SECURITY.TXT

COMPUTER SECURITY

Notes of the presentation to
The Institution of Production Engineers
March 21, 1990 by

E.A.Bedwell, E.D.P. Specialist
ORTECH International (NRC/IRAP)
2395 Speakman Dr., Mississauga L5K 1B3
(416) 822-4111, Ext. 261

The writer wishes to thank the Institution of Production Engineers and it's President for the invitation to make this presentation, and to express sincere appreciation to David Stang, Ph.D., Director of Research, National Computer Security Association, for his contribution both to this paper and to computer security in general. And I would be very remiss if I neglected to mention the professional secretarial assistance provided by Jane Templeman, who makes our whole team tick like the NRC official time clock - the one that gives the CBC time signal.

This document is, hopefully, written softly: after all, it might be easier to digest if I have to eat my words. I do not profess to be "the expert" in the field of computer security; an expert is someone who knows more and more about less and less until s/he knows absolutely everything about nothing. I hope never to stop learning, which means (thankfully) I'll never be an expert.

INDEX

		PAGE
1.	Definition/Scope of "COMPUTER SECURITY"	2
2.	Why Should You Be Concerned?	2
3.	Types of Security Breaches	3
4.	Reasons for Exposure	7
5.	General Security Rules (all computer systems)	8
6.	Viruses:	9
	6.1 History	9
	6.2 Effect	10
	6.3 Why do people do it?	10
	6.4 Symptoms	10
	6.5 Concerns	11
	6.6 Known Virus Software (1)	11
	6.7 Quick Guide to Virus Names (1)	12
	6.8 Table of Virus Effects	16
	6.9 Virus Detector/Antidote software	19
	6.10 Trojan Horses	20
7.	PC Rules of Thumb	22

8. Easy Tricks for PC Security 23
9. So You're Infected (Cure) 24
10. Summary: What Can You Do? 25
11. Security Policy: Points for Consideration 26
12. To run SCAN (included on this diskette) 29

(1) David Stang, Ph.D, "Network Security in the Federal Government,", January, 1990, p.168-169 (updated by E.A.Bedwell, March, 1990)

Tonight's topic is "Computer Security," a subject near and dear to my heart after catching fraud a few times, and cracking system security a few times. The only unfortunate part of this evening is that I have enough material to cover an intensive 2 or 3 day seminar and I only have something over an hour, so in addition to extensive notes from this presentation, I've put an article on viruses, and a PC virus detector program on diskette for you.

1. SCOPE OF COMPUTER SECURITY

Computer security relates to any potential loss of information or your ability to operate, regardless of the source of the problem. Of course, all the publicity about computer security is going to the virus situation. I don't want to dissuade anyone from their concerns about viruses, because it's definitely a growing problem, and if you get hit, you'll be sorry you ever laid eyes on a computer. But, current estimates indicate that viruses represent only 3% of all the computer problems now occurring. Of course, if you're one of the 3%, like CNIB or Barclay's Bank Canada were last fall, you'll feel like you're the only one on earth. The difference between viruses and other computer security issues is apparently one of control: I hope to convince you that you have as much control over viruses and as little control over the other 97% of problems as to make them equal threats to the safety of your computer.

I'm going to get to viruses later, their prevention, detection and cure, but I'd like first like to cover the other major problems that affect computer security - the other 97% - and I'd like to start with reasons why you should be concerned about security.

2. WHY SHOULD YOU BE CONCERNED?

Your data is a valuable asset, just like premises, equipment, raw materials and inventory. Because so much of modern business depends on computers - financial systems, engineering design, medical diagnosis, production and safety control - the destructive potential is greater every year. There has been more than one company that's suffered great losses, and even gone under because of the loss of things like their accounts receivable records: no one is going to pay you if you don't send them a bill, and if they get word of your inability to invoice them, their darned unlikely to volunteer payment - so you're in a financial mess. The same goes for your design information, production data, the consequences if safety control systems malfunction, or even the simple loss of your customer list.

Another reason why you should be concerned is, too often, people don't think about computer security until it's too late. There's a saying in my industry that, "He who laughs last probably made a backup." Another saying is, "Experience is something you don't get until just after you needed it the most." Well, if it means the life of your company, or the loss of potentially millions of dollars, or even just the information on your home computer, it might be wise to get at least some basic knowledge before the disaster strikes.

3. TYPES OF SECURITY BREACHES

Now that the 'why' is out of the way, let's break down the 97% of problems. These are not in a specific order, but just as they came to me. Nor have I attempted to attach percentages to each type of risk, because very few computer crimes are actually reported, so any figures that anyone could estimate would not be realistic:

FRAUD/THEFT

By far the biggest problem is fraud or theft. Some examples of this are:

CHAOS - 1987 - Hamburg -> NASA data bank info sold to USSR

Foreign exchange	}	famous because of big $
Electronic Funds Transfer	}	amounts, and because of the
Insider Trading	}	publicity they've received

Most common: Cookie jar technique - e.g., interest, income tax (aka 'Salami' technique - take a little and no one will notice)

Specific examples I've caught were in Payroll (no crash on < or =), Accounts Payable (dummy companies), Purchasing (failed reasonableness test), and Accounts Receivable (failed balance routine). These were all thefts of money.

Another example of theft which is very interesting is the 28-year-old Canadian who was arrested at UNISYS in Pittsburgh on Dec. 13/89 - what he is alleged to have stolen was NCR's trade secrets - to the tune of US$68M, which comes under a different Canadian law from monetary theft.

MALICIOUS DAMAGE / VANDALISM

The next major type of computer security breach is the disgruntled employee syndrome. Their favourite is the logic bomb or time bomb: on a certain date or condition after they leave the company, something's going to happen, such as at the health centre in LA where all prescriptions suddenly multiplied by 2. That's really serious, even compared to the logic bomb that superzaps all your files off the face of the earth, because someone could die. At least with a superzap, you can recover if you've been backing up and have a disaster recovery plan in effect. Pure physical vandalism occurs more often at educational institutions, but is still a serious threat. I wouldn't let me near your machine if I was angry with you - my vandalism would be difficult to detect (and expensive to repair). A simple application of a magnetized screwdriver ......

LACK OF SECURITY PLANNING IN SYSTEM DESIGN STAGE

One of the biggest logic bombs that's going to occur is on January 1/2000.

Do you know how many computer systems use a 2 digit number for the year? Do you know how much work it's going to be to adapt systems to recognize 00 as being greater than 99? My grandmother was born in 1886, and most systems show her birth year as 99. If she lives to the year 1999, I wonder if they'll start sending her the baby bonus. This time bomb is not

malicious damage, it's pure lack of planning at the system design stage.

