory at the first core war tournament. Scientific American, 8-11.

Dewdney, A. (1989, March). Computer Recreations: Of worms, viruses and Core War. Scientific American, 90-94.

Dierstein, R. (1987, Winter). Computer viruses: A secret threat. Computer Control Quarterly, 1-8.

al-Dossary, G. M. (1990). Computer virus prevention and containment on Mainframe. Computers & Security, 9 (2), 131-137.

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M. S., & Santoro, T. (1989, June). The Cornell commission: On Morris and the worm. Communications of the ACM, 32 (6), 706-709.

Elmer-DeWitt, P. (1988, September 26). Invasion of the data snatchers! Time, pp. 60-65.

Fak, V. (1988). Are we vulnerable to a virus attack? Computers & Security, 7, 151-155.

Farber, D. J. (1989, June). Statements of ethics: NSF poses code of networking ethics. Communications of the ACM, 32 (6), p. 688.

Ferbrache, D. (1990, June). Worm programs: The Internet worm - Action and reaction. Virus Bulletin, 13-17.

Fink, A., & Kosecoff, J. (1985). How to conduct surveys: A step by step guide. Beverly Hills: Sage Publications, Inc.

Fites, P., Johnston, P. & Kratz, M. (1992). The computer virus crisis. New York: Van Nostrand Reinhold.

Fitzgerald, K. J. (1989, Summer). Computer viruses. Computer Control Quarterly, 43-48.

Fowler, F. J. (1984). Survey research methods. Beverly Hills: Sage Publications, Inc.

Gardner, P. E. (1989). The Internet worm: What was said and when. Computers & Security, 8 (4), 291-296.

Gleissner, W. (1989). A mathematical theory for the spread of computer viruses. Computers & Security, 8, 35-41.

Grampp, F. T., & Morris, R. M. (1984, October). UNIX operating system security. AT&T Bell Laboratories Technical Journal, 63 (8), part 2, 1649-1672.

Grocot, R., Palmer, J., & Travis, J. (1990). Computer viruses in tertiary institutions: The Brain virus. Computer Control Quarterly, 8 (1), 22-24.

Hafner, K. M. (1988, August 1). Is your computer secure? Business Week, 50-56.

Highland, H. J. (1988a, October). Computer viruses: Media hyperbole, errors and ignorance. Computers & Security, 7 (5), 442-450.

Highland, H. J. (1988b). How to combat a computer virus. Computers & Security, 7, 157-162.

Highland, H. J. (1988c). Anatomy of a virus attack. Computers & Security, 7, 145-150.

Highland, H. J. (1988d). An overview of 18 virus protection products. Computers & Security, 7, 157-161.

Highland, H. J. (1990). Computer virus handbook. Oxford, England: Elsevier Science Publishers Ltd.

Hruska, J. (1992, January). Conference report: NCSA anti-virus product developers conference, November 25-26th, 1991. Virus Bulletin, 6-7.

Isaac, S., & Michael, W. B. (1981). Handbook in research and evaluation. (2nd ed.). San Diego, California: EdITS Publishers.

Jackson, K. (1988, November 14). Virus [sic] alters networking. Communications Week, pp. 1, 75.

Kamay, V., & Adams, T. (1989). January 1989 periodic figures on computer abuse. ACARB Newsletter, 2 (2), 2-16.

Kamay, V., & Adams, T. (1990). The 1990 profile of computer abuse in Australia. Computer Control Quarterly, 8 (4), 12-27.

Kerlinger, F. N. (1973). Foundations of behavioural research. (2nd ed.). New York: Holt, Rinehart, and Winston.

Kocher, B. (1989, June). A hygiene lesson. Communications of the ACM, 32 (3), pp. 3, 6.

Leiss, E. L. (1990). Software under siege: Viruses and worms. Oxford, England: Elsevier Science Publishers Ltd.

Letter bomb of the computer age. (1988, November 5). New York Times, A(16).

Longley, D., & Shain, M. (1989). Data & computer security: Dictionary of standards, concepts and terms. Hants, U.K.: Macmillan Publishers Ltd.

Markoff, J. (1988, November 5). Author of computer virus [sic] is son of U.S. electronic security expert. New York Times, A(1).

Marshall, E. (1988a). Worm invades computer networks. Science, 242, 855-856.

Marshall, E. (1988b). The worm's aftermath. Science, 242, 1121-1122.

