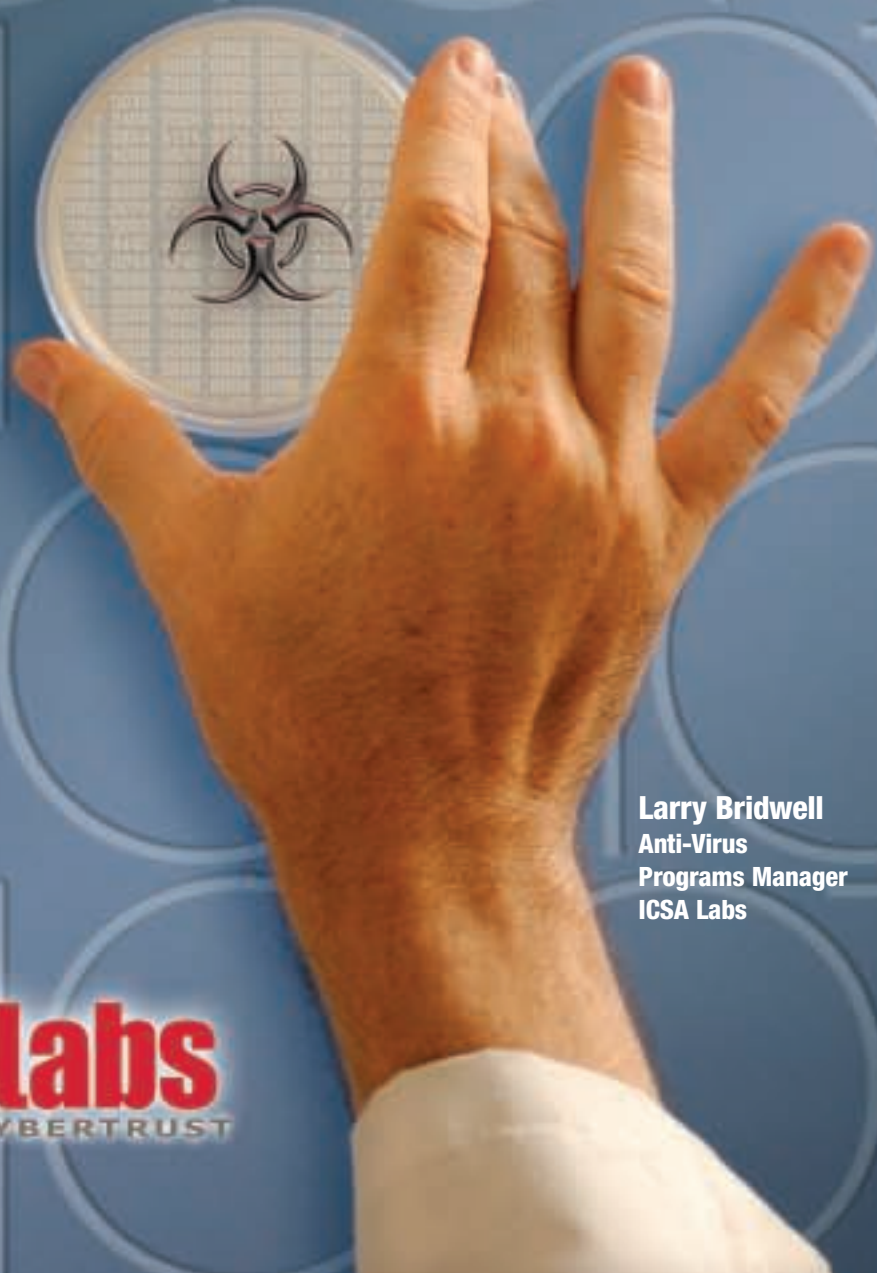


ICSA Labs 10th Annual

Computer Virus Prevalence Survey



Larry Bridwell
Anti-Virus
Programs Manager
ICSA Labs

icsalabs
A DIVISION OF CYBERTRUST



AVG Anti-Virus

PLATINUM SPONSOR

GRISOFT SOFTWARE

Founded in 1991, Grisoft is a privately held company with corporate offices in Europe and the US. Grisoft is focused on developing software solutions that provide protection for computers from viruses. Grisoft's primary focus is to deliver to the market the most comprehensive and proactive protection available for individual consumers, small to medium sized businesses, and large corporations with industry leading software solutions to protect their information and communications systems. Employing some of the world's leading experts in anti-virus software, more specifically in the areas of software developments, virus analysis and detection, and technical support, Grisoft is uniquely positioned to continue its leadership in the industry.



EDUCATIONAL SPONSOR

MIS TRAINING INSTITUTE

Founded in 1978, MIS Training Institute is the international leader in audit and information security training, with offices in the US, UK, and Asia. MIS' expertise draws on experience gained in training more than 100,000 delegates across five continents. MIS presents seminars and conferences in the areas of internal and IT audit; information security; network infrastructure; operating environments; and enterprise applications. MIS offers Web-based training at www.misionline.com as well as a variety of products and services including on site training and publications. MIS Training Institute is a Euromoney Training Group company.



GOLD SPONSOR

McAfee Inc.

McAfee, Inc. [NYSE: MFE] creates best-of-breed computer security solutions that span large enterprises, governments, small and medium-sized businesses, and consumers, helping prevent intrusion on networks and protecting computer systems from the next generation of blended attacks and threats. These next-generation threats attack on multiple levels of the network infrastructure. McAfee, Inc. offers in-depth protection—from the network core to the perimeter to complete desktop security—through two families of products: McAfee® System Protection Solutions, securing desktops and servers, and McAfee Network Protection Solutions, ensuring the protection and performance of the corporate network.



SILVER LEVEL

MICROSOFT CORPORATION

Founded in 1975, Microsoft (NASDAQ: MSFT) is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software any time, any place and on any device.

SOPHOS PLC

Sophos is a world leading developer of anti-virus and anti-spam software. The company protects businesses and organizations - from small enterprises to academic and financial institutions to governments and global corporations - against viruses and spam. Sophos is acclaimed for delivering the highest level of customer satisfaction and protection in the industry. The company's products are sold and supported in more than 150 countries.

TREND MICRO, INC.

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services, focused on providing customers with comprehensive security strategies to manage the impacts of known and unknown threats. Trend Micro has offices in 25 countries, and trades stock on Tokyo Stock Exchange and NASDAQ.

VIRUS BULLETIN

Virus Bulletin has a formidable reputation as the leading specialist publication on computer viruses. Each issue contains news and opinions from the AV community, detailed analyses of the latest threats, comparative product reviews featuring the unique VB 100 percent award scheme and the VB Spam Supplement, covering anti-spam issues. The annual Virus Bulletin conference being cited by many as the anti-virus event of the year. www.virusbtn.com

BRONZE LEVEL

ESET, PLC

Founded in 1992, ESET has focused on developing innovative antivirus software systems. NOD32 has evolved from that development process to be consistently rated as one of the best anti-virus products. For more information, visit www.nod32/home/home.htm

FORTINET

Fortinet is the leader of the Unified Threat Management market. The company's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time without degrading network performance.

ICSA Labs 10th Annual

Computer Virus Prevalence Survey

Sponsors:

PLATINUM SPONSOR

Grisoft Software

GOLD SPONSOR

McAfee, Inc.

SILVER LEVEL

Microsoft Corporation

Sophos PLC

Trend Micro, Inc.