(Lack of Security Planning - continued)

Things like balance checks and reasonableness tests are not built into the system from the beginning, and it's not easy to put them in later. Users must participate at the system design stage, because only they know what's reasonable and what can be balanced. Don't expect a computer technician to know everything there is to know about your job.

DISTORTED SENSE OF HUMOUR

Then there's the practical joker - the one who thinks it's funny to break into the system to see what he can change, or create some dumb message to appear on your screen. That's what happened at IBM when the infamous Christmas tree appeared 2 years ago (1987). The joke was three-fold - first it analyzed your electronic mail distribution lists and reproduced itself to send to everyone you normally send messages to - this clogged the system up with people reading more messages than normal. The second part was a little more technical - everyone who read the message caused a separate load of the offending program to take up space in memory, unlike most systems where two or more people who are doing the same thing are sharing one load of the software. This clogged memory up so that nothing else could run. There was one more part to this: there were delay timers built into the program so it deliberately ran very slowly. The result was that the largest computer network in the world was shut down for 4 hours. Someone must have had a great need for a power trip.

MISTAKE

Next, there's fumble fingers: you know, the one who keys the formula in as 600 grams instead of 60 grams, or the estimated production time of 2 hours instead of 2 days. Or the one who almost took me into court when he blamed "the computer" for a mistake. Without going into details about that incident, I can say that going through the grilling by several lawyers in a preliminary investigation was not the high point of my career. What saved the situation (for me and the organization) was audit trailing: every time a transaction was entered, the system recorded the

terminal i.d., the user i.d., the date and the time. It also saved a copy of the record as it existed prior to the transaction taking place. A more common mistake, though, is to unlatch a diskette door before the light goes out. Few people realize that the FAT (file attributes table) is the last thing written on a disk, and you can corrupt the FAT by removing the disk too early.

"EVERYONE DOES IT" SYNDROME

Then there's everyone's favourite: copying software. Believe it or not, in Canada, that falls under the Copyright law, not under theft, but it has been successfully prosecuted. Even if you reverse engineer it and make some minor changes, it will come under the "look and feel" test of the Copyright law - if it looks and feels the same as the original, you can be prosecuted. Copying software is illegal, and your company as the registered owner could be held liable if it is detected.

ILLEGAL ACCESS

Many major computer crimes are perpetrated by illegal access: the 14-year old who broke into NASA from his basement computer room is just one example. There is password software on all larger machines, and it's not difficult to put it on PCs. On the larger machines, one of the major problems is not changing the standard passwords that are set when the machine is delivered: the standard user-level password may be USER, the standard operator password may be OPERATOR, and the standard field repair person's password may be REPAIR, and so on. Guess how I've cracked security a couple of times. In a 1988 article by Dr. Cliff Stoll in "Computers and Security,", he reported that in 10 months of systematic testing on computers attached to the US Defense Data Network (Milnet), access was gained in 13% of the attempts simply by guessing at passwords!

There should be some rules applied to passwords: not less than 7 or 8 characters, must be changed at least every 60 days, don't use common things like names (another way I've broken security), don't share it under any circumstances and, for heaven's sake, don't post it on the front of your machine or leave it where someone can find it. It's your personal PIN - just like the money machine - and the information you're dealing with is worth money. Some of the most difficult passwords to break (take it from me) are "two words reversed" (e.g., boardwall,

hornshoe, cuptea), or foreign language words (e.g., coupdegrace, millegrazie, caliente). Nonsense is good, too: geebleurql is nice.

If you're installing password security on a PC, consider whether you should have it so tight that there is no recourse to the DOS level or no ability to boot from the A: drive. You'd need really good password software (or a good technician on staff) if you have both of these facilities - otherwise you can lock yourself out - but it's my preference (especially for the guy who's wiped his root directory twice).

PHYSICAL SECURITY

Finally, another area that affects computer security or your ability to carry on computer operations, and one that is often overlooked, is simple physical security: keys, thermal shock, vibration, dirt, water, fire, visibility of information, steady power supply, discharge of static electricity, magnetic fields, are all relevant to security. We have one man in our network who should have (a) cabling bolted to his computer and the floor, (b) a key to his unit, and (c) dust protectors (as well as password access only without recourse to the DOS level).

When it comes to thermal shock, if you work in an area where the heat is reduced on winter weekends, I strongly recommend you leave your unit running over the weekend - just lock the keyboard. If the air conditioning is shut down, turn your unit off, and don't turn it on until the temperature is 23C or less. And please don't leave your machine sitting in the sun, or in front of an open window to attract dust. The internal temperature raises within 20 mins. or so to >30C, and the effects of thermal shock are such that it can, first, rock memory chips out of their sockets, and, worse, misalign the read heads on your disk drive so that nothing can be read.

(Physical Security - continued)

Vibration, too, is a source of problems, especially for drives. The read heads actually float over the surface of drives, not on them the way a

record player needle does, and the space tolerance between is measured in Angstroms (metric version of microinches). Vibration can cause the head to hit the drive, and you can say goodbye to whatever was written there.

If you're in a particularly sensitive field, and your information is what might be called top secret to your company, you might also want to look at two protection devices: one is encryption, and the other is Tempest hardware or shielding. Encryption involves translating your data using algorithms to something unreadable, and de-coding it when you need it. It uses a "key" to choose the algorithm - dont' lose the key! It comes in a few forms: software controlled encryption, hardware based encryption, or a combination of the two. Most encryptors work with standard algorithms, but defense departments and other high-security installations prefer random algorithms. Tempest hardware, or shielding, protects against sniffing of signals. (Signal emanation surveillance is called "sniffing.") I don't have a computer here to demonstrate this, but if you take an old battery-operated transistor radio and set the dial to the bottom of the AM band around 520, try passing it within a foot of your computer. Your ear might not pick up the individual signals, but I assure you there's equipment that does. That's why the US Army was blasting rock music around the Vatican Embassy when Noriega was there - to mask signals.

More important to the average user, though, is avoidance of electro-magnetic fields (such as ringing phones near a disk or disk drive), and having an automatic disk head 'parker' that moves the heads to a safe zone every few seconds. That way, something like a brief power failure is less likely to cause a "head crash" on the disk.

Simple visibility of information is a risk. Recently I went to a bank with a court order in hand to give me access to an account. The clerk simply turned the terminal toward me and, if I'd wanted to bother, I could have had the account numbers of two other people with identical names. There is screen saving software that will blank your screen after an inactivity duration you choose, and personnel should be made conscious that unauthorized viewing of information is a security risk. And watch what your staff throw out on paper, too.

