RISK MANAGEMENT FORUM

AEAI/RIMS International Conference
October 15-18, 1989
Monte - Carlo

Please respond to

MONDAY, OCTOBER 16, 1989

SESSION NR 7

COMPUTER SECURITY

COMBATTING CRIME AND MISUSE OF DATA - IS INSURANCE A SOLUTION ?

SANDRA KOELZER

AEAI

Omer Leroy
UNILEVER
Conference Co-Chairma

Risk and Insurance Management Society, Inc.

gh Loader
etra Pak
ce Co-Chairman

Yet again, technology has presented what appears to be an overwhelming problem of risk identification, analysis, control and financing for risk managers throughout the world. Unwanted, extraneous instructions deliberately introduced into a software program with the specific malicious purpose to damage, delay or even destroy a system's functions are invading computer systems globally. Mainframes, mini computers, personal computers, secured and non secured systems, public, private, academic and military domains, communications systems, medical monitoring systems and financial institutions have all been affected and infected by the ubiquitous Computer Virus.

By using the classic risk management process, the computer virus issue can be properly analyzed, and solutions investigated so that losses can be avoided or damages mitigated by loss prevention activities or by risk financing techniques.

The process for understanding the potential for damage caused by computer virus is to understand the etiology of the virus, the problems that have occurred in the past, and the expected problems that will occur in the future.

Risk Identification:

The hazard to be identified is a computer virus. The following describe the virus:

→ A software program embedded in an apparently harmless second program. The virus contains a set of coded instructions that enable it to invade a host, replicate itself, and infect new hosts. It invariably contains a logic bomb to delay the onset data manipulation, therefore allowing itself to duplicate prior to detection;

→ A parasitic [attaches itself to another program], self-duplicating, Trojan-horse program containing a logic bomb;

→ Electronic infections that threaten the security of computerized information;

→ Can be benign or malicious. Benign viruses are annoying but intend no serious damage. Malicious viruses destroy the integrity of the disk's contents.

What are the different types of viruses?

→ **Computer Virus.** Replicates a form of itself by subverting other programs and spreading throughout a computer system or network where it may destroy or modify other programs, files or data. A virus hides inside other programs.

→ **Computer Worm.** Does not use the resources of other programs in the system, but may destroy or modify files, data or programs already in the system. A worm is written as a separate, stand-alone program.

→ **Trojan Horse.** Is dormant in the system until activated by an unsuspecting party, then performs functions intended by the mischief maker, such as overloading a system or destroying information. The Trojan horse seems benign but contains a small bit of malicious software. It is not self replicating.

→ Bomb. Need not be brought in from the outside, but is concealed in ordinary programs. It is not self replicating.

What is the manifestation of a viral infection in a computer?

- ✔ Slow down of the computer's functions
- ✔ Altered messages appear on the screen
- ✔ Memory space taken up
- ✔ System crashes that result in lost data
- ✔ Programs disappear on certain dates
- ✔ Problems with print command are incurred
- ✔ Files disappear
- ✔ Icons change or are mixed up; symbols or words are displayed on the screen
- ✔ Files grow in size until too large to execute
- ✔ Excessive floppy disk activity for simple tasks
- ✔ "SAVE" commands ignored
- ✔ Executable programs erased
- ✔ Systems suspended so that they will not respond to keyboard entries

What are some of the current viruses?

Viruses are usually identified by the name of their origin or by the screen display that indicates a system is infected: Lehigh, Scores, nVIR, Israeli or Black Hole, Alameda, Pakistani Brain, Italian, Ping-Pong, IBM Christmas Tree, Amiga, Flu-Shot 4, NASA,CyberAIDS, USPA & IRA Co., Falling Tears, and the like.

How are viruses transmitted?

Viruses seem to be transmitted by electronic means and by manual dissemination. Forensic study shows that viruses have spread between computers that communicate with other computers via telephone lines or by local area networks. Someone can infect his computer by copying an infected program from a computer bulletin board. There is some risk when using public domain software. Borrowed floppy disks that are used to boot personal computer systems can be carriers of bad programs.

What computer systems are susceptible to infection?