Virus Bulletin

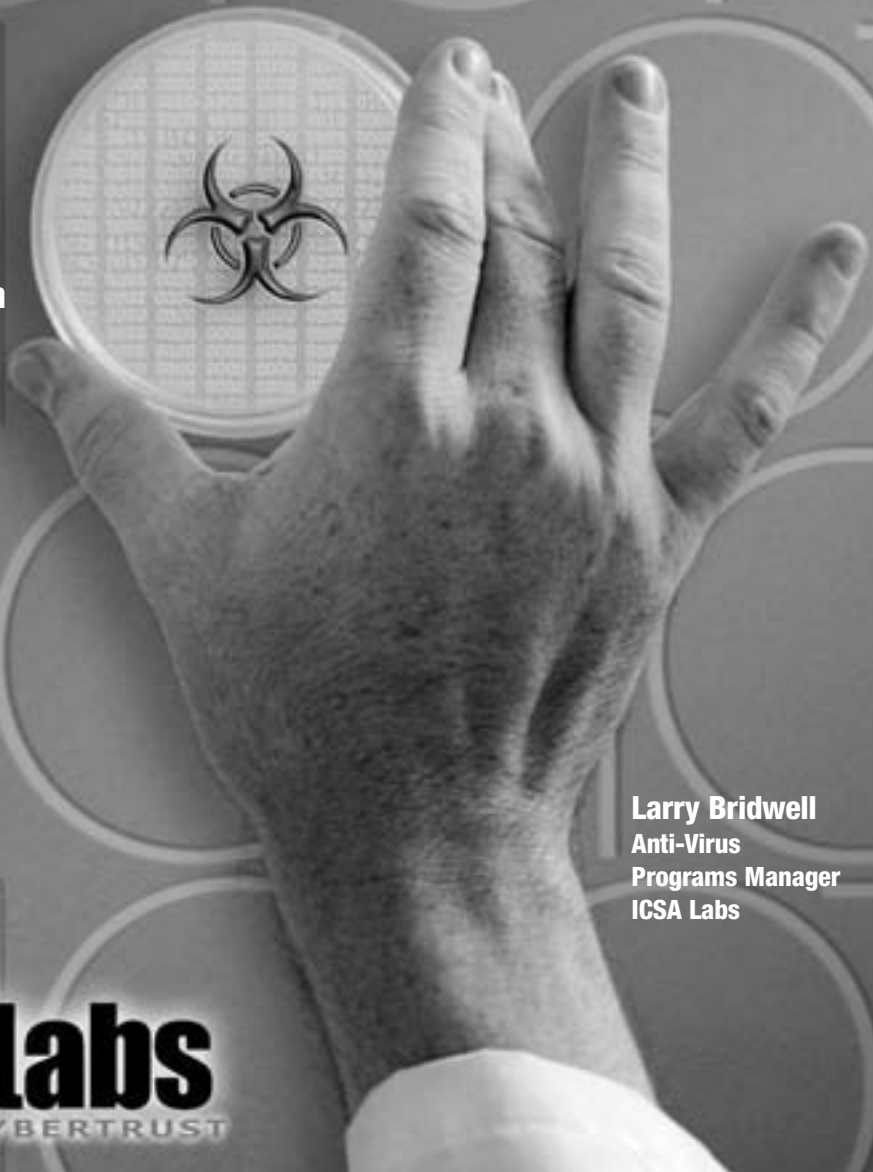
BRONZE LEVEL

Eset, PLC

Fortinet, Inc.

EDUCATIONAL SPONSOR

MIS Training Institute



Larry Bridwell
Anti-Virus
Programs Manager
ICSA Labs

icsalabs
A DIVISION OF CYBERTRUST

Table of Contents

EXECUTIVE OVERVIEW	1
How common are virus encounters?.....	1
What are the characteristics of virus disasters?	1
What are the effects of virus disasters?.....	1
How did respondents perceive the evolution of the virus problem?.....	1
How are anti-virus products used?.....	2
SURVEY OBJECTIVES.....	3
RESEARCH METHODOLOGY.....	3
Confidence	3
Selection.....	3
Rounding.....	3
Previous Work	3
PRINCIPAL FINDINGS.....	4
2004 Demographics	4
How Common Are Virus Encounters?	4
Chance of a Disaster	5
Respondent Perception of the Virus Problem.....	5
DETAILED FINDINGS.....	7
The Ever-Changing Picture of Computer Viruses and Their Prevalence.....	7
Virus Encounters versus Virus Infections.....	7
Top Reported Viruses	7
Virus Disasters.....	8
Date of last virus disaster?	9
Which virus caused the most recent disaster?.....	10
How many machines were infected in disasters?	10
What are the effects on victims of virus disasters?.....	11
How long were servers down?.....	11
What was the cost of the disaster in person-days?.....	11
What was the cost in dollars to your company?	12
Virus Impact	14
What are the organizational effects of viruses?	14
Where Do They Come From?.....	15
Usage of Anti-Virus Products.....	16
Overall Level of Usage	16
Anti-Virus products employed on desktops.....	17
Server anti-virus methods	19
Anti-virus Usage on Perimeter Services.....	19
Perimeter anti-virus methods	20
DISCUSSION SECTION	23
The virus problem continues to worsen.....	23

Virus Types	23
Perceptions of the Virus Problem	24
Virus Disasters and Costs	24
Virus disaster impact	24
Protection Strategies	25
APPENDICES	28
Appendix A: Survey Questionnaire	28
Appendix B: Possible Biases	31
Retrospective Study	31
Correctness.....	31
Site Selection	31
Familiarity.....	31
Appendix C: Glossary of Common Terms in Anti-virus Discussion	32

List of Figures

Figure 1: Infections per 1,000 PCs per month	5
Figure 2: Opinions of the virus problem 2003	6
Figure 3: Encounters per month, 2003	7
Figure 4: Respondents experiencing virus disaster	9
Figure 5: Viruses causing most recent disaster	11
Figure 6: Frequency distribution of server downtime	11
Figure 7: Loss in person-days due to disaster	12
Figure 8: Distribution of dollar costs	14
Figure 9: Effects of viruses	15
Figure 10: Virus encounter vectors	15
Figure 11: Desktop anti-virus usage	16
Figure 12: Desktop coverage by frequency of response	17
Figure 13: Anti-virus methods used	18
Figure 14: Anti-virus methods used on file servers	19
Figure 15: Comparison of perimeter anti-virus coverage, 1997-2004	20
Figure 16: Anti-virus methods used on gateway by percentage	22

List of Tables

Table 1: Top viruses for 2004	8
Table 2: Date of most recent disaster	9
Table 3: Virus causing most recent disaster	10
Table 4: Frequency distribution of dollar costs	13
Table 5: Sources of infection, 1996-2004	15
Table 6: Anti-virus software usage	16
Table 7: Desktop anti-virus products in use	17
Table 8: Respondents using specific anti-virus methods	18
Table 9: Perimeter coverage by frequency distributions	19
Table 10: Anti-virus methods in use on email gateways	21
Table 11: Anti-virus methods used on proxy servers	21
Table 12: Anti-virus methods used at the firewall	21

ICSA Labs Virus Prevalence Survey 2004

Executive Overview

ICSA Labs' annual Virus Prevalence Survey gathers data to measure the prevalence of computer viruses and malware in medium to large companies. The ICSA Content Security Lab and corporate sponsors, who support the survey each year, organized the Tenth Annual Virus Prevalence Survey 2004. Qualified respondents who work for corporations and government agencies with more than 500 PCs, two or more local area networks (LANs), and at least two remote connections completed the survey questionnaire. The annual report describes the existing computer virus problems and attempts to interpret trends of virus propagation and infection vectors, and explores possible risk mitigation methods.