When it comes to fire and water, there are two basic rules that everyone can follow: first, don't smoke around the PC, and second, don't feed the PC coffee and donuts. You might be able to save a keyboard or some parts with a bath in distilled water, possibly followed by drying with a warm hair dryer, but there's no guarantee. I prefer pure isopropyl alcohol - without the hairdryer so I don't get fried in the process. Don't blast a computer with a fire extinguisher if you can avoid it. If you do have a fire or a flood, though, you'd better have a tested disaster recovery plan, and your backups stored off-site.

All of these issues are reasonably within your control: fraud, theft, disgruntled employees, practical jokers, fumble fingers, software copying and physical security, at least as much as the infamous viruses that are around, but let's take a look at why you're at risk.

4. REASONS FOR EXPOSURE

Concentration of data in one place

Instantaneous adjustment

Alteration without a trace

Lack of visible records

Complexity of the system

Networking

Technical persons can befuddle

General ignorance by non-techie and management

Detection problems

Lack of training

Security checks in programs not specified

Systems not documented

Limited staff resource for programming/management

No separation of duties

Possibility of enormous losses remaining undetected

Reluctance to report - Embarrassment

Lack of sufficient evidence to prosecute
Cost to prosecute outweighs recovery
Company policy ("Press would have a field day")

5. GENERAL SECURITY RULES (All Systems, big and small)

Disaster Recovery } Backup Backup Backup
Plan } Restore (test it to make sure it works)

Store your backup off-site (not in your car!)

Physical security

Password for access control (don't stick your password on
the front of your machine!)

Access to menu only - not to system control level

Reasonableness tests

Balance checks (rounding: up, down, (out?); cross-calculations

Audit trails - all records (terminal i.d., user i.d., date and
time stamping, history record retention)

Fall-through coding (if it doesn't meet a condition, does it go to limbo)

Payroll/Accounts payable: don't pay the same # twice

Fault tolerance level supported (user friendly/hostile -
balance between fault tolerance & productivity)

Call back or no answer on dial-up systems

UPS (Uninterrupted Power Supply, or allowance for graceful
degradation) - or at least an automatic head parker

Logical view rights (your user 'privileges' allows access only to the
data you need to see, e.g., accounting clerks don't need to see
production formulae)

Multi-user environment: protection against deadly embrace

Automatic logoff on inactivity timer / Screen saver

Policy statement re purchasing/use/theft/illegal
software, etc.

Encryption (?) - don't lose the key!

Shielding ("Tempest" hardware for secure systems)

Educate users

6. VIRUSES

As in medicine, a virus needs an 'organism' to which it may attach itself, and a virus is 'contagious'.

In the case of computers, a virus is usually a destructive piece of code which attaches to a working program, such as your word processor, spreadsheet or CAD/CAM software. Viruses are usually written to detect any load of a computer file that has an extension of .EXE, .COM, .OVL, .BIN - such extensions representing executable programs. Often, the virus loads itself into memory, then loads the program you just called, so the virus is sitting at the front. Then when you exit the program, the virus code calls for the re-writing of the program back onto the disk - with the virus still sitting at the front. Other viruses simply go straight into your boot sector, so they get loaded every time you turn on your machine. Some do both.

However they 'hide', and whatever they attach to, they got to your machine on an infected diskette. If you are infected and then copy your software to use on another machine, guess what happens? Right! That's where the 'contagious' element comes in.

In 1989, more viruses were discovered than in all previous years. There were over 110 at the end of the year, and 7 were discovered in December alone. Sources have been from as far away as Pakistan and Bulgaria.

Only .004% have reported infections, but most are not reported. Consider this: if only 1% were infected, that would be 1/2 million units in the U.S. alone. At a cost ranging from $300 to $3,000 per unit to recover, the problem starts to impact the economy as well as the productivity of staff at your organization. It cost one Texas company US$10M to shut down their 3,000-unit network for 4 days to find 35 infected units.

One of the major problems with viruses is that 90% of the users who recover are re-infected within 30 days. One person at my organization was re-infected 7 times in 2 months! Most reinfections occur for one of two reasons (not necessarily in this order): your back-up was infected, or it was a virus that hid in the boot sector on track 0, and track 0 is not re-written by the standard "FORMAT" command (only a low-level format will get rid of a track 0 virus). Be careful of some new software as well: there has been more than one instance of shrink-wrapped software being infected (software companies have disgruntled employees, too, it seems).

6.1 HISTORY

1959 - Scientific American article about 'worms'
1963 - caught my first two frauds (Payroll & Accounts Payable)
1970 - Palo Alto lab - worm which directed activities
1982 - Anonymous Apple II worm
1984 - Scientific American CoreWare Series: held contest to find the most clever/difficult to detect 'bug'
1987 - Apparent change from intellectual exercise to dangerous activity.

6.2 EFFECT

Massive destruction:	Reformatting
	Programs erased
	Data file(s) modified/erased
Partial/Selective destruction:	Modification of data/disk space
	File allocation tables altered
	Bad sectors created
	If match with event, alter or delete
Random havoc:	Altering keystroke values
	Directories wiped out
	Disk assignments modified
	Data written to wrong disk
Annoyance:	Message
	Execution of RAM resident programs suppressed
	System suspension

6.3 WHY DO PEOPLE DO IT?

Financial gain
Publicity
Intellectual exercise
Terrorism/Fanaticism/Vandalism
Revenge
Just plain wierd

6.4 SYMPTOMS

Change in file size (Usually on .COM, .EXE
.OVL, .BIN, .SYS or .BAT files)
Change in update time or date
Common update time or date
Decrease in available disk or memory space
Unexpected disk access
Printing and access problems
Unexpected system crashes

6.5 CONCERNS

Variety: Virus vs Bug vs Worm vs Trojan Horse vs Superzapper
vs Trap Doors vs Piggybacking vs Impersonation
vs Wiretapping vs Emulation
Strains / Complexity / Growing Sophistication
Bulletin board use and free software
Largest threats from taking computer work home

Kids using same machine at home
Networked mainframe systems
Travel/airline computers (AA wiped out early 1989)
Work message systems (E-Mail)
POS terminals
Banking / Credit Cards / Money Machines
Income Tax records
Health records

```
**************************************************************
*    Global disaster may be on the way                       *
*    No specific laws to deal with malicious programming     *
*    No single national centre to gather data on infections  *
**************************************************************
```

6.6 KNOWN VIRUS SOFTWARE

12 viruses (and their strains) account for 90% of all PC infections:

- [ ] Pakistani Brain
- [ ] Jerusalem
- [ ] Alameda
- [ ] Cascade (1701/1704)
- [ ] Ping Pong
- [ ] Stoned
- [ ] Lehigh
- [ ] Den Zuk
- [ ] Datacrime (1280/1168)
- [ ] Fu Manchu
- [ ] Vienna (DOS 62)
- [ ] April First

6.7 QUICK GUIDE TO VIRUS NAMES (Cross referenced)

Name	Synonym-1	Synonym-2	Synonym-3	Synonym-4
1168	Datacrime-B			
1184	Datacrime II			
1280	Datacrime	Columbus Day	October 12th	Friday 13th
1536	Zero Bug			
1701/1704	Cascade	Falling Letters	Falling Tears	Autumn Leaves
1704	Cascade			
1704	Cascade-B			
1704	Cascade-C			
1704	Cascade-D			
1704 Format	1704	Blackjack	Falling Letters	
1704	Blackjack	1704 Format	Falling Letters	
1808	Jerusalem	Black Box/Hole	Israeli PLO	1808/1813
1813	Jerusalem	Black Box/Hole	Israeli PLO	1808/1813
2086	Fu Manchu			
2930				
3066	Traceback			
3551	Syslock			
3555				
123nhalf				
405				
500 Virus	Golden Gate			
512 Virus	Friday 13th	COM virus		
648	Vienna	DOS 62	DOS 68	Austrian
AIDS	VGA2CGA	Taunt		
AIDS Info Disk				
Alabama				
Alameda Virus	Yale	Merritt	Peking	Seoul
Alameda-B	Sacramento	Yale C		
Alameda-C				
Amstrad				
Anti				
Apple II GS	LodeRunner			
April 1st	SURIV01	SURIV02		
April 1st-B				
Ashar				

Austrian	648	Vienna	DOS 62	DOS 68
Australian	Stoned	New Zealand	Marijuana	
Autumn Leaves	Cascade	1701/1704	Falling Letters	Falling Tears
Basit virus	Brain	Pakistani Brain	Lehore	
Black Box	Jerusalem	Israeli	Black Hole	1808/1803 PLO
Black Hole	Jerusalem	Black Box	Israeli	1808/1813 PLO
Black Hole	Russian			
Blackjack	1704	1704 Format	Falling Letters	
Bouncing Ball	Vera Cruz	Ping Pong	Bouncing Dot	Italian virus
Bouncing Dot	Italian virus	Bouncing Ball	Vera Cruz	Ping Pong
Brain-B	Brain-HD	Harddisk Brain	Houston virus	
Brain-C				
Brain-HD	Harddisk Brain	Houston virus	Brain-B	

Brain	Pakistani Brain	Basit virus	Lehore	
Cascade	1701/1704	Falling Letters	Falling Tears	Autumn Leaves
Cascade(-B-C-D)	1704			
Century	Oregon	Jan.1, 2000		
Century-B				
Chroma				
Clone				
Clone-B				
Columbus Day	1280/Datacrime	October 12th	Friday 13th	
COM virus	512 virus	Friday 13th		
COM-B	Friday 13th-B			
COM-C	Friday 13th-C			
Cookie virus	Sesame Street			
Dark Avenger				
Datacrime	1280			
Datacrime-B	1168			
Datacrime-II	1184			
dBASE virus				
Den Zuk	Search	Venezuelan		
Disk Killer	Ogre			
Do-Nothing (don't believe it!)				

DOS-62 Vienna DOS-68 648 Austrian
DOS-68 Vienna DOS-62 648 Austrian
DOS-62 UNESCO
DOS-62-B
Falling Tears Cascade 1701/1704 Falling Letters Autumn Leaves
Falling Letters 1704 Blackjack 1704 Format
Falling Letters Cascade 1701/1704 Falling Tears Autumn Leaves
Falling Letters-Boot Ping Pong B
Fat 12 Swap Israeli Boot
FluShot4 (a corrupted version of a virus detector - use FluShot4+)
Friday 13th 1280/Datacrime Columbus Day October 12th COM
Friday 13th-B COM-B 512
Friday 13th-C COM-C
Fumble Type
Fu Manchu 2086
Ghost-Boot
Ghost-COM
Golden Gate 500 Virus
Golden Gate -B
Golden Gate-C Mazatlan
Golden Gate-D
Harddisk Brain Brain-B Brain-HD Houston virus
Holland Girl Sylvia
Houston virus Brain-B Brain-HD Harddisk Brain
Icelandic Disk-Crunching-virus Saratoga 2
Icelandic 1 Saratoga 1
Icelandic 2 System virus
INIT29
IRQ v. 41
Israeli Friday13 Jerusalem Black Box/Hole 1808/1813 PLO
Israeli Boot Swap Fat 12

Italian virus Bouncing Ball Vera Cruz Ping Pong Bouncing Dot
Jan.1, 2000 Century Oregon
Jerusalem Israeli Black Box/Hole 1808/1813 PLO Friday 13th

Jerusalem-B New Jerusalem
Jerusalem-C
Jerusalem-D
Jerusalem-E
Jork
Key
Lehigh
Lehigh-2
Lehore Brain Pakistani Brain Basit
Lisbon
LodeRunner Apple II GS
MacMag Peace virus
Madonna (while the nice music plays, your hard disk is being destroyed)
Mailson
Marijuana New Zealand Stoned
Mazatlan Golden Gate-C
Merritt Alameda virus Yale Peking Seoul
Mix1
Music virus Oropax virus
New Jerusalem Jerusalem-C
New Zealand Stoned Marijuana Australian
New Zealand-B Stoned-B
New Zealand-C Stoned-C
nVIR
October 12th 1280/Datacrime Columbus Day Friday 13th
Ohio
Ogre Disk Killer
Oregon Century
Oropax virus Music virus
Pakistani Brain Lehore Basit Brain
Palette Zero Bug
Payday
Peace Virus MacMag
Pearson
Peking Alameda virus Yale Merritt Seoul
Pentagon
Ping Pong Bouncing Dot Italian virus Bouncing Ball Vera Cruz
Ping Pong-B Falling Letters-Boot
PLO Jerusalem Friday 13th 1808/1813 Israeli
Russian Black Hole
Sacramento Alameda-B Yale C
Saratoga 1 Icelandic 1
Saratoga 2 Icelandic Disk-Crunching-virus
Scores
Search Den Zuk Venezuelan
Seoul Alameda virus Yale Merritt Peking
Sesame Street Cookie virus
SF virus