McMillan, J. H., & Schumacher, S. (1989). Research education: A conceptual introduction. (2nd ed.). Glenview, Illinois: Scott, Foresman and Company.

Monk, T. (Ed.). (1990, February). News: Viruses infect Melbourne's Chisholm Institute. Computer Fraud & Security Bulletin, 4-5.

Monk, T. (Ed.). (1992, March). News: Virus survey. Computer Fraud & Security Bulletin, 5-6.

Montz, L. B. (1990a). The worm case: From indictment to verdict. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 260-263). Reading, Massachusetts: Addison-Wesley Publishing Company.

Montz, L. B. (1990b). U.S. General Accounting Office report highlights the need for improved Internet management. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 456-471). Reading, Massachusetts: Addison-Wesley Publishing Company.

Murray, W. H. (1988). The application of epidemiology to computer viruses. Computers & Security, 7, 139-145.

News track: Crime statistics (1989, June). Communications of the ACM, 32 (6), 657-658.

News track: Virus fever (1991, April). Communications of the ACM, 34 (4), 9-10.

Oppenheim, A. N. (1966). Questionnaire design and attitude measurement. New York: Basic Books, Inc.

Parker, D. B. (1976). Crime by computer. New York: Charles Scribners.

Palmer, I. C., & Potter, G. A. (1989). Computer security risk management. London: Jessica Kingsley Publishers Ltd.

Pozzo, M. M., & Gray, T. E. (1987). An approach to containing computer viruses. Computers & Security, 6, 321-331.

Quarterman, J. S., & Hoskins, J. C. (1990). Notable computer networks. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 20-96). Reading, Massachusetts: Addison-Wesley Publishing Company. (Reprinted from Communications of the ACM, 29 (10), October 1986, pp. 932-971.)

Radai, Y. (1989). The Israeli PC virus. Computers & Security, 8 (2), 111-113.

Reid, B. (1987, February). Reflections on some recent widespread computer breakins. Communications of the ACM, 30 (2), 103-105.

Rochlis, J. A., & Eichin, M. W. (1989, June). With microscope and tweezers: The worm from MIT's perspective. Communications of the ACM, 32 (6), 689-698.

Ross, S. J. (Ed.). (1989). Computer viruses: The proceedings of an invitational symposium, October 10-11, 1988. New York: Deloitte, Haskins & Sells.

Routh, R. L. (1984). A proposal for an architectural approach which apparently solves all known software-based internal computer security problems. Operating systems review, 18 (3), 31-39.

Scherlis, W. L., Squires, S. L., & Pethia, R. D. (1990). Computer emergency response. In P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 495-504). Reading, Massachusetts: Addison-Wesley Publishing Company.

Shoch, J. F., & Hupp, J. A. (1982, March). The "worm" programs - Early experience with a distributed computation. Communications of the ACM, 25 (3), 172-180.

Simons, G. (1989). Viruses, bugs and star wars. Oxford, England: NCC Blackwell.

Spafford, E. H. (1989). Crisis and aftermath. Communications of the ACM, 32 (6), 678-687.

Spafford, E. H. (1990). Computer viruses: Presentation for technology corporation, 28 May 1990 - 1 June 1990. West Lafayette, Indianapolis: Purdue University.

Spafford, E. H., Heaphy, K. A., & Ferbrache, D. J. (1990). A computer virus primer. In P. J. Denning (Ed.), Computers under attack: Intruders, worms,

and viruses (pp. 316-355). Reading, Massachusetts: Addison-Wesley Publishing Company. (Excerpted from Computer viruses: Dealing with electronic vandalism and programmed threats. Published by ADAPSO, the computer software and services industry association, 1989.)

Stoll, C. (1988, May). Stalking the wily hacker. Communications of the ACM, 31 (5), 484-497.

The Computer Virus Handbook. (no date). (Available from Price Waterhouse, Perth).

Thompson, K. (1984, August). Reflections on trusting trust. Communications of the ACM, 27 (8), 761-763.

Tuckman, B. W. (1988). Conducting educational research. (3rd ed.). San Diego: Harcourt Brace Jovanovich, Inc.

VIRUSCAN Version 8.4B89 [Computer program]. (1992). Santa Clara, California: McAfee Associates.

Webster, A. E. (1989). University of Delaware and the Pakistani computer virus. Computers & Security, 8 (2), 103-105.