HOW COMMON ARE VIRUS ENCOUNTERS?

This year's sample of respondents reported more than 3.9 million virus incidents on more than 900,000 desktops, servers, and perimeter gateways. This translates into 392 encounters per 1,000 machines, per month over the survey period from January 2004 through December 2004, with a rate of 116 infections per month by the end of the survey period.

WHAT ARE THE CHARACTERISTICS OF VIRUS DISASTERS?

For this survey, a virus disaster equates to an incident in which 25 or more PCs or servers are infected at the same time with the same virus or an incident causing significant damage or monetary loss to the organization. When using the latter criterion, the respondents were asked to qualify the disaster, i.e. number of machines, loss of data, loss of productivity, revenue loss, etc.

WHAT ARE THE EFFECTS OF VIRUS DISASTERS?

This year 112 of 300 respondents reported a *virus disaster* representing a 12 percent increase over the 92 reports in 2003. Another point of significance was an increased recovery time. While recovery time had risen only slightly in 2003, this year's rise was an increase of seven person days or almost 25 percent. 2004 also saw a significant jump in cost related to recovery, which rose to more than \$130,000 marking, for the second year in a row of sharply increasing costs. When one considers our respondents are technical persons responsible for virus protection and remediation, it is not hard to understand the historical under-estimation of recovery costs. Our past research reveals technical respondents to our surveys have historically underestimated recovery costs by at least a factor of seven, when one considers both direct and indirect costs. With that underestimation in mind, it is easy to see real recovery costs for a virus disaster being a great deal larger when all costs, both soft and hard are measured.

HOW DID RESPONDENTS PERCEIVE THE EVOLUTION OF THE VIRUS PROBLEM?

Again, respondents believe the problem is worsening. Only nine percent of this year's respondents felt the problem was *About the Same* and none felt the situation was *Better*. This is an interesting point because last year was considered by respondents the worst year reported! Ninety-one percent of respondents felt the virus problem was either *Much* or *Somewhat Worse*.

ICSA Labs Virus Prevalence Survey 2004

HOW ARE ANTI-VIRUS PRODUCTS USED?

Almost all (99 percent) of respondents report anti-virus software products protect at least 90 percent of their machines. The products protecting the majority of desktops, servers, and perimeter devices are those sold by McAfee, Inc., Symantec Corporation, and Trend Micro.

The 2004 results revealed a continuing up-tick in the use of anti-virus products at the internet perimeter. Email gateway coverage is up significantly with 96 percent of participants reporting installation of anti-virus products. Firewall and proxy server protection is also up slightly. However, this year's survey respondents also report that gateway filtering (blocking, quarantining, or stripping) of email and attached files have increased to more than 90 percent.

ICSA Labs Virus Prevalence Survey 2004

Survey Objectives

The objectives of this project are to examine the prevalence of computer viruses in mid- and large-sized organizations; describe the computer virus problem in computer networks, including desktop computers, application and file servers, and perimeter devices such as firewalls, gateways, and proxy servers; and observe trends in computer virus growth, infection methodologies, and attack vectors. The scope of the survey report includes Intel-based or Intel-compatible PCs¹ at sites with more than 500 PCs, multiple LANs, and two or more remote connections. We surveyed only the commercial, government, and industrial business sectors.

Research Methodology

CONFIDENCE

Data was collected from 300 qualified respondents. The sample size provided an accuracy rate of ± 6 percent with a confidence limit of 94 percent for questions that relate to the entire data sample.

SELECTION

We selected survey participants from a qualified list of sites with 500 or more PCs, two or more LANs, and two or more remote connections at that site. We also screened respondents to insure that they were the persons most responsible for computer virus protection within their organizations.

ROUNDING

Occasionally percentages will total more than 100 percent because some questions allowed for multiple responses. In some cases, rows or columns in tables may total either 99 percent or greater than 100 percent due to rounding. Likewise, charts or graphs may show less than 100 percent due to the exclusion of *Don't Know*, *Refused*, or *Other* responses.

PREVIOUS WORK

Some 2004 survey results will compare directly with the results of five previous surveys²:

- A previous survey conducted for ICSA during January through Feb 2004
- A previous survey conducted for ICSA during January through Feb 2003
- A previous survey conducted for ICSA during January through Feb 2002
- A previous survey conducted for ICSA during May through June 2001
- A previous survey conducted for ICSA during May through June 2000

¹Data gathered for Macintosh and other non-Intel servers and workstations may be referred to; however, they will only be considered anecdotal in this report.

²Data from surveys from 1996, 1997, 1998, and 1999 is considered when applicable.

ICSA Labs Virus Prevalence Survey 2004

Principal Findings

2004 DEMOGRAPHICS

The 2004 survey represents a total of 947,632 desktops, servers, and perimeter gateways. The average site in the survey had 3,002 PCs (the median was 1,325) and 157 file and application servers (median was 59).

HOW COMMON ARE VIRUS ENCOUNTERS?

All of the companies responding to the survey experienced at least one virus encounter during the survey period.

These organizations experienced more than 3.9 million encounters during the 12 month period from January 2004 through December 2004. This translates to 392 encounters per 1,000 machines per month over the survey period, with a rate of 116 infections per site per month by the end of the survey period. This rate continues the trend of an increase in infection rate each year. Most noteworthy is the marked increase in *encounters* versus actual *infections*. For the purposes of this survey, an encounter is anytime a virus has been encountered and dealt with in some fashion, but not necessarily activated. Examples of encounters may be finding an infected file on a backup diskette or tape, filtering, blocking, otherwise intercepting files at the gateway, or detecting a virus in a downloaded file or an actual activation and propagation.

In a comparison of the survey data for 1996 – 2004, Figure 1 shows that from 1996 through 1998, virus encounters show a steady rise of approximately 12 virus infections per 1,000 machines per month each year through 1998 and again from 1999 – 2001. The rate spike anomaly from 1998 to 1999 specifically relates to the Melissa outbreak incident of 1999 and its mass mail payload. From 2001 to 2004, the increase per year remains rather level, with 2004 showing the largest increase in infections since 1999. We derived this data by determining the average infection rates reported two months immediately before collection of survey data. The prior two months (i.e., November and December) were used for comparison because, historically, they produce the greatest accuracy in participant responses.