Shoe virus UIUC virus (see also Terse Shoe)

Shoe virus-B
Stoned New Zealand Marijuana Australian
Stoned-B New Zealand-B
Stoned-C New Zealand-C
SUMDOS
Sunday
SRI (destroys anti-viral programs before it damages your system)
SURIV01 April 1st
SURIV02 April 1st
SURIV03
Swap Israeli Boot Fat 12
Sylvia Holland Girl
SYS
Syslock 3551
System virus Icelandic 2
Taunt AIDS VGA2CGA
Terse Shoe (see also Shoe virus)
TP04VIR Vacsina
TP25VIR Yankee Doodle
TP33VIR Yankee Doodle
TP34VIR Yankee Doodle
TP38VIR Yankee Doodle
TP42VIR Yankee Doodle
TP44VIR Yankee Doodle
TP46VIR Yankee Doodle
Traceback 3066
Typo (boot)
Typo (COM) Fumble
UIUC virus Shoe virus
UNESCO DOS-62
Venezuelan Den Zuk Search
Vera Cruz Ping Pong Bouncing Dot Italian Virus Bouncing Ball
Vacsina TP04VIR

VGA2CGA	AIDS	Taunt		
Vienna	DOS-62	DOS-68	648	Austrian
Vienna-B				
Yale	Alameda virus	Merritt	Peking	Seoul
Yale C	Alameda-B	Sacramento		
Yankee Doodle	TP25VIR			
Yankee Doodle	TP33VIR			
Yankee Doodle	TP34VIR			
Yankee Doodle	TP38VIR			
Yankee Doodle	TP42VIR			
Yankee Doodle	TP44VIR			
Yankee Doodle	TP46VIR			
Zero Bug	1536			

6.8 TABLE OF VIRUS EFFECTS (by virus name)

This information is a reformatted version of that which was made available to the writer by the National Computer Security Association, Suite 309, 4401-A Connecticut Ave. NW, Washington, D.C., 20008.

This list is not as complete as the list of names preceding. Since viruses must be created and caught before they can be analyzed for the type of information that follows, this list will never be as complete as the list of names. In some instances, you may have been infected with a variation of the name. You might wish to check this list for all possible variations of a name you've found on the list of synonyms.

Explanation of codes used under "What it does", and analysis of frequency of occurrence of each effect:

	EFFECT	#	OCCURRENCES	%
1.	Virus uses self-encryption	13		12
2.	Virus remains resident	83		74
3.	Infects COMMAND.COM	8		7
4.	Infects .COM files	62		55
5.	Infects .EXE files	41		37
6.	Infects .OVL files	15		13
7.	Infects floppy disk boot sector	36		32
8.	Infects hard disk boot sector	14		13
9.	Infects partition table	1		1
10.	Corrupts or overwrites boot sector	31		28
11.	Affects system run-time operation	53		47
12.	Corrupts program or overlay files	57		51
13.	Corrupts data files	4		4
14.	Formats or erases all/part of the disk	17		15
15.	Corrupts file linkage (FAT)	9		8
16.	Overwrites program	4		4
17.	Mac virus (as opposed to PC virus)	2		2

VIRUS NAME	Increase in Prog'm size	Disinfector that works	What it does
1168/Datacrime B	1168	SCAN/D	1, 4, 12, 14
1184/Datacrime 2	1184		1, 4, 5, 12, 14
123nhalf	3907		2, 5, 11, 13
1280/Datacrime	1280	SCAN/D	1, 4, 12, 14
1514/Datacrime II	1514	SCAN/D	1, 4, 5, 12, 14
1536/Zero Bug	1536	SCAN/D	2, 4, 11, 12
1701/Cascade	1701	M-1704	1, 2, 4, 11, 12
1704/Format	1704	M-1704	1, 2, 4, 11, 12, 14
1704/Cascade	1704	M-1704	1, 2, 4, 11, 12
1704/Cascade-B	1704	M-1704	1, 2, 4, 11, 12
1704/Cascade-C	1704		1, 2, 4, 11, 12
1704/Cascade-D	1704		1, 2, 4, 11, 12
2930	2930	SCAN/D	2, 4, 5, 12

3066/Traceback	3066	M-3066	2, 4, 5, 12
3551/Syslock	3551	SCAN/D	1, 4, 5, 12, 13
3555	3555		1, 3, 4
405		SCAN/D	4, 16
AIDS		SCAN/D	4, 16
AIDS Info Disk	0	AIDSOUT	11
Alabama	1560	SCAN/D	2, 5, 11, 12, 15
Alameda-B			2, 7, 10
Alameda-C			2, 7, 10
Alameda/Yale		MDISK	2, 7, 10
Amstrad	847	SCAN/D	4, 12
April 1st			2, 4, 11
April 1st-B			2, 5, 11
Ashar		MDISK	2, 7, 10
Black Hole	1808		2, 4, 5, 6, 11, 12, 15
Brain-B			2, 7, 8, 10
Brain-C			2, 7, 8, 10
Century			2, 4, 5, 6, 11, 12, 14, 15
Century-B			2, 4, 5, 6, 11, 12, 14, 15
Clone-B			2, 7, 10, 15
Clone virus			2, 7, 8, 10
dBASE	1864	SCAN/D	2, 4, 11, 12, 13
DOS-62-B			3, 4, 11
DOS-62-UNESCO	650		3, 4, 11
Dark Avenger	1800	M-DAV	2, 3, 4, 5, 6, 11, 12, 15
Datacrime II-B	1917	SCAN/D	1, 3, 4, 5, 12, 14
Disk Killer		MDISK	2, 7, 8, 10, 11, 12, 13, 14
Do-Nothing	608	SCAN/D	4, 12
Fri 13th COM	512	SCAN/D	4, 12
Fri 13th COM-B	512		4, 12
Fri 13th COM-C	512		4, 12
Fu Manchu	2086	SCAN/D	2, 4, 5, 6, 11, 12
Ghost-Boot ver.		MDISK	2, 7, 8, 10, 11
Ghost-COM ver.	2351	SCAN/D	4, 10, 12
Golden Gate			2, 7, 10, 14
Golden Gate-B			2, 7, 10, 14
Golden Gate-C			2, 7, 10, 14
Golden Gate-D			2, 7, 10, 14
IRQ v. 41			4, 5, 11
Icelandic I	642	SCAN/D	2, 5, 11, 12
Icelandic II	661	SCAN/D	2, 5, 11, 12
Italian/Ping Pong		MDISK	2, 7, 10, 11
Italian-B		MDISK	2, 7, 8, 10, 11
Jerusalem	1808	SCAN/D/A	2, 4, 5, 6, 11, 12
Jerusalem-B	1808	M-JERUSLM	2, 4, 5, 6, 11, 12