White, C. E., Jr., (1989). Viruses and worms: A campus under attack. Computers & Security, 8 (4), 283-290.

Wilding, E. (Ed.). (1990a, August). For management. The enemy within: Bomb programs & Trojan Horses. Virus Bulletin, 4-6.

Wilding, E. (Ed.). (1990b, September). Technical notes: "Companion" viruses. Virus Bulletin, p. 3.

Wilding, E. (Ed.). (1991a, July). Editorial. Virus Bulletin, p. 2.

Wilding, E. (Ed.). (1991b, July). Known IBM PC viruses. Virus Bulletin, 12-33.

Wilding, E. (Ed.). (1991, December). Technical notes: Virus prevalence table. Virus Bulletin, p. 4.

Wilding, E. (Ed.). (1992, April). Technical notes: Virus prevalence table. Virus Bulletin, p. 6.

Wiseman, S. (1989). Preventing viruses in computer systems. Computers & Security, 8 (5), 427-432.

Witten, I. H. (1987, Summer). Computer (in)security: Infiltrating open systems. Abacus, 4 (4), 7-25. (Also appears in P. J. Denning (Ed.), Computers under attack: Intruders, worms, and viruses (pp. 105-142). Reading, Massachusetts: Addison-Wesley Publishing Company.)

Wong, K., & Watt, S. (1990). Managing information security: A non-technical management guide. Oxford, England: Elsevier Science Publishers Ltd.

van Wyk, K. R. (1989). The Lehigh virus. Computers & Security, 8 (2), 107-110.

Zajac, B. P., Jr. (1988, May-June). Computer viruses: The new global threat. The Computer Law and Security Report, 2-3.

Zajac, B. P., Jr. (1990). Computer viruses: Can they be prevented? Computers & Security, 9, 25-31.

Zajac, B. P., Jr. (1992). Cost-effectiveness of anti-viral software. Computers & Security, 11 (3), 217-226.

Appendix 1

Known IBM PC computer viruses (as of July 1991)

Known IBM PC computer viruses (as of July 1991)
(adapted from "Known IBM", 1991)

Name	Aliases	Type*
8 Tunes		CER
10-past-3		CR
268-Plus		CN
432		C?
483		CER
535A		CN
555	Dutch 555	CER
777 Revenge		CR
800		CR
905		ER
928		CER
1024PrScr		CR
1028		CER
1067		CR
1077		CER
1226		CR
1260	V2P1	CN
1575		CER
1600		CER
2100		CER
2144		CER
2480		CR
3445		CER
5120		CEN
4K	4096, Frodo, IDF, Israeli Defence Forces	CER
Advent		CEN
Aircop		DR
Agiplan		CR
AIDS		CN
AIDS II		PN
Akuku		CER
Alabama		ER
Ambulance	RedX	CN
Amoeba		CER
Amstrad		CN
Amstrad-852		CN
Amstrad-877		CN
Anthrax		MCER
AntiCAD	Plastique	CER
AntiCAD 2576		CER
AntiCAD/Plastique	3004	CER

* *Type Codes*

C = Infects COM files
D = Infects DOS boot sector (Logical Sector 0 on disk)
E = Infects EXE files
M = Infects master boot sector (Track 0, Head 0, Sector 1 on disk)
N = Not memory-resident after infection
P = Companion virus
R = Memory-resident after infection

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
Anti-Pascal (1)		CN
Anti-Pascal (2)		CN
Apocalypse		CER
Apocalypse II		CER
Arf		CN
Armagedon		CR
Attention		CR
Australian 403		CR
Azusa		DR
Backtime		CR
Bad Boy		CR
Bandit		EN
Bebe		CN
Best Wishes		CR
Big Joke		CN
Black Monday		CER
Bijec		CN
Blood		CN
Beijing	Bloody!	MR
Boys		CN
Brain	Ashar, Shoe	DR
Burger		CN
Burger 382		CN
Burger 405		CN
CARA		CR
Carioca		CR
Cascade	Fall, Russian, Hailstorm	CR
Cascade YAP		CR
Casino		CR
Casper		CN
Cemetery		ER
Christmas in Japan		CN
Christmas Tree	Father Christmas, Choinka	CN
Christmas Violator		CN
Cinderella		CR
Cookie		CER
Crazy Eddie		CER
Damage		CER
Dark Avenger		CER
Darklord		CER
Darth Vader		CR
Datacrime		CN
Datacrime II		CEN
Datalock		CER
dBASE		CR
DBF Blank		CER
December 24th		ER
Deicide		CN
Demon		CN
Den Zuk	Search	DR