ICSA Labs Virus Prevalence Survey 2004

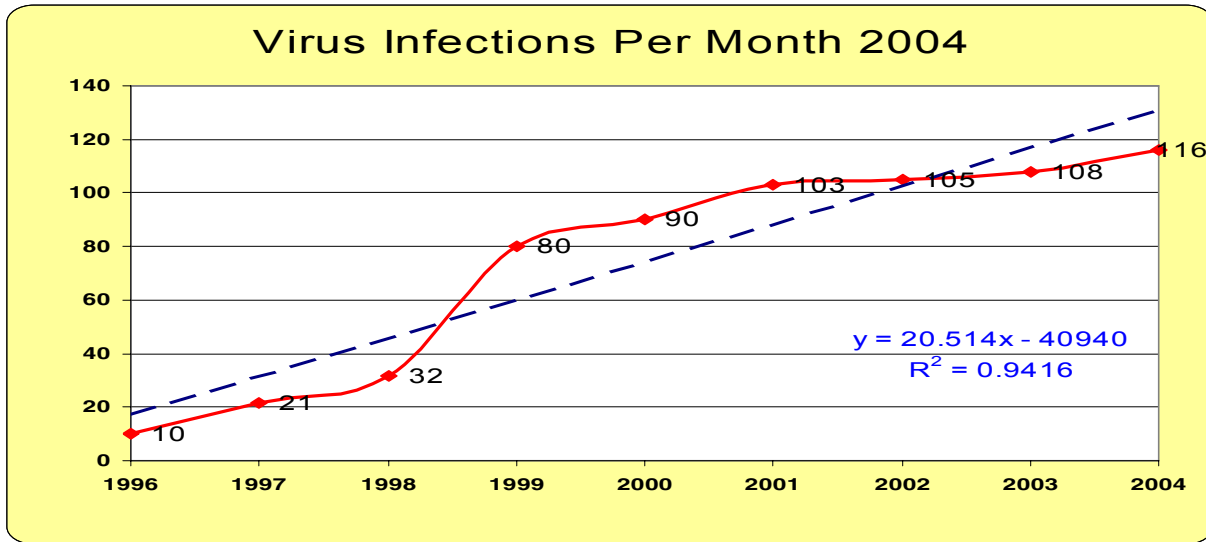


Figure 1: Infections per 1,000 PCs per month

CHANCE OF A DISASTER

For the purposes of this survey, a virus disaster is defined as an incident in which 25 or more machines experienced a single virus at or about the same time. Due to the changes in virus infection and propagation vectors, we have expanded the definition to include virus incidents that caused organizations significant damage or monetary loss. Survey respondents were asked if their organizations had experienced a “disaster” during the survey period; 92 responded in the affirmative.

ICSA Labs Virus Prevalence Survey 2004

RESPONDENT PERCEPTION OF THE VIRUS PROBLEM

We asked respondents to express their opinion of the computer virus problem, and to respond on a scale of *Much Worse* to *Much Better*. Figure 2 represents these answers. The respondents clearly believe that the problem of computer viruses, in general, was much worse in 2003 than in 2004. Of the respondents, only 12 percent felt the problem was about the same or better, the lowest percentage ever reported in this survey.

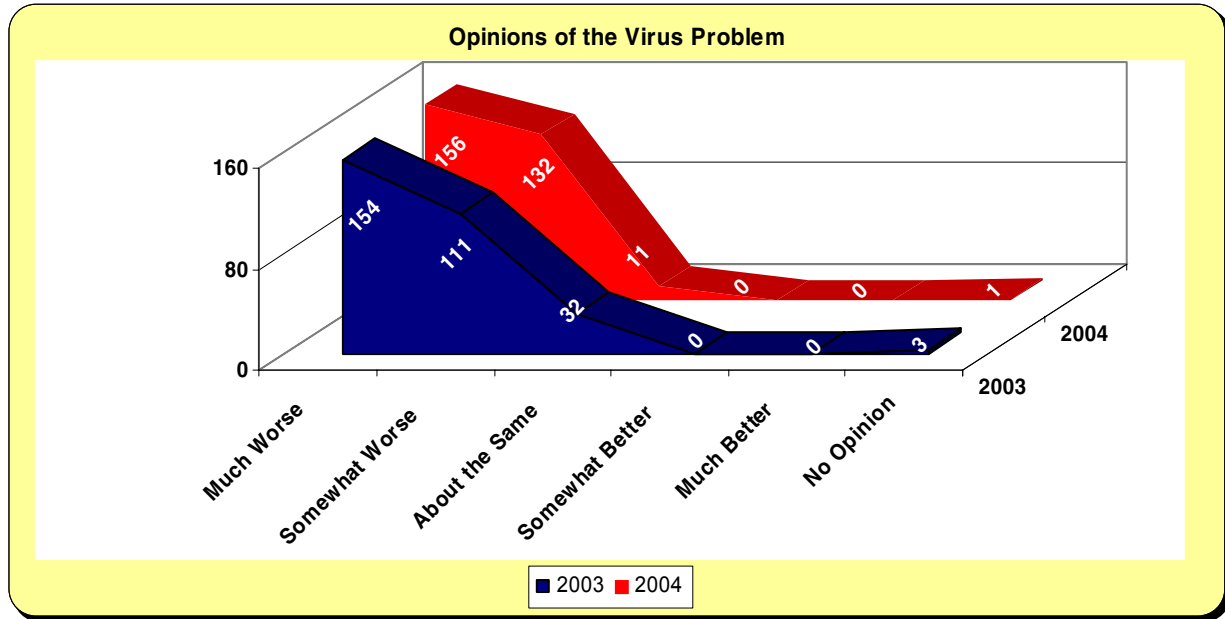


Figure 2 Opinions of the virus problem 2003 compared to 2004

ICSA Labs Virus Prevalence Survey 2004

Detailed Findings

The Ever-Changing Picture of Computer Viruses and Their Prevalence

The primary objective of this work each year is to ask the question, “How has computer virus prevalence changed?” The following detailed findings offer insights into several significant changes in computer viruses. These include not only growth in prevalence, but also growth in the severity of payloads, consequences of infection, and changes in attack vectors. These detailed findings also help us determine the risks posed by computer viruses.

VIRUS ENCOUNTERS VERSUS VIRUS INFECTIONS

As reported above, virus encounters continue to rise. Figure 3 below gives us a picture of the survey period January 2004 through December 2004.

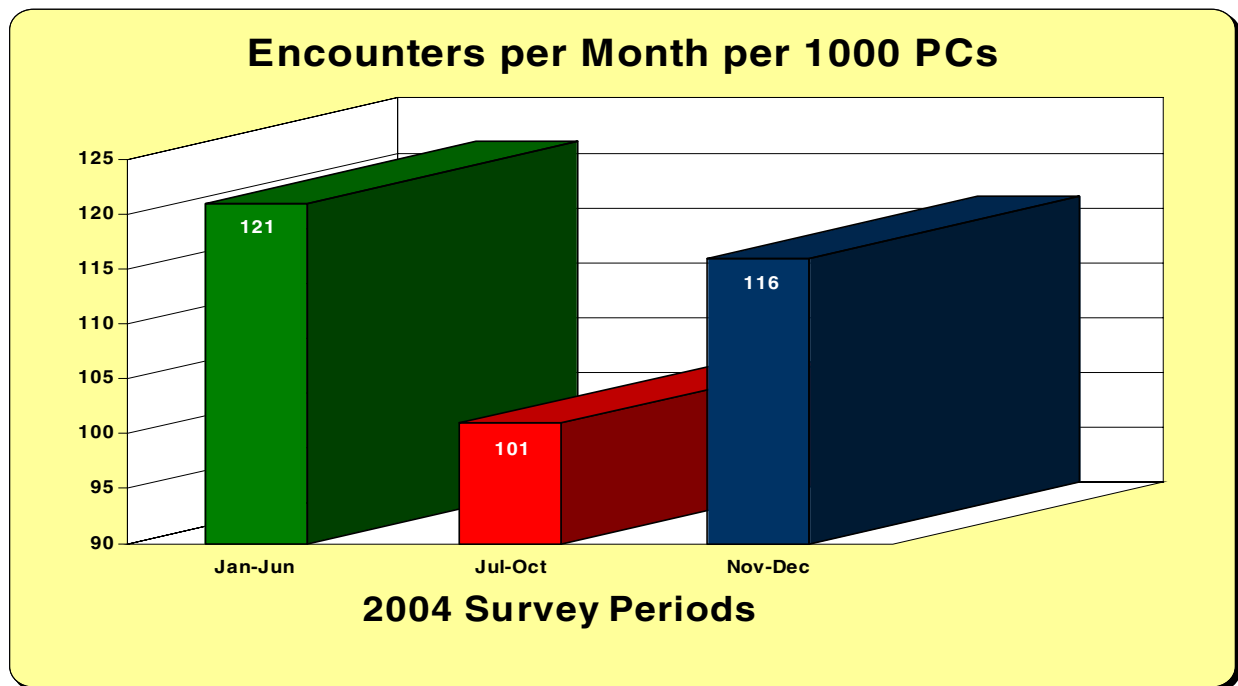


Figure 3: Encounters per month, 2004

TOP REPORTED VIRUSES

Certain viruses are more likely to spread than others. Many factors determine whether a virus is likely to spread. Viruses such as mass mailers continue to grow in prevalence while others, such as simple macro viruses, are in decline. Still others, such as boot sector viruses seem to have disappeared. Respondents were asked which viruses effected their group. Due to the large number of known viruses and their many variants³; a lack of

