



WHITE PAPER

Designing and Implementing a Virus Prevention Policy: Key Issues and Critical Needs

Because Central Control
is the *Only* Virus Control

Trend Micro, Inc.

10101 N. De Anza Blvd., Suite 400
Cupertino, CA 95014

Phone: 1-800-228-5651 / 408-257-1500

Fax: 408-257-2003

Web: www.antivirus.com

Abstract:

Most computer managers in Fortune 1000 companies realize that computer viruses are a major threat to information security. And many believe that virus infection can be costly and lead to losses in productivity. But all too many do not know quite what to do about the threat of viruses. Before they even begin developing some type of company policy to address their concerns, many want to know what questions they should be asking and what issues they should be addressing. This paper provides the basis for development of a corporate anti-virus policy by identifying key issues, listing general tasks that must be performed to develop a policy, and referring to existing suggested outlines for security policies that are applicable to the development of an anti-virus policy. Products, people, and procedures are discussed, with an eye towards protecting companies from viruses transmitted via electronic file exchange--by far the most common method of virus distribution today. With this paper as a guide, MIS professionals now have a foundation for their efforts to develop an anti-virus policy tailored to their company's specific needs.

**September 1997
Trend Micro, Inc.**

©1997 by Trend Micro, Inc., 10101 North De Anza Blvd., Suite 400, Cupertino, CA 95014

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher. InterScan VirusWall and Trend are

registered trademarks of Trend Micro, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

Table of Contents

BACKGROUND	4
SCOPE AND ORGANIZATION OF DOCUMENT	6
PRODUCTS, PEOPLE AND PROCEDURES	7
PRODUCT SOLUTIONS	8
THE HUMAN ELEMENT	9
PUTTING IT TOGETHER WITH PROCEDURES	11
CONCLUSIONS	12
APPENDIX I: QUESTIONS TO ANSWER PRIOR TO ANTI-VIRUS POLICY DEVELOPMENT	14
CORPORATE CULTURE	14
PRODUCT/SERVICE STATUS AND USE	14
VIRUS HISTORY	14
APPENDIX II: ANTI-VIRUS POLICY DEVELOPMENT AND ADOPTION TASKS	15
REFERENCES	16
BIBLIOGRAPHY	16
ABOUT TREND MICRO	17

Background

Computer viruses are a major threat to information security. In a survey conducted by McGuire Research Services, Inc., for Trend Micro, computer managers surveyed in Fortune 1000 companies view viruses as the greatest threat to information security they face, above human error, hackers, and disgruntled employees. And a full 67 percent of survey respondents rated viruses as at least some threat to information security [1]. Dennis Miller, a comedian on the popular “Saturday Night Live” television program, made an observation about computer viruses during a recent news update sketch. He said, comparing computer viruses to the biological AIDS virus, “Remember, when you connect with another computer, you re connecting to every computer that that computer has ever been connected to.”

As viruses become more prevalent, the threat becomes more real, with over 13,000 existing in the world today. According to a survey released in April 1997 by the National Computer Security Association (NCSA), almost every medium and large organization in North America has experienced at least one computer virus infection firsthand. The survey also indicated that about 40 percent of all computers used in the surveyed companies would experience another virus infection within a year [2].

Computer viruses (i.e., any program or code that replicates itself) are insidious. Without virus detection or protection, users typically do not know their systems are being infected until they see results that can range from annoying to catastrophic. And virus infection is on the rise. Despite a significant increase in the usage of anti-virus products, the incidence of computer virus infection in corporate America nearly tripled in 1996 [2].

Although several factors are behind the rise in computer virus infection, the main one is the meteoric rise in popularity and use of the Internet in business. The Internet can be thought of as an information highway—an evolving global electronic mode of communicating, providing information, and obtaining information. Two important ways of enabling this communication are e-mail for exchanging mail and the file transfer protocol (FTP) for exchanging files. Growing at a staggering rate, the Internet is an unprecedented link between more people in more countries than ever before.