Computer viruses can appear in any type or class of computer, but have been most prevalent in personal computers and large computerized networks.

Where did viruses originate?

Viruses are not new. In the 1950's researchers studied programs called "self-altering automata" In the 1960s, computer scientists had viruses battling each other in a game called Core Wars, where the object was to create a virus small enough to destroy opposing viruses without being caught. The terms "virus" and "worm" were used in science-fiction novels in the 1970s, and some researchers devised self-replicating code that was intended to be productive by becoming tracers and timesaving devices.

By the 1980s, viruses had "escaped" from computer science laboratories and had fallen into the hands of "cyberpunks", unprincipled programmers. Almost anyone with computer programming skills can develop a virus program: disgruntled employees, publicity-seeking individuals or groups, extortionists, and similar persons. Some programmers have modified other writers' viruses to generate new strains, and there is much speculation regarding the true number of viruses in circulation.

Risk Analysis:

The assessment stage is intended to quantify the frequency and severity loss potential of a virus infection. The ability of rapid, worldwide electronic communication and the inherent potential for undetectable viruses that can infect any type of computer is not truly assessable in terms of monetary quantification. Herein lies the difficulty for information managers and risk managers. The assessment response may indeed be incalculable.

One of the most common exposures to viral infection arises from unlimited access. When to many people have access to information stored on a system, there is a greater chance of sabotage, mismanagement or accidental loss of data.

Mainframe or mini computers are usually used by more than one user and do have security features designed in them, even though it is common for businesses to use systems that are based on standard components and architecture. There appear to be fewer problems with viruses on mainframes than on microcomputers because of this security feature. With the micros, individuals manage the usage and access to a system, and are more apt to not conform to sound, sensible security measures without influence to do so. Further, due to the unlimited possibilities available to programmers, a "sure" cure for all viruses in all their forms may never be possible, so the assessment function can be altered by everchanging base assumptions.

Risk assessment may also identify the need for a company to become prepared for responses to business interruption resulting from damage to the data.

Risk Control:

Avoiding risk in the computer environment may only be accomplished by not using computers, and this solution is not satisfactory in the current environment, culture and technological climate. The management of risk may have to be a flexible program including assumption of some risk, reducing risk, and transferring risk, all they while having a prepared business resumption or recovery plan.

What then can be done about the computer viruses? Controlling virus invasion is the surest method to avoid expensive consequences. However, viruses appear to be far more difficult to protect against than any of the more familiar business threats of a purely physical nature.

A checklist of action items intended to avoid or mitigate damages is listed below:

✔ Prohibit downloading utilities or other programs from on-line services
✔ Install access-control programs and suitable physical security on all computers
✔ Copy files frequently onto backup disks
✔ Prohibit unlicensed, borrowed, public domain or software obtained outside an organization's approved channels to be introduced to a system
✔ Change individual network access codes frequently
✔ Allow 'read only' access for those employees who need only information from the system
✔ Provide a personal computer for testing and inspection by anti-viral programs of new or unknown software before such are introduced to the user community
✔ Use write protection on diskettes
✔ Preserve original program disks in a safe place and maintain duplicates of the originals prior to installing programs on a system
✔ Keep a record of all software loaded, when loaded and by whom

- ✓ Do not "boot" from borrowed floppy disks
- ✓ Maintain an employee awareness education program stressing reliance on good habits as a means of preventing virus, rather than specifically curing a virus outbreak
- ✓ Establish a written contingency and emergency notification plan for viral attacks
- ✓ Use anti-viral programs for detection or eradication of viruses

There are currently three types of anti-virus software programs being used. The first is a filter program designed to prevent infections. It stays in the computer's memory at all times, monitoring operations and watching for signs that a virus is attempting to infiltrate. When a filter spots abnormal behavior it freezes the system and flashes a warning message. Viruses have, unfortunately, been written to easily fool filters; also, filters can interrupt the user with false alarms.

The second program is an infection-detection program that takes a "snapshot" of the system and from time to time compares the operations of the system with that snapshot. If anything changes, an alert is given. The detection program uses computer processing time because it must periodically stop to perform its calculations.