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
Destructor		CER
Devil's Dance		CR
Diabolik		CER
Diamond	1024	CER
Diamond-1173	David	CER
Dir		CR
Discom		CR
Diskjeb		CER
Disk Killer	Ogre	DR
Do-nothing		CR
Doom2		CER
Doom II-B		CER
Dot Killer		CN
Durban	Saturday 14th	CER
Dyslexia	Solano	CR
Eddie-2	651	CER
Eddie-1801		CER
E.D.V.		DR
Enigma		ER
Erasmus		CER
ETC		CN
Evil		CR
Evil Empire		MR
Evil Empire B		MR
Faust	Spyer	CER
Fellowship		ER
Fichv 2.1		CN
Filler		DR
Finger		CER
Fish 6		CER
Flash		CER
Flip		MCER
Form		DR
Formiche		CR
Frog's Alley		CR
Fu Manchu		CER
F-word	USSR-417	CR
Gergana		CN
GhostBalls		CN
Goblin		CER
GP1		CER
Gremlin		CER
Grither		CN
Guppy		CR
Hallochen		CER
Hero		CER
HIV		CER
Horse	Hacker, Black horse	CER
Horse group		CER
Hybrid		CN

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
Hymn		CER
Icelandic	Saratoga	ER
INT13		CR
Internal		EN
Iraqui Warrior		CN
Italian	Pingpong, Bouncing Ball, Vera Cruz	DR
Itavir		EN
Jeff		CN
Jerusalem	PLO, Friday the 13th, Israeli	CER
Jo-Jo		CR
Jocker		
Joker-01		CR
Joshi		MR
July 13th		ER
Justice		CR
Kamikaze		EN
Kemerovo		CN
Kennedy		CN
Keypress	Turku, Twins	CER
Keypress-1228		CER
Kiev		CR
Klaeren		CER
Korea	NJH	DR
Kylie		CER
Lehigh		CR
Leprosy		CN
Leprosy-B		CER
Leszop		DR
Liberty	Magic, Mystic	DCER
Little Pieces		ER
Lozinsky		CR
LoveChild		CN
Lucifer		CER
Macho		CEN
Magnitogorsk	2560	CER
Mardi Bros		DR
MG		CR
MG-3		CR
MG-4		CR
MGTU		CN
Micro-128		CR
Microbes		DR
Migram-1		ER
Migram-2		ER
Minimal-30		CN
Minimal-45		CN
MIR		CER
Mirror		ER
Mistake	Typoboot	DR
MIX1		ER

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
MIX2		CER
MLTI		CR
Monxla	Time	CN
Monxla-B		CN
Murphy		CER
Murphy-3		CER
Murphy-4		CER
Music Bug		DR
Mutant		CN
New Zealand	Stoned, Marijuana	MR
Nina		CR
No Bock	440	CN
Nomenklatura		CER
NTKC	C-23693	CN
Number One		CN
Number of the Beast	666, V512	CR
Ohio	Hacker	DR
Old Yankee		EN
Ontario		CER
Oropax	Music virus	CR
Paris	TCC	CEN
Parity		CN
PcVrsDs		CER
Pentagon		DR
Perfume		CR
Perfume-731		CR
Pest		CER
Phantom		CR
Phenome		CER
Phoenix	P1	CR
Piter	Polish 529	CR
Pixel		CN
Pixel-257,275,295,283		CN
Pixel-892		CN
Pixel-779,837,850,854		CN
Pixel-936		CN
Plague		CR
Plastique 521		C?
Polimer		CN
Polish 217		CR
Pretoria	June 16th	CN
PrintScreen		DR
Protecto		C?
Proud		CR
Prudents		EN
PSQR		
Rat		ER
Raubkopi	Raub	CR
Russian Mirror		CR
Saddam		CR