³ Over 70,000 known

ICSA Labs Virus Prevalence Survey 2004

standardized identification scheme⁴; and, at times, poor record keeping, respondents were not always able to identify the viruses with certainty. In all instances, every effort was made to identify individual responses at least to the virus family name. In instances where exact names were not known, partial names were given, or virus types were given and the data was pooled as, *unspecified*.

In contrast to 2002, 2003 saw a noteworthy increase in serious viruses and saw a significant number of virus outbreaks. In fact, several viruses that made the Top 10 list in previous years' surveys did not make it in this year's top viruses. Table 2 presents the Top 10 reported viruses for 2004 by rank from 1 to 10.

The table shows virus encounters per month for the period January – December 2004.

2004 Rank	Virus Name
1	W32/Netsky
2	W32/Zafi
3	W32/Bagle
4	W32/Dumaru
5	W32/Sober
6	W32/Mimail
7	W32/MyDoom
8	W32/Sasser
9	W32/Lovegate
10	W32/Klez

Table 1: Top viruses for 2004

Virus Disasters

Survey respondents were asked, "Has your group had a virus disaster anytime since January 2004?" Figure 4 shows that 112 survey respondents reported a virus disaster event. This year's 37 percent response was a 6 percent increase over the 31 percent rate in 2003.

⁴ In 1991, a group of security experts known as the Computer Anti-Virus Researcher Organization (CARO), developed a computer virus naming scheme and it was dubbed the "1991 New Virus Naming Convention" (NVNC '91). This scheme promoted the now commonly used 'Family_Name.Group_Name.Variant' formulation as well as setting laying out guidelines for what NOT to use in naming viruses. While this scheme is being used by more companies and with greater consistency than in the past, the fact is there is no standardized identification or naming convention accepted and used by the entire anti-virus industry. There is research being done on this at this time.

ICSA Labs Virus Prevalence Survey 2004

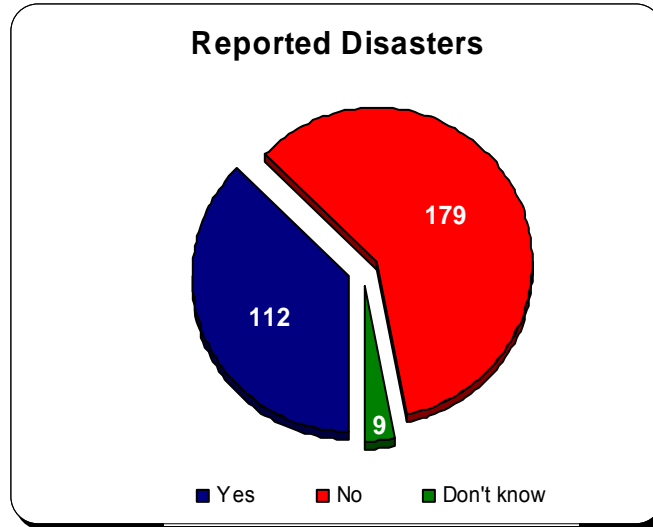


Figure 4: Respondents experiencing virus disaster

Date of last virus disaster?

Respondents were asked the month of their most recent disaster. Table 2 presents these as a frequency distribution. This table is sorted by calendar year beginning with January 2003.

Month of Last Disaster	Response	Percent
January	10	9%
February	13	12%
March	18	16%
April	7	6%
May	31	28%
August	12	11%
September	4	4%
October	11	10%
November	4	4%
December	2	2%

Table 2: Date of most recent disaster

Interestingly, almost three-fourths (71 percent) of the disaster incidents were reported to have taken place in the first half of 2004 and more than a third (37 percent) in the first quarter (Jan-Mar). Those reported in the first quarter were likely due to the *virus war* carried out by the writers of the Netsky, Bagle, and MyDoom viruses and variants. We will touch more on that in our discussion section at the end of the report. Those reported in May were likely due to the Sasser variant release in May that exploited the LSASS service in Windows XP and 2000.

ICSA Labs Virus Prevalence Survey 2004

WHICH VIRUS CAUSED THE MOST RECENT DISASTER?

We asked the survey participants to identify the viruses responsible for their latest disaster. Table 3 lists these viruses, the frequency of response, and the total number of machines affected in the disaster.

Virus Name	Frequency	Machines Involved
W32/Netsky	19	131,719
W32/Slammer	13	78,231
W32/MyDoom	11	76,491
W32/Sober	11	45,967
W32/Mimail	9	18,360
W32/Sobig	9	17,310
W32/Swen	8	3,198
W32/Zafi-B	7	1,153
W32/Bagle	6	3,185
W32/Dumaru	6	2,500
W32/Lovgate	5	7,800
W32/Gibe	4	1,130
W32/SirCam	2	1,190
W32/Klez	2	1,397

Table 3: Virus causing most recent disaster

HOW MANY MACHINES WERE INFECTED IN DISASTERS?

Based on the data above, Figure 5 gives a graphical picture of the number of machines reportedly involved in the latest disasters. The total number of machines reported to be involved in disasters was 389,631.

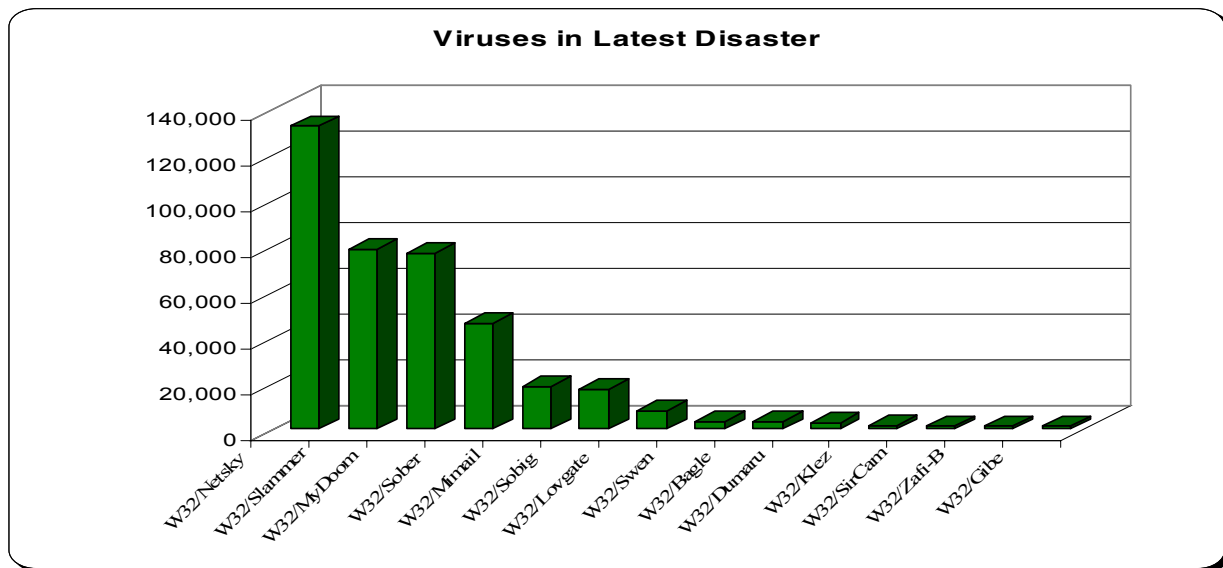


Figure 5: Viruses causing most recent disaster

ICSA Labs Virus Prevalence Survey 2004

What are the effects on victims of virus disasters?