Jerusalem-C	1808		2, 4, 5, 6, 11, 12
Jerusalem-D	1808		2, 4, 5, 6, 11, 12
Jerusalem-E	1808		2, 4, 5, 6, 11, 12, 15
Jork			2, 7, 10
Lehigh		SCAN/D	2, 3, 12, 14, 16
Lehigh-2			2, 3, 12, 14, 15, 16
Lisbon	648	SCAN/D	4, 12

MIX1	1618	SCAN/D	2, 5, 11, 12
New Jerusalem	1808	M-JERUSLM	2, 4, 5, 6, 11, 12
New Zealand		MD	7
New Zealand-B			7, 8
New Zealand-C			7, 8
nVIR			11, 17
Ohio		MDISK	2, 7, 10
Oropax			2, 4
Pakistani Brain		MDISK	2, 7, 10
Palette/Zero Bug	1536		2, 3, 4,
Payday	1808	M-JERUSLM	2, 4, 5, 6, 12
Pentagon		MDISK	7, 10
SF Virus			2, 7, 11, 14
SRI	1808		2, 4, 5, 6, 11, 12
SURIV01	897	SCAN/D	2, 4, 11, 12
SURIV02	1488	SCAN/D	2, 5, 11, 12
SURIV03		SCAN/D	2, 4, 5, 6, 11, 12
SYS			2, 7, 8, 11, 12
SYS-B			2, 7, 8, 11, 12
SYS-C			2, 7, 8, 11, 12
Saratoga	632	SCAN/D	2, 5, 11, 12
Saratoga-2			2, 5, 11, 12
Scores			11, 17
Search HD			2, 7, 8, 10, 11
Search-B			2, 7, 10, 11
Search/Den Zuk		MDISK	2, 7, 10, 11
Shoe virus			2, 7, 8, 10

Shoe virus-B			2, 7, 10
Stoned/Marijuana		MDISK/P	2, 7, 9, 10, 11, 15
SumDOS	1500		4, 5, 14
Sunday	1636	SCAN/D	2, 4, 5, 6, 11, 12
Swap/Israeli Boot		MDISK	2, 7, 10
Sylvia/Holland	1332	SCAN/D	2, 4, 12
Terse Shoe virus			2, 7, 10
Typo (Boot)		MDISK	2, 7, 8, 10, 11
Typo/Fumble (COM)	867	SCAN/D	2, 4, 11, 12
Vacsina/TP04VIR			2, 4, 5
Vienna-B	648	SCAN/D	2, 4, 5, 12
Vienna/648	648	M-VIENNA	4, 12
Yankee Doodle	2855	SCAN/D	2, 4, 5, 11, 12
Yankee Doodle/TP25VIR			2, 4, 5
Yankee Doodle/TP33VIR			2, 4, 5
Yankee Doodle/TP34VIR			2, 4, 5
Yankee Doodle/TP38VIR			2, 4, 5
Yankee Doodle/TP42VIR			2, 4, 5
Yankee Doodle/TP44VIR			2, 4, 5
Yankee Doodle/TP46VIR			2, 4, 5

6.9 VIRUS DETECTOR AND ANTIDOTE SOFTWARE

*** None offer complete protection ***

Some do NOT test for boot sector viruses, modification of the command interpreter, branching into the BIOS, etc., unconventional things that nasty viruses are known to do. This is not a comprehensive list, but you'll have an idea of what's available, either commercially or through public domain. Look for a product that will detect as many of the

effects identified in the previous section as possible. Warning: some highly publicized virus detectors only search for ONE (1) virus! Others are more sophisticated, and may even act as a disinfector as well as a detector.

Old virus symptoms vs file changes
Antidote
Antigen

Bombsqad
Canary
Cylene-4
C-4
Disk Defender * recommended (add-on board - write-protects hard disk)
Disk watcher
Dr. Panda Utilities
IBM - COMPare in DOS
Mace vaccine
Magic Bullets
Syringe
Sentry * recommended for systems booted regularly
Vaccine
Viraid
Virus-Pro * recommended for large corporate environments
Shareware: Novirus
Flushot4+
Virusck
Viruscan

Plus what's shown on preceding pages as a "Disinfector that works". I also have a list of over 100 shareware products that do everything from detect and/or disinfect to write-protecting the hard drive and requiring password access .... but my fingers are getting tired from typing at this point, and there are more important things to cover - after all, if you're careful, you won't need a list of detectors/disinfectors.

6.10 TROJAN HORSES

While a "virus" is something hidden within another program that is waiting to make your system really sick, and a "worm" may be something that lives on its own and usually transmits through networked computers, a "Trojan Horse" is a little of both, so I've included it with this virus section if only to warn you of its existence. It lives on its own as a program, and will bring you down like Helen of Troy's soldiers. "I wouldn't copy something like that," you say. Well, like Helen's horse, it comes disguised. It will purport to do something really neat, like compress files (so you have more disk space available), sort your directories (so you can find things more easily), or play chess or another game with you. In actuality, it's really just waiting to do the things that viruses do - trash your files, scramble your boot sector, fry your FAT, or erase your hard disk. It doesn't usually do anything it promises to do.

The following are just a few examples of the known Trojan Horses, most of which come from bulletin boards. Please don't misunderstand me, most BB operators are honest people who are trying to help the computer industry as a whole, but they can't be held responsible for the people who might dial into their BB and leave a disaster waiting until the next caller(s).

SCRNSAVE.COM: This is supposed to blank your screen after x seconds of inactivity, thus preventing image burn-in or apparently offering a sense of security; say goodbye to your files while it erases your harddisk.

TSRMAP: For the 'sophisticated' user who uses Terminate and Stay Resident programs, it's sometimes handy to have a map of where these programs are loaded in memory, and be able to delete some if you're short of memory; hopefully this same 'sophisticated' user has a copy of track 0, because his was just sent to heaven ..... or elsewhere.

DOS-HELP: Sounds great, doesn't it? This TSR program is supposed to give on-line help on DOS commands. Your hard disk was

just formatted.

ULTIMATE.EXE: This is supposed to be a DOS shell (if you've used Directory Scanner or some other software that allows you to move around directories and load programs easily, or even a menu system, then you know what a DOS shell is). While the "Loading..." message shows on your screen, the FAT (file allocation table) of your hard disk went to the trash bin.