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
Scott's Valley		CER
Sentinel		CR
September 18th		CEN
Sex Revolution		MR
Shake		CR
Simulation		CN
Skism		CER
Slow		CER
Smack	Patricia	CER
South African	Miami, Munich, Virus-B	CN
South African 408		CN
South African 416		CN
Spanish Telecom		MCER
Sparse		CR
Staf		CN
Striker 1		CN
Subliminal		CR
Sunday		CER
Suomi		CN
Suriv 1.01	April 1st COM	CR
Suriv 2.01	April 1st EXE	ER
Suriv 3.00	Israeli	CER
SVC		CER
SVC 3.1		CER
Sverdlov		CER
Svir		EN
Swami	Guru, Bhaktivedanta	CER
Swap		DR
Swedish disaster		MR
Swiss-143		CN
Sylvia		CN
Sylvia-2	Sylvia B	CN
Syslock		CEN
Taiwan		CN
Taiwan-C		CN
Taiwan-D		CN
Tenbyte	Valert	CER
Tequila		EMR
Terror		CER
Testvirus B		CN
Tiny		CN
Tiny Family		CR
TPworm		PN
Traceback	Spanish	CER
Trackswap		DR
Trilogy		?
Tumen		CR
TUQ	RPVS	CN
Turbo 448		CR
Turbo Kukac		CR

Known IBM PC computer viruses (as of July 1991)
[continue]

Name	Aliases	Type
Typo	Typo COM, Fumble	CR
USSR-311	V-311	CN
USSR-492	492	CR
USSR-516	516, Leapfrog	CR
USSR-600	600	CR
USSR-696	696	CN
USSR-707	707	CR
USSR-711	711	CR
USSR-948	948	CER
USSR-1049	1049	CER
USSR-1594		EN
USSR-2144		CER
V-1		DCR
V2P2		CN
V2P6		CN
Vacsina		CER
Vcomm		ER
VCS 1.0		CN
VFSI		CN
Victor		CEN
Vienna	Austrian, Unesco, DOS62, Lisbon	CN
Vienna-622		CN
Vienna-644		CN
Vienna-645		CN
Vienna-822		CN
Violator		CN
Virdem		CN
Virdem-792		CN
Virus-90		CN
Virus-101		CN
Virus-B		CN
Voronezh		CER
VP		CN
Vriest		CN
W13		CN
Warrior		EN
Westwood		CER
Whale		CER
Wisconsin	Death to Pascal	CR
Wolfman		CER
WWT		CN
XA1		CN
Yale	Alameda, Merritt	DR
Yankee		CER
Yaunch	Wench	EN
Yukon		CN
Zeleng		CER
Zero Bug	Palette	CR
Zero Hunt	Minnow	CR
ZK-900		CER

Appendix 2

Questionnaire for the Survey

Edith Cowan University
School of Information Technology and Mathematics

An Investigation of IBM PC Computer Viruses Infection Rates and Types in A Western Australian Environment

Subject No. __

A. Organization Profiles

1. To help estimate the approximate size of your organization, could you estimate the gross actual budget for the current financial year?
   $ _____ Million dollars

2. Approximately how many staff are employed in the whole organization?
   _____ people

3. Does your organization have a separate computing/computer services department?
   ( ) Yes
   ( ) No

   If YES:
   (a) How many staff (e.g., Operators, Programmers, Analysts, Management, Engineering Support, Vendor staff permanently on site, Consultant permanently on site) are there in the computing centre?
   _____ people

B. Profile of the IBM PC Use

4. How many IBM PCs (including IBM XT, AT, PS/2 and compatibles) are there currently in the whole organization?
   _____

5. How many Apple Macintoshs are there currently in the whole organization?
   _____

6. How many staff are IBM PC users in the whole organization?
   _____ people

7. How many staff are Macintosh users in the whole organization?
   _____ people

8. When did your organization obtain its first IBM PC?
   _____ months/years

9. Are any of the _____ IBM PCs in the whole organization networked?
   ( ) Yes
   ( ) No

   If YES:

(a) For each network,

(i) How many IBM PCs are linked to this network in your organization?

_____

(ii) What is the Network Operating System for this network?

_____

(iii) If this network was put out of action, this would have
( ) Minimal effect on company operation
( ) Inconvenience effect on company operation
( ) Major effect on company operation

(b) Does your organization have Access Control Procedures that can be used for controlling and limiting all unauthorised access into its IBM PCs?
( ) Yes
( ) No

If YES:

(a) Does the procedures prescribe

(i) Instructing users never to leave a terminal unattended while logged on?
( ) Yes
( ) No

(ii) Instituting such sound password standards as:
. not using common passwords that are easy to guess
. disabling vendor-supplied accounts and passwords
. changing passwords regularly
( ) Yes
( ) No