But along with these Internet capabilities comes a major problem. As the it becomes more popular as an e-mail and file transfer medium, users are at a growing risk from the many viruses that can be spread via e-mail attachments and FTP downloading/uploading. The NCSA survey reports that e-mail attachments as a source of infection tripled from 1996 to 1997--from 9% of all infection sources to over 26% of infections. At the same time, virus infection via downloading of files from the Internet increased from 10% of all infections to 16% [2].

To make matters worse, a relatively new class of viruses, called macro viruses, is now taking advantage of widespread Internet usage to spread like wildfire. In fact, these viruses are spreading faster than most anti-virus software makers can find ways to detect and remove them. Macro viruses are now the most prevalent form of computer virus in the world, representing 80% of all infections in North America in 1997, compared to 49% a year ago [2]. This prevalence is largely due to the new way in which they spread. Because they are written in Microsoft Visual BASIC, they can

insert themselves into the macros used in word processor and spreadsheet documents, which often are transmitted as e-mail attachments. And now, a new type of malicious code, carried by ActiveX and Java controls that spice up web pages, poses the potential for PC damage simply by users browsing the web.

Before widespread Internet popularity, viruses spread slowly from one part of the world to another. For example, the Michelangelo virus that appeared in Asia in 1991 did not appear prominently in Europe until 1992 and the U.S. one year later. Today, viruses migrate much faster than this rate of one continent per year. The Concept macro virus that became prominent in the U.S. in August 1995 appeared in Asia only two months later. On the Internet, an e-mail attachment alone can transmit a virus from one country to another in less than a minute, and the number of files now transmitted through the Internet each year may number in the billions.

What this means is that if you do not have an anti-virus security policy, you need one, because inaction can be costly. Depending on the size of the infection, a virus infection incident can cost between \$2,000 and \$500,000 in data loss and loss of productivity [3]. One study showed that the average cost of recovering from a virus infection on a network is \$15,000 and that 85 percent of those sites were re-infected within 30 days [3]. You can estimate the cost of an e-mail virus infection at your company using an Excel worksheet prepared by Trend Micro [4].

Scope and Organization of Document

The purpose of this document is to help MIS professionals understand the issues they face when considering the threat from computer viruses and help them identify the specifics in order to develop an anti-virus policy in their organization.

The scope of this document is limited to the anti-virus aspects of information security. While computer viruses are widely considered to be the greatest threat to that security, they are by no means the only threat. Many of the principles discussed in this paper are applicable to other aspects of information security, such as employee information theft, and other references provide additional information on these aspects [5,6].

Since electronic file exchange is now the primary vehicle of virus transmission, this document focuses here. File exchange includes sending and receiving Internet and Intranet e-mail attachments and file downloading from the Internet to internal local area networks as well as standalone PCs. These means of spreading viruses have largely supplanted the previously most common infection route of floppy diskettes. Of course, corporate anti-virus policies should not ignore the possibility of virus spread via floppies received from other firms or brought from home by employees.

This document stops short of guiding readers through a step-by-step process of developing an anti-virus policy. Such a policy must be tailored to the individual needs of each company. However, it does provide the basis for that development process by raising key issues, listing general tasks that must be performed to develop a policy, and referring to existing suggested outlines for security policies that are applicable to an anti-virus policy.

Products, People and Procedures

This section raises the key issues that MIS professionals must consider when formulating an anti-virus policy. These issues can be organized into the "three P's:" products, people, and procedures (see Figure 1).

Certainly, products such as anti-virus software are needed to thwart computer viruses. But even product vendors agree that, while a valuable part of the puzzle, products alone do not solve problems. People do. And if people understand the need for virus protection and the benefits of that protection, they are more likely to take appropriate steps. Defining these specific operational steps, "procedures", completes the triad. Through procedures, people make best use of available products to achieve the goal of comprehensive virus protection.