BARDTALE.ZIP This purports to be a commercial game from Electronic Arts (BARDTALE I) Someone reverse engineered this program, and wrote in a routine to format your hard disk upon invocation.

COMPRESS.ARC This is dated April 1 1987, is executed from a file named RUN-ME.BAT, and is advertised as "shareware from Borland" (Borland is a highly reputable company). It will not compress your files, but it will very competently destroy your FAT table.

DANCERS.BAS You'll actually see some animated dancers in colour - while your FAT is being tromped on.

DEFENDER.ARC Think you're going to get a copy of Atari's DEFENDER for nothing, huh? There's still no such thing as a free lunch, and this one will be particularly expensive: it not only formats your hard disk, but it writes itself to your ROM BIOS - the chip that holds the Basic Input Output System for your machine. Get your wallet out.

SIDEWAYS.COM The good "SIDEWAYS.EXE" is about 30Kb, while this version is about 3Kb. The really big difference, though, is what happens to your hard drive - it's spun off into oblivion.

These are only a few of the 70 or so Trojans I have listed at work, but I'm sure you've got the idea. These programs (a) stand alone, (b) often claim to do something useful, (c) may be hacked versions of good software, (d) may be named the same as good software, (e) may send you back to using a quill pen.

7. PC RULES OF THUMB (Additional to Basic Rules of Thumb)

Run virus check BEFORE backup

Boot floppy systems from known, protected disks only

Never work with masters - first make copies on a trusted machine

Store data on floppy:
     set path in autoexec.bat, but load from A: to
     ensure data goes to floppy

Save your data periodically while working

Use write protect tabs

Use write protect software on hard disk / backup track 0

Never boot HD systems from floppies (unless known and
     protected)

New/repaired hard disk? - run a virus detector

Use protection package (practice safe hex)

Avoid shareware / BB demos
     if you use a BB, set path to A: beforehand,
     download only to A:, poweroff immediately after,
     then powerup and do a virus scan on the floppy;
     always scan shareware

Know the source of your software

Don't use illegal copies

If your data is truly confidential, don't depend on
     DELETE - you must use, e.g., Wipefile

Autopark software

Hardcards

6. A FEW EASY TRICKS FOR PC SECURITY

1. Set Read only attributes on all files ending with .COM, .EXE, .SYS, . OVL, .BIN, .BAT

   e.g.: ATTRIB +R *.SYS

2. Use an undocumented trick in DOS of naming your data files ending with an ASCII blank or NUL character (ASCII 32 or 255): ***

   e.g.: COPY A:OLDFILE.TXT NEWFILECHR$(255).TXT
   or REN A:MYFILE.DAT MYFILECHR$(32).DAT

   *** Newer versions of DOS will give the ASCII blank or null by holding the [Alt] key and striking the numeric keypad numbers; e.g. COPY A:OLDFILE.TXT NEWFILE[Alt]255

3. Prevent inadvertent formatting of the hard disk:

   Rename FORMAT.EXE to (e.g.) DANGER.EXE
   Write a 1-line batch file called FORMAT.BAT:
   DANGER A: %1 %2 %3 %4 %5 %6

4. Have a batch program as a shutdown routine, to run:

   1. Virus Check
   2. Copy Track 0

3. Back up your data files
4. Park the heads

9. SO YOU'RE INFECTED

Terminate all connections with other computers

Record your last activities

Determine the nature and extent of the damage

Notify other users

Contact the source of the carrier software

_ _

Back up data files to new diskettes

Erase infected disk (using high or low level format -
low level is preferred to re-write track 0)

Check master disks with detection program(s)

Restore system files

Restore data files

Run detection program(s) again

Be careful in future - think like a thief!
---

10. SUMMARY: WHAT CAN YOU DO?

There are many aspects to computer security, none of which are totally within your control, but all of which are reasonably within your control. One of the major methods of getting control is to establish an enforceable security policy AND a disaster recovery plan. However, it's almost impossible to establish a plan unless you first know what the risks are.

WHEN YOU GO BACK TO YOUR OFFICE

Try putting some staff into two teams: "hackers" and "police" (or call them Blue Jays and Cardinals if you find that offensive). The role of the hackers is to try to dream up all the things they could get from or do to the company (or to a department) by breaking computer security. The role of the police is to respond with defenses. Then switch roles. List all the ideas, no matter how "far out" they seem, then use this for the basis of risk analysis and disaster recovery planning. The only rule to this game is that no idea is initially rejected.

Now that you have some idea of the value of your data and the risks it is under, you can begin to work on a "Computer Security Policy" and a "Disaster Recovery Plan." While many suggestions have been made on the previous pages, recognize that not all risks/solutions apply to all organizations: you have to make some judgement calls based on your assessment of the risk. The judgement is based on how much loss you can comfortably sustain, yet remain in business. The level of security protection you require may not always be the same. It may vary with the value of the hardware, software or data under consideration; the security level, therefore, might be stated as "minimal," "discretionary," "mandatory," or "verified." The point is, as long as it's been considered, you're closer to having a good security system than if you have no policy or a policy that's based on guesswork.

You may find, after working on this for a while, that you may wish to develop a separate policy for the selection or development, change, testing and implementation of software. This might be stated as simply as, "No system shall be acquired, developed, changed or implemented without the prior approval of the Systems Steering Group." This might also go on to cover documentation; e.g., "Documentation must be complete for all systems prior to implementation, and must include sections on files used, access controls, security considerations and controls (etc.)."

Some further points for consideration are included in the next section.

11. COMPUTER SECURITY POLICY: POINTS FOR CONSIDERATION

Any policy on computer security must be based on the premise that information is a valuable asset of the company, just like its premises, equipment, raw materials, inventory and so on. More than one company has gone under because they lost their accounts receivable data in a fire, flood, or from a simple hard disk failure. The value of your data should be subjected to a risk analysis, and all identifiable risks assessed. It is not until you identify the risks that you can plan for a disaster recovery.

Your policy might include some of the many things addressed previously in this paper: e.g., storing data only on removable media (diskettes or tapes), limiting access to bulletin boards, establishing password controls, rules on physical security, use of immunization software, etc. There are, however, some other specific points not previously discussed:

RESPONSIBILITY

Recognize that security is a management issue, not a technological issue, and that setting policy is the responsibility of senior management. They must be 'on board' and understand why a security policy is needed to make it sensible and effective, and they must give overt support.

Someone should be in charge of computer and network security. Without someone in charge, important security tasks may not get done. The duties of the security manager would include responsibility for limiting access

to the network, securing the information that passes over it, overseeing password systems, and installing security packages that protect computers from illegal tampering once a user is on the network. Other duties might include analyzing the network for security weaknesses and helping users understand the security strengths and weaknesses of the network.