HOW LONG WERE SERVERS DOWN?

Figure 6 shows the pattern of responses on the question of how long servers were down after a virus disaster. Ninety-five (95) participants reported disasters that included servers. The average server downtime reported was 23 hours. Eighty percent of responding companies reported downtime of 20 hours or less.

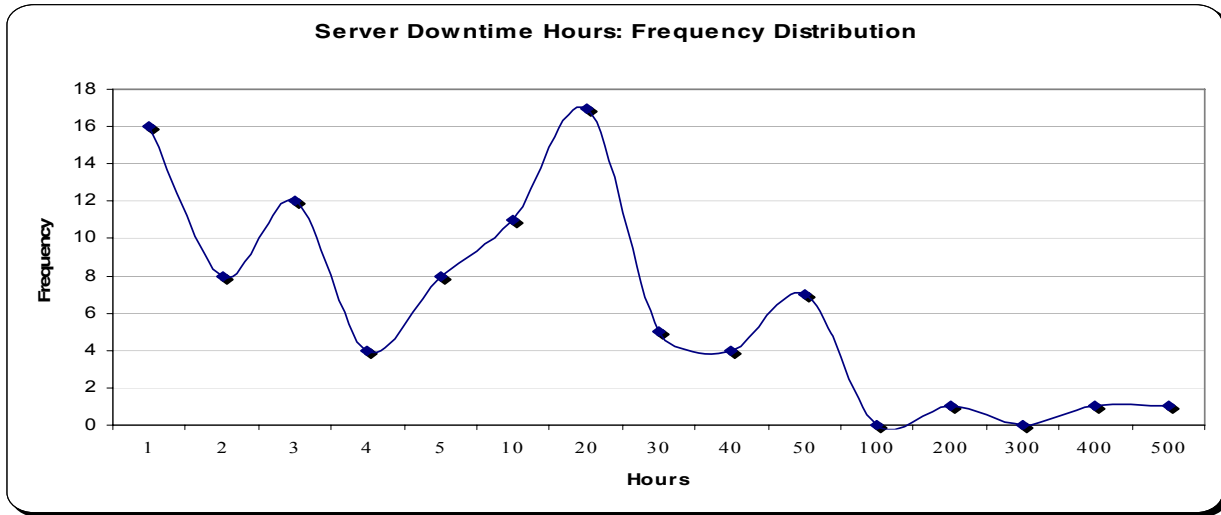


Figure 6: Frequency distribution of server downtime

ICSA Labs Virus Prevalence Survey 2004

WHAT WAS THE COST OF THE DISASTER IN PERSON-DAYS?

Respondents were asked how many cumulative person days were lost during the disaster that affected their company. Figure 7 is a frequency distribution chart of those responses. Of those reporting disasters, 99 participants (96 percent) were able to respond to the question. Of those responding, half of the respondents reported ten person days or less. Last year, there are two higher spikes at the ten day and twenty day points. The difference this year is the twenty day spike is higher, and the ten day spike is somewhat lower. The average time for full recovery was 31 person days.

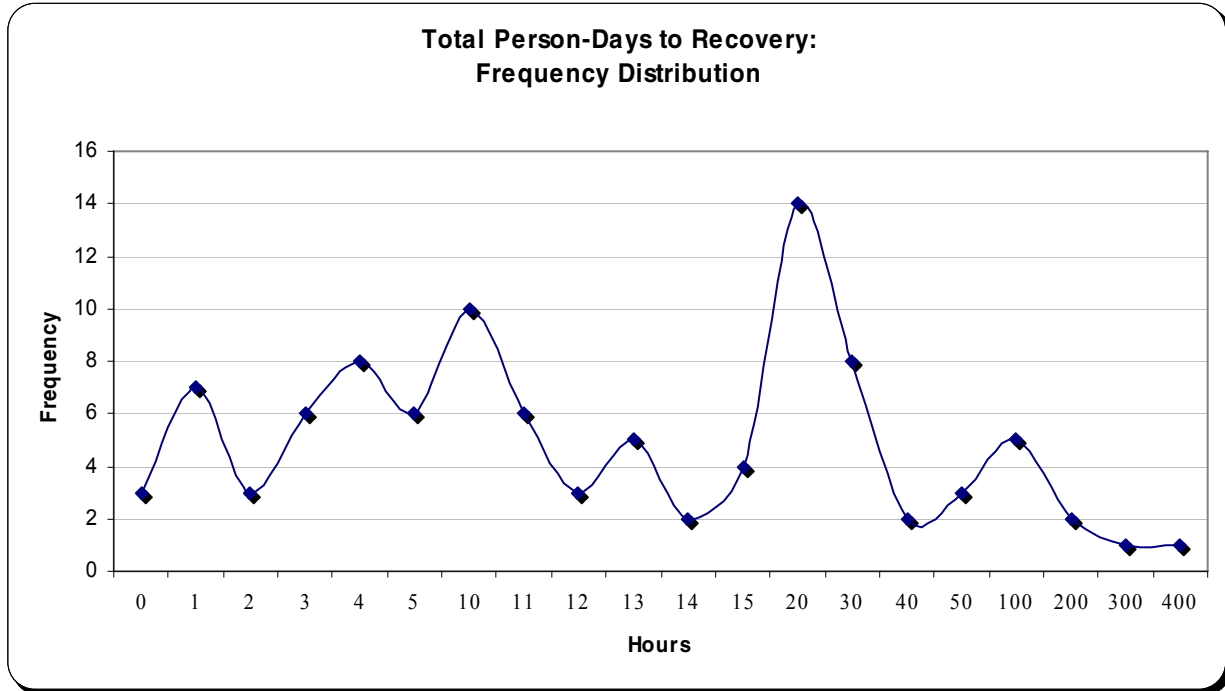


Figure 7: Loss in person-days due to disaster

WHAT WAS THE COST IN DOLLARS TO YOUR COMPANY?

We also asked respondents to estimate the cost in dollars for their latest disaster. These estimates should include ALL costs, including employee downtime, overtime to recover, lost opportunity, etc. Table 4 shows these responses in a Cost Frequency Distribution table.