Figure 1 also illustrates the important distinction between procedures and the overall corporate policy. Charles Cresson Wood, an independent information-security consultant, defines policy as "high level statements intended to provide guidance to those who make decisions...typically including general statements of goals, objectives, beliefs, ethics, and responsibilities"[5]. Conversely, Wood defines procedures as "specific operational steps that workers must take to achieve goals--goals which are often outlined in the policy" [5]. Hence, any discussion of a corporate policy must also address procedures--the way the policy is to be implemented.

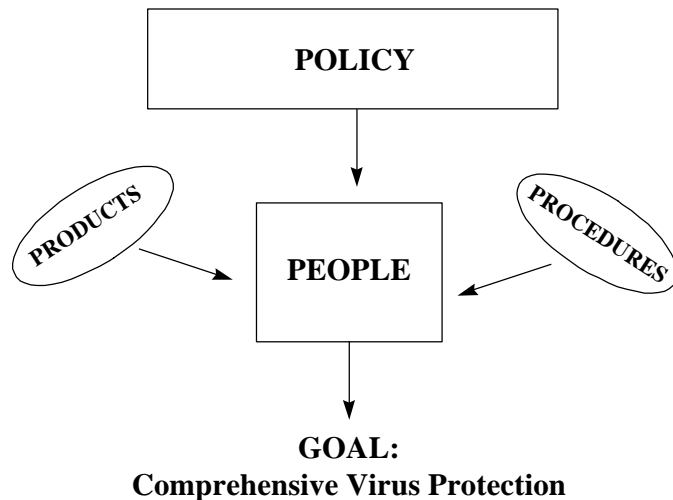


Figure 1. Products, people and procedures are needed to thwart computer viruses.

Product Solutions

The most effective way to ensure that your internal network remains virus-free is to monitor all entryways for viruses. While a detailed treatment of these entryways is beyond the scope of this paper, an overview of each key such gateway follows. For more information, refer to Trend Micro's network diagram and solution propositions at www.antivirus.com/products/enterprise/index.htm.

Figure 2 illustrates these entryways. Trend Micro's integrated family of virus protection products covers every access point--Internet gateways, groupware and Internet servers, LAN servers, and desktops. For example, in the case of remote users and those connected through remote servers, a remote server dials into the network several times during the night to exchange files with a number of different servers (see Figure 2). Trend Micro's ScanMail for Lotus Notes, for example, detects viruses in Notes mail and databases before they can be replicated and spread. Similarly, remote or telecommuting users can adopt Trend Micro's OfficeScan Corporate Edition desktop anti-virus product or the on-line HouseCall, a free service that scans on demand for in-the-wild and macro viruses at housecall.antivirus.com.

To protect your LAN from viruses that enter via the web, FTP downloads, and SMTP mail attachments, Trend Micro's InterScan VirusWall detects and eliminates viruses and other malicious mobile code in FTP, web, and e-mail traffic at the Internet gateway--before they can reach inside the network. A recently-introduced optional plug-in module adds spam blocking, e-mail content filtering, and mail traffic management capabilities to the InterScan product.