10. Are external dial-in capabilities allowed in your organization?
( ) Yes
( ) No

If YES:

(a) Does your organization use a dial-back system to allow only access from an approved list of numbers?
( ) Yes
( ) No

C. IBM PC Virus Problem Experience

11. How serious is the viruses problem in your organization's IBM PCs?
( ) No problem
( ) Only a minor problem
( ) A reasonable serious problem
( ) A major problem

12. Has your organization had any IBM PC virus infection before?
( ) Yes
( ) No

If YES:

(a) How many times has your organization had an IBM PC virus infection (including reinfection)?
_____ times

(b) For each infection,

(i) When did it occur?
_____ (DD/MM/YY)

(ii) Do you know the type of the infecting virus?
( ) Yes
( ) No

If YES:
(i) What was the type of the virus?
_____

If NO:
(i) Can you describe the symptoms of the virus?
_____

(iii) Did you know how many IBM PCs were infected in the process?
( ) Yes
( ) No

If YES:
(1) How many PCs are infected in each infection?
_____ PC(s)

(iv) How long did it take for the virus to be cleared?
_____ days/weeks

(v) Were there additional costs associated with each clean-up?
( ) Yes
( ) No

If YES:
(1) What was the approximate cost of the clean-up?
$ _____ dollars

(vi) Did you identify the person or persons (or the mechanism) responsible for introducing the virus?
( ) Yes
( ) No

If YES:
(1) Could you identify if it was perpetrated or assisted by a/an:
( ) User staff
( ) Computer staff
( ) External person (e.g., Consultant, computer service personnel)
( ) Unknown
( ) Other (Please describe)
_____

(vii) What action was taken as a result of this incident?
( ) None

( ) Formal inquiry
( ) Informal enquiry
( ) Other (Please specify)

_____

D. IBM PC Virus Control

13. Does your organization have any formal reporting and recording of IBM PC computer viruses procedures?
( ) Yes
( ) No

If YES:
(a) What are they? (Please describe briefly)

_____

14. Does your organization have formal IBM PC viruses clean-up procedures? (i.e., Does your organization assign any person responsible for the expeditious removal of contaminated software and the recovery and restoration of destroyed or lost data and programs?)
( ) Yes
( ) No

15. Does your organization have a formal Contingency (or Disaster Recovery) Plan that can be used to ensure minimal interruption to normal business operations in the event of an IBM PC virus attack?
( ) Yes
( ) No

If NO:
(a) Please explain briefly the reason:

_____

16. Does your organization prescribe storing back-up copies of original software (e.g., systems software and vendor packages) at the offsite location as soon as the package is open for use for your organization's:

(a) stand-alone IBM PCs? (This is to allow restoration of a system that has been contaminated by a time-released virus.)
( ) Yes
( ) Yes, but not at the offsite location
( ) No

(b) networking systems? (if applicable)
( ) Yes
( ) Yes, but not at the offsite location
( ) No

17. Does your organization prescribe creating back-up copies of all applications run on your organization's:

(a) stand-alone IBM PCs on a regular basis?
( ) Yes
( ) No

If YES:
(1) How often do you create the back-up copies?

_____

(b) networking systems? (if applicable)
( ) Yes
( ) No

If YES:
(1) How often do you create the back-up copies?

_____

18. Does your organization prescribe instituting, updating, and testing standard procedures for back-up and recovery for your organization's:

(a) stand-alone IBM PCs' data and/or applications?
( ) Yes
( ) No

If YES:
(1) How often do you carry out the testing of your back-up and recovery procedures?

_____

(2) When did you last test the back-up and recovery procedures?
_____ months ago

(b) networking systems' data and/or applications? (if applicable)
( ) Yes
( ) No

If YES:
(1) How often do you carry out the testing of your back-up and recovery procedures?