A third type of program is a virus remover. It recognizes and eradicates common viruses. Unfortunately, because in this period of rapid evolution, virus writers keep releasing new mutations and eventually may even be able to create self-modifying viruses, the virus remover program may not be effective as a long term solution.

At the present time, it seems that backups of files are the single most important action that can be taken to protect a system against viral attack. Backup diskettes or tapes are also the lowest cost solution, when used in conjunction with operating a computer system in a sensible manner.

Risk_Financing:

While there is no comprehensive cure for computer viruses, insurance might be available as a risk financing mechanism to reimburse for damages suffered by a entity. At present, there are no insurance contracts with specific reference to viruses as perils or actions either covered or excluded, except in a few limited instances relating to large financial institutions.

The question of coverage, however, will undoubtedly be subject to a case-by-case review by insurers.

Policy types that should be considered and reviewed prior to occurence of loss are Electronic Data Processing policies, Property policies, Computer Crime policies, and Fidelity policies.

For first party EDP policies, the intent is to cover the actual cost of reproduction or replacing destroyed data damaged by certain physical perils or accidental data erasure. One issue for concern would be the virus that has not actually destroyed data but has caused the software and hardware to not function. If this is the cause of damage, meaning no physical loss or damage has occurred, there might be coverage available under an Extra Expense or Business Income coverage part. Coverage under EDP would not apply if the wrongdoer is a party named in the policy exclusions.

If a virus were to get into a system but does not destroy data or programs but simply used up space, the machine could not be used. However, the EDP policy would probably not cover losses since no physical loss or damage has occurred. When the virus does destroy data, loss would probably be covered since it physical loss or damage resulted. Generally, there should be attention to insurance policy language regarding destruction or damage to computer data and computer programs. It appears that unless the word "programs" is specified, there could be a problem recovering for program losses.

Property policies should be examined carefully for an understanding of "Property Subject to Limitations". It may be that the property policy has computer programs and electronic media covered for specified perils, including vandalism and malicious mischief. If an insurer can be convinced that computer virus losses resulted from vandalism or malicious mischief, the recovery may be limited to the cost of media in its blank form, not the cost to replicate the lost data.

Other considerations on the property policy should be a review of the "Perils Insured" definition, observing whether the language states coverage is for "all risks of loss or damage", or "all risks of *direct physical* loss or damage". Other potential areas for coverage question would be exclusions for unexplained or mysterious disappearance or employee dishonesty.

Once coverage is established for the damages caused by computer viruses, extra expense or business interruption coverage may be available, as such extra expenses resulted from an insured peril.

Computer crime policies may be a source for insurance recovery from loss or damages to electronic data, but may exclude losses caused by employees, by programming errors or by data entered by unauthorized persons. There may also be exclusion of coverage for fraudulent or intentional acts.

Fidelity insurance policies generally do not cover vandalism or malicious mischief losses.

It seems that at present, insurers may be unable to confirm coverage or intent with regard to damages caused by computer viruses. Present contract conditions and definitions may or may not be interpreted at the time of claim presentation to provide the needed coverage. A carefully designed, comprehensive EDP insurance program should respond to a virus claim.

Monitoring:

Ongoing risk assessment by individual computer users, by computer systems managers and by risk managers will review controls established for information protection as well as point out amendments needed to better manage the computer virus risk.

Conclusion::

The computer viruses is ubiquitous, insidious and potentially debilitating for any computer system anywhere in the world. Computer programmers without principle may never be stopped or detained from their destructive actions or pranks. It is indeed the responsibility of all users of computers, as well as certain corporate management, to become aware of potential problems and assist computer users with action plans that will offset efforts of virus attacks, therefore preserving system integrity and continuity of business operations.

While some effort has been made or is in progress with regard to legislation and statutory punishments for virus writers and damage perpetrators, the legal system will not be the sole deterrent or eradicator of problems.

Similarly, while there may be some financial recovery from insurance policies, a potential settlement or negotiated settlement will not preserve system integrity nor ensure business continuity.

Risk management, especially risk control and monitoring is the only sound solution for a long term system maintenance and resilience to computer virus attacks.