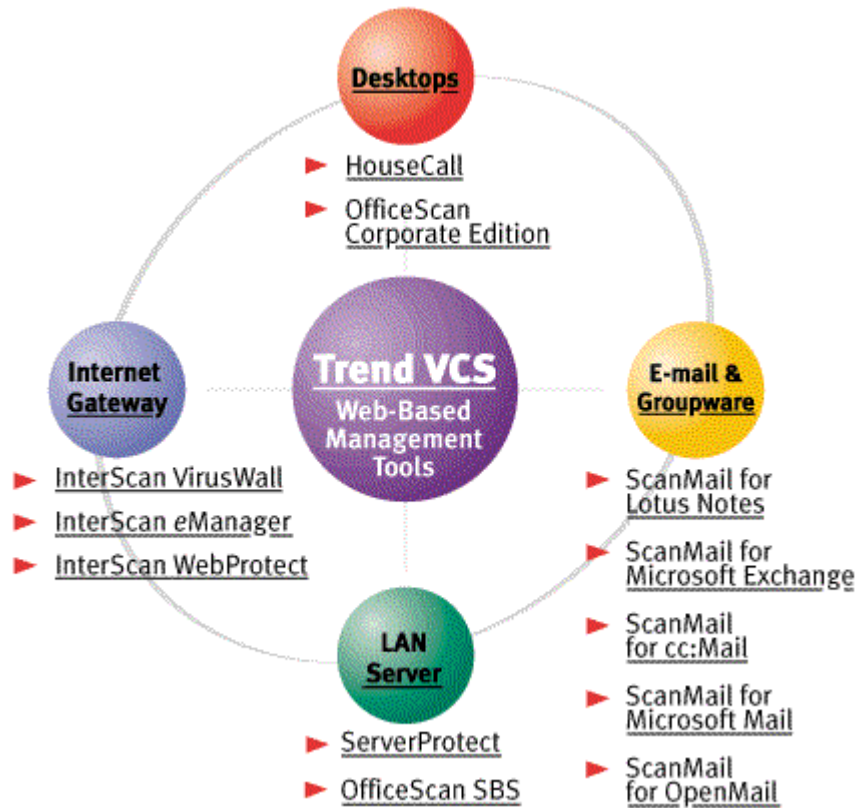
For the local area network servers themselves, Trend Micro offers ServerProtect for Windows NT and NetWare. Like other Trend Micro products, ServerProtect includes MacroTrap technology to detect known and unknown macro viruses.

For e-mail and groupware environments, Trend Micro has the ScanMail product line, which now includes ScanMail for Lotus Notes, ScanMail for Microsoft Exchange, ScanMail for Microsoft Mail, ScanMail for OpenMail and ScanMail for Lotus cc:Mail.

Where applicable, Trend virus protection products are certified by the National Computer Security Association (NCSA). All products provide comprehensive incident logging and reporting, customizable alert notification, and customizable configuration.

For an anti-virus product to be useful, it must reliably intercept viruses without impairing system performance and reliability or user productivity. Configuration and usage flexibility, management capabilities, and customer support are also key considerations when evaluating virus protection.

Figure 2. Complete virus protection for an enterprise requires anti-virus products at each virus entryway.



The Human Element

The key players, and of course, the ultimate target, in an anti-virus policy are the users and managers inside the company. Understanding the attitudes of the company's staff towards information exchange and an awareness of the history of virus infection and corresponding action taken will go a long way towards enabling you to understand your organization's unique "corporate culture". And this understanding is critical to the ultimate development of a policy that is right for your company. Two companies with different corporate cultures are likely to develop different policies. And beyond policy development, these two companies may very well implement their policies in different ways.

Let's examine a couple of very different company cultures and how their approaches to virus protection policies are closely linked to those cultures.

Company A, which grew quickly from a small firm to a medium-sized one, is quite open with its data and information. Few, if any, procedures have been established regarding information exchange, either between employees or with those outside the

company. Moreover, resistance to formalized procedures is high, as the company fosters a relaxed working environment as an alternative to the typical office environment of its competitors. So far, Company A has been lucky. Its only virus experience has been a couple of isolated run-ins with a relatively benign macro virus that was quickly eliminated from a floppy disk that had come in from an outside client. The employee had recently installed desktop anti-virus software that was able to detect the virus on the floppy before it could be copied to a hard disk. Both the employee and management reacted calmly to the virus detection, and no disciplinary action was regarded as necessary.

MIS professionals at Company A face the challenge of a workforce that is highly resistant to the kinds of procedures they view as necessary to reduce the virus threat. Employee motivation to act is low, since they have not experienced the stress and frustration of recovering from a major infection. Company A needs a campaign to promote awareness of the virus threat, reinforced by high level corporate commitment for this endeavor. Orientations and training seminars for all employees on the virus threat and of measures to be taken to minimize it, both initially and later to remind them of the need for compliance, will go a long way toward elevating their knowledge and understanding. Through this education process, Company A employees will learn that they can retain their relaxed working environment by taking a few simple precautions and following some procedures that require little time. Company A also needs a highly visible show of support by top management for efforts to minimize virus infection from the beginning of the policy adoption process. This can be done most easily by placing a management statement of support upfront on the anti-virus policy document.