_____

(2) When did you last test the back-up and recovery procedures?
_____ months ago

19. Does your organization prescribe assigning personnel to specific responsibilities regarding back-up procedures for your organization's:

(a) stand-alone IBM PCs?
( ) Yes
( ) No

(b) networking systems? (if applicable)
( ) Yes
( ) No

20. Does your organization have any antiviral software that can be used (to ensure minimal interruption to normal business operations) in the event of an IBM PC virus attack?
( ) Yes
( ) No

If YES:
(a) How many separate antiviral software packages do you have?
_____

(b) For each software packages,
(i) What is the name of the antiviral software packages?
_____

21. Does your organization have a Software Acquisition Policy that can be used for controlling and inspecting all software brought into your organization's IBM PCs?
( ) Yes
( ) No

If YES:
(a) Does this policy prescribe
(i) Purchasing software only from reputable vendors?
( ) Yes
( ) No

(ii) Accepting only software received in original sealed packaging?
( ) Yes
( ) No

(iii) Reviewing, inspecting and testing new software as well as upgrades to existing software before installation?
( ) Yes
( ) No

(iv) Testing any shareware, freeware, and user-developed programs in quarantine (e.g., test/development machine or stand-alone microcomputers) prior to use in production?
( ) Yes
( ) No

Appendix 3

Sample Letter of Transmittal

School of Information Technology and Mathematics
Phone 370 6470

EDITH COWAN UNIVERSITY
PERTH WESTERN AUSTRALIA
MOUNT LAWLEY CAMPUS

2 Bradford Street, Mount Lawley
Western Australia 6050
Telephone (09) 370 6111
Facsimile (09) 328 2910

7 April 1992

Manager, Information Technology
State Government Insurance Commission
170 St. George's Tce PERTH WA 6000

Dear

An Honours student in the Department of Computer Science at Edith Cowan University, Mr. Boon LEE, is currently undertaking a research study to investigate the infection types and rates of IBM PC viruses at large in WA. There appears to be a good deal of media coverage with regard to computer viruses but very little real data on infection types and rates exists. This study is concerned specifically with determining the present status of the computer viruses problem in Western Australia and is interested in assessing the position in the Government I.T. sector. Your name and department has been suggested by the State I.T. Department as an appropriate person to contact for support in the first instance. What we are seeking is an interview of approximately 30 minutes with an appropriate person in your organization who could make comments on the computer virus infection problem to date.

Data on which the research findings will be based will be obtained from the interviews that will be carried out in participating organizations. A standardized questionnaire that comprises limited choice questions directed at obtaining such information as infection rates of various types of computer viruses will be used as a basis for the interview so that the potential for subjectivity and bias can be reduced. The participants will be assisted by the interviewer in identifying the types of infecting viruses should the need arise.

We are particularly desirous of obtaining your support to conduct this study at your organization because there is a dearth of detailed factual information about the prevalence of different viruses in Western Australia, and in Australia in general. For example, it is suggested that 4% of the world's IBM PC computer viruses are created in Australia and New Zealand but there is very little empirical research to support this claim. The present study is thus significant in that knowledge about the extent and nature of IBM PC viruses in the government sector of Western Australia can be determined. It is interesting to note that a similar study conducted during October 1991 in the USA has shown 63% of the responding sites had been exposed to at least one virus over the past year, and 9% had more than 25 PCs infected in the process.

The questionnaire has been field tested to make it possible for the research to obtain all necessary data while requiring a minimum of your time. It is anticipated that the interview will take about half an hour to complete.

It is not anticipated that the interview will cause any discomfort or have any possible hazards to the participants. It should also be noted that, in keeping with the policies of the university's Committee for the Conduct of Ethical Research, all data gathered for the research will be kept in strictest confidence at all times. Participation in the study is entirely voluntary.

A copy of a written statement that describes the study to potential participants is attached. We will phone your department to confirm your participation and the name of a contact person on April 13 or 14. Any questions concerning the study entitled An Investigation of IBM PC Computer Viruses Infection Types and Rates in a Western Australian Environment can be directed to Mr. Boon LEE (Principal Investigator) on 370 6380.

Thanking you in anticipation of your reply.

Yours sincerely

Tony Watson
Associate Professor
HEAD OF SCHOOL
INFORMATION TECHNOLOGY AND MATHEMATICS

Boon Guan Lee
Principal Investigator

Appendix 4

Letter of Approval for the Conduct of Ethical Research

EDITH COWAN
UNIVERSITY
PERTH WESTERN AUSTRALIA
MOUNT LAWLEY CAMPUS

2 Bradford Street, Mount Lawley
Western Australia 6050
Telephone (09) 370 6111
Facsimile (09) 370 2910

4 May 1992

Mr Boon G Lee
3 Pindale Gardens
BALLAJURA WA 6066

Dear Mr Lee

I am pleased to advise you that the Honours and Higher Degree Committee has determined that your research proposal is in accordance with the standards that are required for the conduct of ethical research.