The amount of time required of the system security specialist may depend on the size of the organization, and on the number and complexity of the systems in use or planned.

Having one person in charge is probably the ideal security arrangement. The security specialist can become aware of all of the issues affecting computer/network security, can schedule and establish priority for actions, and can ensure that the actions are taken.

This position in the organization requires some authority and autonomy. For instance, security is compromised if the boss shares his/her password. The security specialist needs to be able to change the boss's password if this happens, and gently but firmly discuss the problems which could result.

In many organizations, putting two or more people in charge of something diffuses responsibility. Each can think that some security concern was the responsibility of the other. If two individuals are charged with network security, be certain that they work well together, communicate

well, and will each put in their fair share of the analysis and work that is required for security.

In some organizations, a "communications manager" is responsible for limiting access to the network (with dialback modems and encryption devices), while the network manager maintains password systems and installs security software.

If someone is in charge of network security and you don't know about it,

then they haven't been very obvious about it. They need not be. But if it is evident to you that security is lacking, then perhaps the issue of responsibility should be examined (or re-examined).

BACKUPS

Those who are most zealous about backups are those who've been affected in the past by a loss of data. If backups are performed every day, your computer or network is probably in good shape when the hard disk or file server goes to heaven. You will want to verify that this is the case, since most organizations (and individuals) put this off... and off... until it's too late.

Backing a system up once a week is not enough, unless the system is rarely used. If your last backup was a week ago, and your hard disk or the hard disk in the file server crashes, all users of the network have lost one week's work.

This cost is enormous. If you have 10 users who have lost 30 hours of work each, if each user is paid $20/hour, and overhead is 100%, then you have just lost 10 x 30 x 20 x 2 = $12,000. If you assume that backup takes one $20 hour with a tape drive, you could back the system up 600 times for $12,000. That's nearly three years, if backups are done five times a week. Many hard disks will not run continuously for three years. Even if you're a 'stand alone' computer user, your time is valuable. You might consider a policy that, if recovery covers a period of more than 'x' days, it must be done on the employee's own time, and all deadlines must be met - tough, but it get's the point across!

Irregular backups are a sign that backup is not taken as seriously as it should be. It is probably wisest to do the arithmetic, comparing the costs of backup with the costs of losing work for multiple users. The cost comparison in the commentary on the second answer doesn't even consider the possibility of losing irreplaceable files, such as those containing new accounts receivable entries or new prospects.

Since file backup is a "private" activity, not knowing how often it occurs does not mean that it does not occur. But if you have a security concern, you should find out what the correct answer is. After all, if you use the network, and it is not backed up frequently, it is your work that is lost when the hard disk in the server crashes.

BEWARE: backing up is NOT enough! You MUST periodically run your recovery procedure .... how else will you know it will work when you need it most?

PURCHASING
The policy should state the controls in place for purchase of both hardware and software, and it should be consistent and centralized. Unless you've seen what some software can do to destroy security, or how difficult it is to interconnect different equipment, this might seem to destroy some autonomous activities in your organization. Autonomy be darned, it's the company that's paying the bill.

MAINTENANCE AGREEMENTS
All warranty registrations must be mailed to the manufacturer, and records kept of purchase dates, expiry dates and repairs made under the warranty. Keeping accurate records has substantiated the complete replacement of more than one machine.

SOFTWARE LOADING
The checking, copying and loading of software should be the responsibility of one person or department. The 'penalty' for loading illegal/unauthorized software can range from a note in the personnel file to dismissal, depending on the organization. The opposite, copying the organization's software for loading in another location, should also be covered in the policy, because the company (as the registered owner) could be party to a lawsuit without the ability to plead ignorance.

EMPLOYMENT TERMINATION
In several organizations, when a person submits their resignation, their access to the computer system is immediately withdrawn. This, of course, requires a close liaison with the personnel department in large organizations. Many of these companies feel it's worth the salary cost

to have the person leave the premises immediately (escorted), and simply pay out their notice period. If your company adopts such a policy, it should be made very clear that it is not an indication of trust in the person, but simply a means to reduce risk to the valuable resources of hardware, software and data. It must be administered consistently and equitably to avoid problems. There are problems with such a policy, not the least of which could be someone who gives a very lengthy notice period simply because they're aware of the policy - but you could transfer them to a clerical job for the interim (like the mail room) or to maintenance staff (washroom detail).

- -

12. TO RUN SCAN (Virus detection software included on this diskette)

SCAN looks for 42 viruses in software files, but not in data files. I know it works on Jerusalem-B because I used SCAN to detect that virus on a machine at work. This is NOT the latest version of SCAN, but then again, you're not likely to have the latest viruses (I hope).

If you want to print the documentation, type: COPY A:SCAN.DOC PRN
If you want to run SCAN, just type: A:SCAN [drive identifier]
e.g., A:SCAN C:

An article from the Washington Post, January 14, 1990, on Computer Viruses was added to the diskette after this paper was written.

To read this article, key TYPE A:ARTICLE|MORE
To print the article, key COPY A:ARTICLE PRN

- -

If you have found this presentation useful, either by attending or by reading or using the information on this diskette, then I am rewarded. If you found it useful, please feel free to copy this diskette or its contents and share it with others - I would ask that you don't change anything, though. (It was virus free at the time I made the original diskette - but if you trust that statement, you might just have made your first mistake.)

If you'd like to make suggestions that would improve the information on this diskette, I would be very happy to hear from you. I'd also like to hear from you if you wish to discuss security issues, get a virus infection or hit by a Trojan Horse, or even just to comment on the contents of this paper. My address and phone number are on the first page of this document.

If you would like to join the National Computer Security Association, a 'form' for application is on the next page. They provide benefits such as a Virus Self-Defense Kit that's more sophisticated than the software on this diskette, newsletters, a virus-free bulletin board with hundreds of security-related programs, discounts on software, books and conferences, and advice if you run into trouble.

Happy (and safe) computing!

E. A. (Liz) Bedwell

National Computer Association
Suite 309

4401-A Connecticut Ave. NW
Washington, DC
USA 20008 Phone: (202) 364-8252

[ ] I wish to join NCSA. Cheque enclosed for $45.00 (US funds)

[ ] I wish to join NCSA. Please bill me for $45.00 (US funds)

Name: _____

Organization: _____

Address: _____

_____

City, Prov.: _____ Postal Code _____

Phone (with area code): _____

Title or Position, or interest in computer security:

_____

_____