In contrast, Company B is an established firm, with conservative employees. The company is not in a high technology field, but computers are used in various administrative functions. Company B's employees are accustomed to rules and regulations, and have come to value them for their assistance in minimizing problems. Most aspects of employee tasks are carefully organized to maximize productivity. The company has encountered macro viruses several times, without resulting in any major loss of productivity. But recently, Company B was infected by a virus received via an e-mail attachment from one of their customers that cost them considerable loss of productivity over several days. The employee who received the virus but, for whatever reason, did not detect it, feared he would lose his job, and management was upset over the incident.

Company B requires less training on the need for an anti-virus policy, but more emphasis on how to implement such a policy. Less computer savvy than their counterparts in Company A, Company B employees need periodic training to learn how to combat the threat. They are already motivated to comply with procedures, given their virus encounters, and they would have no problem in adapting to the inclusion of one more set of procedures in their work environment.

Putting it Together with Procedures

While the approach taken to developing an anti virus policy is likely to vary from company to company, some issues must be addressed in all cases--issues best addressed with a corporate policy that includes specific procedures.

For example, procedures are needed for making best use of selected product and service solutions, such as how to install and set up software to take advantage of automatic configuration and deployment, how to customize the level of protection appropriately for different types of user, and, most importantly, how to ensure that regular updates are obtained and deployed to all the workstations. New viruses are appearing at a rate of 250 or more every month. Operating too long without virus pattern updates unnecessarily exposes your company to new viruses 'in the wild' – particularly when product families like Trend Micro's can deliver these updates to fit your schedules, in the background without interrupting work, and use a single file to update both server and workstation-based protection.

But procedures go beyond product and service solutions. Procedures must address how new behaviors can be integrated into corporate culture to replace past practices that may have exposed the company to viruses. While centralized, server-based virus protection is important, it must be supplemented by commitment from the workforce to ensure a virus-free environment.

One way to encourage this distributed responsibility is to establish a virus response team. Similar to an emergency response team or other cross-disciplinary group in an organization, a virus response team can be assembled from many different departments, then trained and empowered to deal calmly, effectively and professionally with any virus incident. One advantage of such a team is that when an incident does occur, specific people are already selected to immediately tackle cleanup. Of equal importance, providing team members with a specific identity and status sends a message to all employees that virus protection is important and that it involves more than 'the guys in MIS'.

Another way to draw attention to an anti-virus policy after its adoption is to periodically review and revise it to reflect changing conditions. An annual review is usually sufficient and serves to reinforce an important issue that may not have been discussed for some time.

One particularly sensitive issue is dealing with policy noncompliance. The key is to foster an environment that encourages personal (and group) responsibility and that rewards honesty.

Consider, for example, an employee who promptly reports the appearance of a virus on their machine, probably because they downloaded unauthorized software from the web. If this is a first time occurrence for this individual, a formal meeting to discuss and reinforce anti-virus policy and procedures is appropriate, but further disciplinary action would discourage prompt reporting of virus incidents, allowing viruses to potentially spread unchecked through an organization. Of course, repeat offenses would call for more stringent actions. The idea is that failure to comply with anti-virus policy and procedures should be treated in a manner consistent with violations of other company policies.

Using the two hypothetical companies described in the previous section, Company A employees who detect a virus would probably not suffer an overreaction to a virus detection from management. Dismissal would not be considered for a first-time offender. Promoting awareness of the potential magnitude of the virus threat would promote understanding of the seriousness of violating anti-virus policy.

Conversely, managers at Company B might consider dismissing an employee who violated an anti-virus policy and cost the company significant loss of productivity, even if it was a first offense. At this company, taking advantage of the situation to demonstrate to others that management encourages virus reporting and to reinforce anti-virus procedures would have a more positive impact than dismissing the employee.