You should now proceed with the empirical phase of the study. In doing so, you should be guided by the information contained in the University booklet "Information for Honours, Masters and Doctoral candidates on Research Policies and Procedures".

Yours sincerely

J CROSS
Chair
Honours and Higher Degree Committee
Faculty of Science and Technology

cc Honours file
Supervisor, J Millar (for information)

EDITH COWAN
UNIVERSITY
PERTH WESTERN AUSTRALIA
MOUNT LAWLEY CAMPUS

2 Bradford Street, Mount Lawley
Western Australia 6050
Telephone (09) 370 6111
Facsimile (09) 370 2910

4 May 1992

Mr Boon G Lee
3 Pindale Gardens
BALLAJURA WA 6066

Dear Mr Lee

I am pleased to advise you that the Honours and Higher Degree Committee has determined that your research proposal is in accordance with the standards that are required for the conduct of ethical research.

You should now proceed with the empirical phase of the study. In doing so, you should be guided by the information contained in the University booklet "Information for Honours, Masters and Doctoral candidates on Research Policies and Procedures".

Yours sincerely

J CROSS
Chair
Honours and Higher Degree Committee
Faculty of Science and Technology

cc Honours file
Supervisor, J Millar (for information)

Appendix 5

Form of Disclosure and Informed Consent

Edith Cowan University
School of Information Technology and Mathematics

Form of Disclosure and Informed Consent

This is a written statement that describes the project to potential participants so that they may choose whether or not to participate after reading it. A copy of the statement is made available to participants for their records.

---

1. The present study is conducted by the interviewer in partial fulfilment of the requirements for the award of Bachelor of Applied Science (Information Science) Honours at Edith Cowan University. The main purpose of the study is to investigate the infection types and rates of IBM PC viruses in limited Government I.T. organizations in Western Australia. The data gathering instrument for this study will be a standardized questionnaire which will comprise limited choice questions directed at obtaining such information as infection rates and types of various computer viruses. The questionnaire will be used by the interviewer as a basis for the interview so that the potential for subjectivity and bias can be reduced. The participants will be assisted by the interviewer in identifying the types of infecting viruses should the need arise.

2. It is not anticipated that the present study will cause any discomfort or have any possible hazards to the participants.

3. It is anticipated that the interview will take about half an hour to be completed.

4. The present study is significant in that knowledge about the extent and nature of IBM PC viruses in the government sector of Western Australia can be determined. The information will be provided to participants in summary form. No organization will be directly identifiable from the reports developed during the study.

5. A participant's further care will not be prejudiced in any way by his or her refusal to participate.

6. Any questions concerning the study entitled An Investigation of IBM PC Computer Viruses Infection Rates and Types in a Western Australian Environment can be directed to Mr. Boon LEE (Principal Investigator) of the Department of Computer Science on 370 6470.

I (the participant) have read the information above and any questions I have asked have been answered to my satisfaction. I agreed to participate in this activity, realising I may withdraw at any time.

I agree that the research data gathered for this study may be published provided my organization and I are not identifiable.

Participant or authorised representative Date

Investigator Date

Appendix 6

State Government IT Organizations

State Government IT Organizations

Agriculture Protection Board
Authority For Intellectually Handicapped Persons
Central Metropolitan College of TAFE
Department of Land Administration
* Department of Mines
Department of Planning and Urban Development
Department of Productivity and Labour Relations
Department of State Development
Department of State Services
* Department of Transport
Environmental Protection Authority
Fremantle Port Authority
Government Employees Superannuation Board
Health Department of WA
Homewest
Industrial Relations Commission
Legal Aid Commission
Lotteries Commission
Main Roads Department
Ministry of Consumer Affairs
* Ministry of Education
Ministry of Premier and Cabinet
Ministry of Sport and Recreation
Museum of Western Australia
Occupational Health Safety & Welfare
Office of Racing and Gaming
* Office of the Auditor General
Perth Theatre Trust
Public Service Commission
Secondary Education Authority
South Metropolitan College of TAFE
South West Development Authority
State Energy Commission (WA)
State Government Insurance Commission
State Library Services of WA
* State Taxation Department
Stateships
Transperth
Treasury Department
Valuer General's Office
WA Electoral Commission
WA Fire Brigades Board
WA Police Department

WA Regional Computing Centre
WA Tourism Commision
* Water Authority of WA
Westrail
Workers Compensation and Rehabilitation Commission

* indicates not participating organizations