ICSA Labs Virus Prevalence Survey 2004

Cost	Frequency	Percent
\$2,500	1	1%
\$3,000	3	3%
\$5,000	5	5%
\$10,000	11	12%
\$20,000	9	10%
\$30,000	12	13%
\$40,000	13	14%
\$50,000	10	11%
\$100,000	8	9%
\$200,000	7	8%
\$300,000	3	3%
\$400,000	2	2%
\$500,000	2	2%
\$1,000,000	4	4%
>\$1,000,000	3	3%

Table 4: Frequency distribution of dollar costs

The average dollar costs rose sharply for the second straight year to more than \$130,000 (up from \$99,000). The median cost was more than \$30,000 (up from \$11,000) and the most frequent response was \$40,000 (up from \$10,000). All of these numbers are dramatic increases from the 2003 survey. We continue to see large variances between the average, median, and most frequently stated costs. This is due to several very large reports over \$1,000,000 each. However, it should be noted that the *median* and *most frequently stated* categories are getting closer. This is more easily recognized when depicted in Figure 8.

ICSA Labs Virus Prevalence Survey 2004

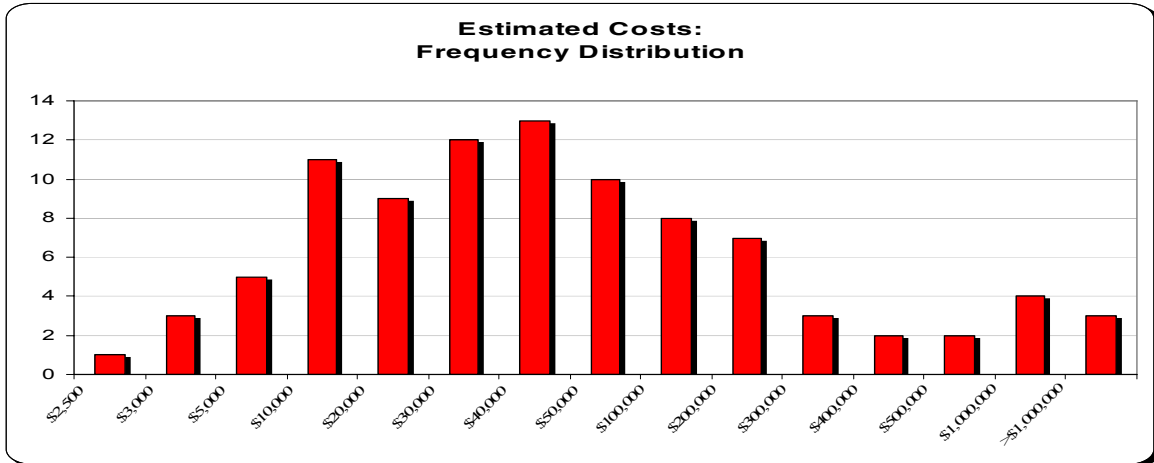


Figure 8: Distribution of dollar costs

Virus Impact

WHAT ARE THE ORGANIZATIONAL EFFECTS OF VIRUSES?

The effects of viruses and virus disasters are more than dollars. We asked the participants what organizational effects the latest disaster or incident had on the company or working group. Figure 9 illustrates their responses. You will note that the numbers sum to greater than 300 as respondents were allowed to choose as many effects as were seen within their various organizations.

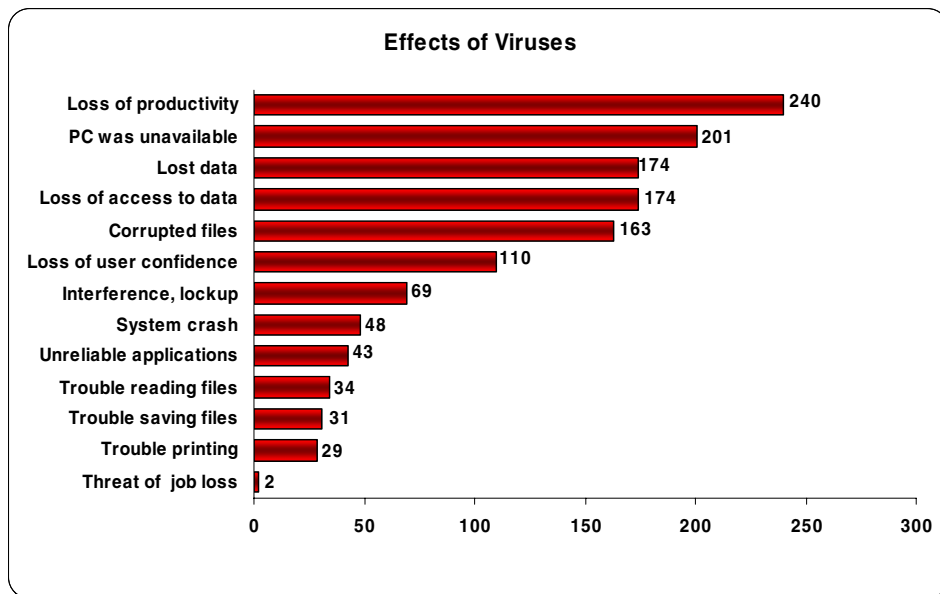


Figure 9: Effects of viruses

ICSA Labs Virus Prevalence Survey 2004

Where Do They Come From?

We asked respondents to identify the means of infection for their most recent virus incident, disaster, or encounter. Again, responses total more than 100 percent because participants were allowed to select more than one means of infection. Table 5 compares responses from the 2004 survey to all previous surveys.

Virus Source	1996	1997	1998	1999	2000	2001	2002	2003	2004
Email Attachment	9%	26%	32%	56%	87%	83%	86%	88%	92%
Internet Downloads	10%	16%	9%	11%	1%	13%	11%	16%	8%
Web Browsing	0%	5%	2%	3%	0%	7%	4%	4%	2%
Other Vector	0%	5%	1%	1%	1%	2%	3%	11%	12%
Software Distribution	0%	3%	3%	0%	1%	2%	0%	0%	0%
Diskette	71%	84%	64%	27%	7%	1%	0%	0%	0%

Table 5: Sources of infection, 1996-2004

Respondents reported that the email vector continues to be the primary point of virus encounter. In addition, for the first time since doing this survey, there were NO instances of boot sector viruses reported. Figure 10 below gives a more meaningful picture of the points of virus encounter.