Conclusions

Trend Micro recommends that you address a series of issues before developing an anti-virus policy. These issues can be captured in the form of questions organized in three groups--corporate culture, anti-virus product/service status and use, and virus incident history (see Table 1). These questions encourage you to address issues specific to your company, enabling you to tailor an anti-virus policy to meet your company's unique needs and situation.

The policy you develop must integrate anti-virus products/services, people, and procedures in a manner consistent with your corporate culture, mission and goals. The resulting policy must be clear, concise, and consistent with other corporate policies. Several references contain suggested outlines of security policies, which can be used as a model for your anti-virus policy [5,8].

Table 2 lists the steps necessary to address issues prior to policy development, develop a policy, maximize the chances of its successful implementation, and periodically review and reinforce it. After policy development, review, revision, approval, and distribution, further steps might include developing an anti-virus procedure manual, assembling and empowering a virus response team, upgrading anti-virus product/service use, and beginning an employee awareness campaign (see Figure 3).

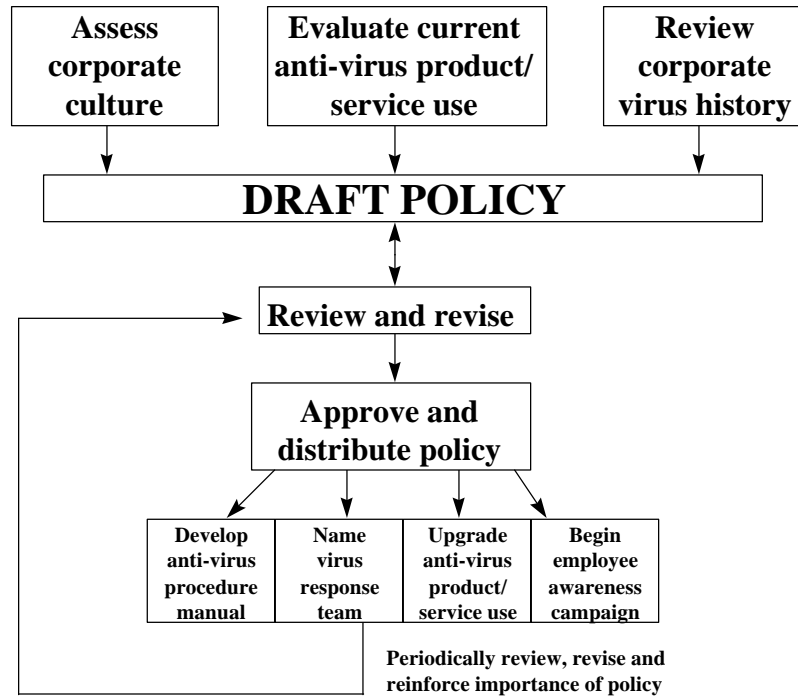


Figure 3 Effective virus prevention goes beyond anti-virus policy development

Appendix I: Questions to Answer Prior to Anti-Virus Policy Development

Corporate Culture

How would you characterize the openness of information exchange in your organization?

Are your employees open or resistant to formalized procedures?

Do any formalized procedures exist that regulate information exchange in your company? If so, to what extent do they explicitly address virus protection?

Has management made any mention of anti-virus policy or procedures in formal announcements to employees? Any mention of other security issues?

Do new employees sign an agreement that includes any mention of anti-virus policy? If so, what are employees' responsibilities?

Does your company have a virus response team? If so, what are their responsibilities? How widely is it represented across the company? Are team members given a different status in any way?

Product/Service Status and Use

What anti-virus products or services does your company currently employ?

What virus entryways are protected with anti-virus products or services? (Refer to Figure 2 for virus entryways.)

Are anti-virus software products periodically updated? If so, how often?

Virus History

Has your company experienced any virus incidents? If so, how many in the last year?

What type of impact did the infection(s) have on operations?

How widespread within the company was knowledge of the incident(s)?

How did the employee(s) who reported the incident(s) react? Did they downplay its importance or were they highly concerned?

How did management react to the incident(s)? Was any disciplinary action taken against the employee(s)?

Appendix II: Anti-Virus Policy Development and Adoption Tasks

1. Assess corporate culture
2. Evaluate current anti-virus product/service use
3. Review corporate virus history
4. Draft policy
5. Review and revise draft anti-virus policy
6. Approve and distribute anti-virus policy
7. Draft, review, revise, approve, and distribute anti-virus procedure manual
8. Name members of virus response team
9. Upgrade anti-virus product/service use
10. Begin employee awareness campaign
11. Periodically review and revise anti-virus policy
12. Periodically reinforce importance of policy

References

1. McGuire Research Services, Inc., "*Report of Results from a Telephone Survey of 250 MIS Managers in Major U.S. Businesses*," prepared for Trend Micro, Inc., August 30, 1995.
2. "NCSA® 1997 Computer Virus Prevalence Survey," NCSA, available at www.antivirus.com/corporate/white/index.htm#NCSA
3. Dataquest Survey, 1994
4. "Assessing the cost of e-mail virus infection and prevention," Trend Micro, worksheet, www.antivirus.com/products/vcost.html
5. "Policies From the Ground Up," Charles Cresson Wood, Infosecurity News, March/April 1997, pp 24-28.
6. "The Wolf Within," Sara Edington, Corporate Online, April 1997.
7. "Trend Micro Delivers the First Free On-Line Virus Scanning Service," Trend Micro, press release, May 7, 1997
8. "Policy Format and Structure," Gerald W. Grindler, Infosecurity News, March/April 1997, p. 29.

Bibliography

- "Trapping the World's Most Prevalent Viruses," Trend Micro, June 1997, available at www.antivirus.com/corporate/white/index.htm#Trapping
- "Trend Micro Delivers the First Free On-Line Virus Scanning Service," Trend Micro, press release, May 7, 1997, available at www.antivirus.com/corporate/media/1997/pr050797.htm.
- "ActiveX and Java: The Next Virus Carriers?" Trend Micro, May 1997, available at www.antivirus.com/corporate/white/index.htm#ActiveX and Java
- "Policies From the Ground Up," Charles Cresson Wood, Infosecurity News, March/April 1997, pp 24-29.
- "Policy Format and Structure," Gerald W. Grindler, Infosecurity News, March/April 1997, p. 29.
- "NCSA 1997 Computer Virus Prevalence Survey," NCSA, available at www.antivirus.com/corporate/white/index.htm#NCSA
- McGuire Research Services, Inc., "*Report of Results from a Telephone Survey of 250 MIS Managers in Major U.S. Businesses*," prepared for Trend Micro Devices, Inc., August 30, 1995.

About Trend Micro

Trend Micro provides centrally controlled server-based virus protection. By protecting information that flows through file servers, e-mail servers and Internet gateways, Trend Micro lets major companies worldwide stop viruses from a central point before they ever reach the desktop. Trend Micro's award-winning products have been chosen by Check Point Software, Hewlett-Packard, IBM, Intel, Lotus Softswitch, Microsoft, Netscape, Oracle, Sun Microsystems, Wingra and WorldTalk as a key part of their server security solutions. Trend Micro is privately held and based in Cupertino, Calif., with offices worldwide.

Trend Micro's Web site, <http://www.antivirus.com>, features the most comprehensive enterprise-level virus protection information available on the Internet. Visit this Web site often for management advice, technology updates, and evaluation copies of all of Trend's products. Additional information about Trend's products can be obtained by sending an e-mail directly to info@trendmicro.com.

For More Information

For more information on Trend Micro's range of virus protection solutions, contact:

Trend Micro, Inc.
10101 N. DeAnza Blvd., Suite 400
Cupertino, CA 95014
Phone: (408) 257-1500
Fax: (408) 257-2003