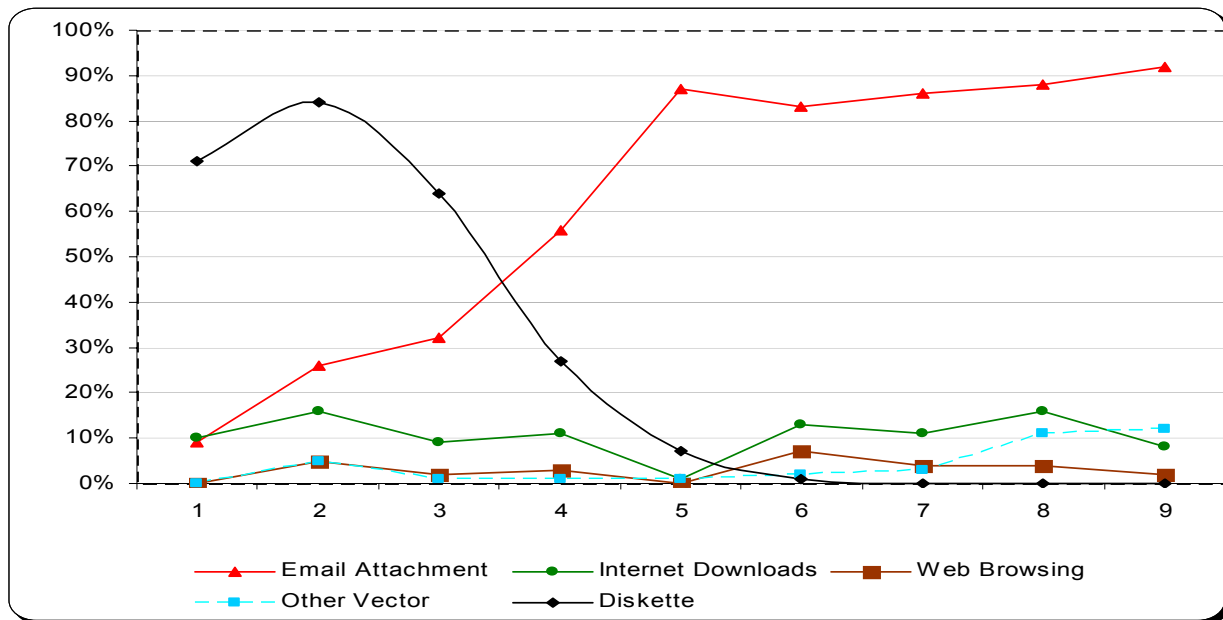


Figure 10: Virus encounter vectors

ICSA Labs Virus Prevalence Survey 2004

Usage of Anti-Virus Products

OVERALL LEVEL OF USAGE

We asked participants, “How many desktops have no anti-virus protection?” This year, 99 percent of the 300 qualified respondents reported that at least 90 percent of all desktop computers are protected with anti-virus software; 84 percent claimed 100 percent protection. Table 6 gives a frequency distribution sorted by frequency of response.

Distribution	Frequency	Percentage
0%	251	84%
10%	45	15%
20%	2	1%
30%	2	1%
40%	0	0%
50%	0	0%
60%	0	0%
70%	0	0%
80%	0	0%
90%	0	0%
100%	0	0%

Table 6: Anti-virus software usage

Figure 11 displays data of the percentage of desktops covered by anti-virus products.

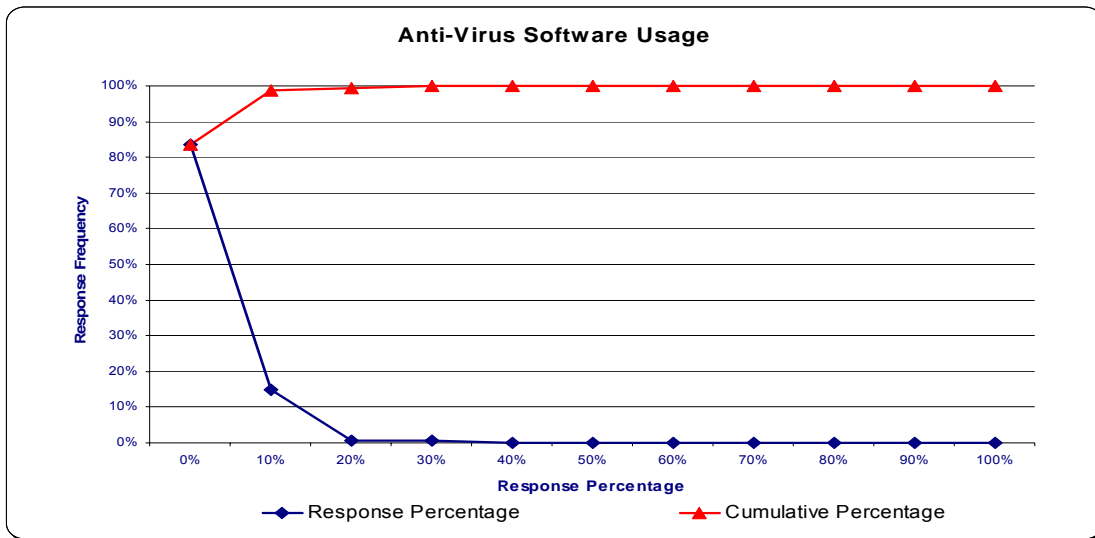


Figure 11: Desktop anti-virus usage

ICSA Labs Virus Prevalence Survey 2004

ANTI-VIRUS PRODUCTS EMPLOYED ON DESKTOPS

Table 7 is the list of anti-virus product developers and the reported usage of each company's products. The table is sorted by frequency of response and provides both frequency of response and number of desktops represented by those responses. Note: both categories will sum to more than 100 percent as organizations may use more than one developer's product.

Product	Response Frequency	Frequency Percent	Desktop Response	Desktop Percent
Symantec Corp	132	44%	355,611	39%
McAfee, Inc.	129	43%	355,520	40%
Trend Micro	61	20%	89,437	12%
Computer Assoc.	48	16%	47,691	7%
Sophos, Inc.	18	6%	9,103	1%
Command Software	9	3%	7,708	1%

Table 7: Desktop anti-virus products in use

The survey's participants report that McAfee and Symantec maintain their market share dominance. However, Trend Micro's percentage in both frequency of response and desktop percentage has risen in each of the past two surveys. Figure 12 shows the graphical results of the survey taking into consideration only whether a respondent reported using one or more specific anti-virus products on the organization's desktops.

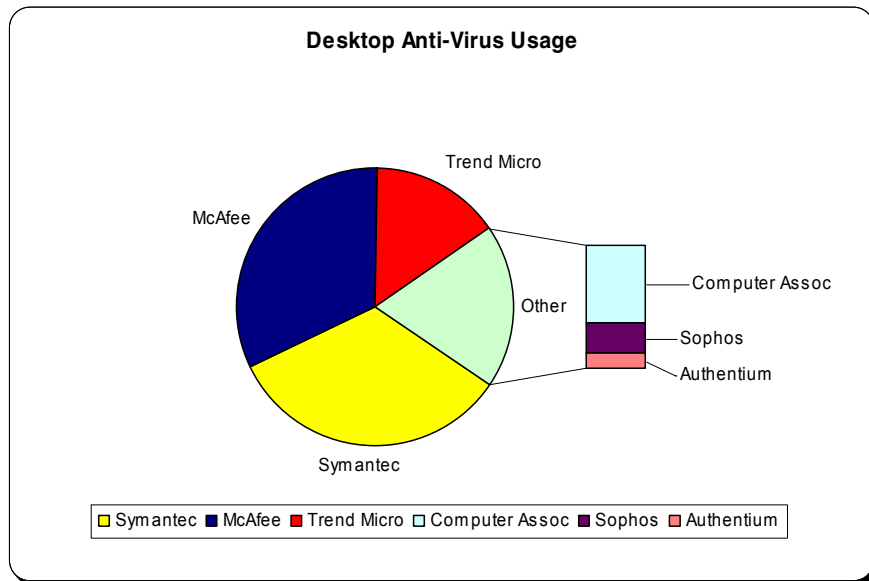


Figure 12: Desktop coverage by frequency of response

ICSA Labs Virus Prevalence Survey 2004

We also asked respondents what mechanisms were in use on their anti-virus-protected PCs. These responses are listed in Table 8.

Method	Frequency
Users check diskettes and files for viruses	61
Anti-virus software scans hard drive for viruses every boot-up	280
Anti-virus software scans hard drive for viruses every login	215
Anti-virus software scans full time in the background	294
Other periodic anti-virus detection on the desktop	180
Other full-time anti-virus detection on the desktop	20

Table 8: Respondents using specific anti-virus methods

In this year's survey almost all (98 percent) survey participants claim to be using full-time background anti-virus protection. This is a significant increase over the reported 89 percent in the 2003 survey. Additionally, survey responses indicate that 72 percent of companies configure their anti-virus protection to scan desktops on boot-up. Figure 13 shows this data as a graph.

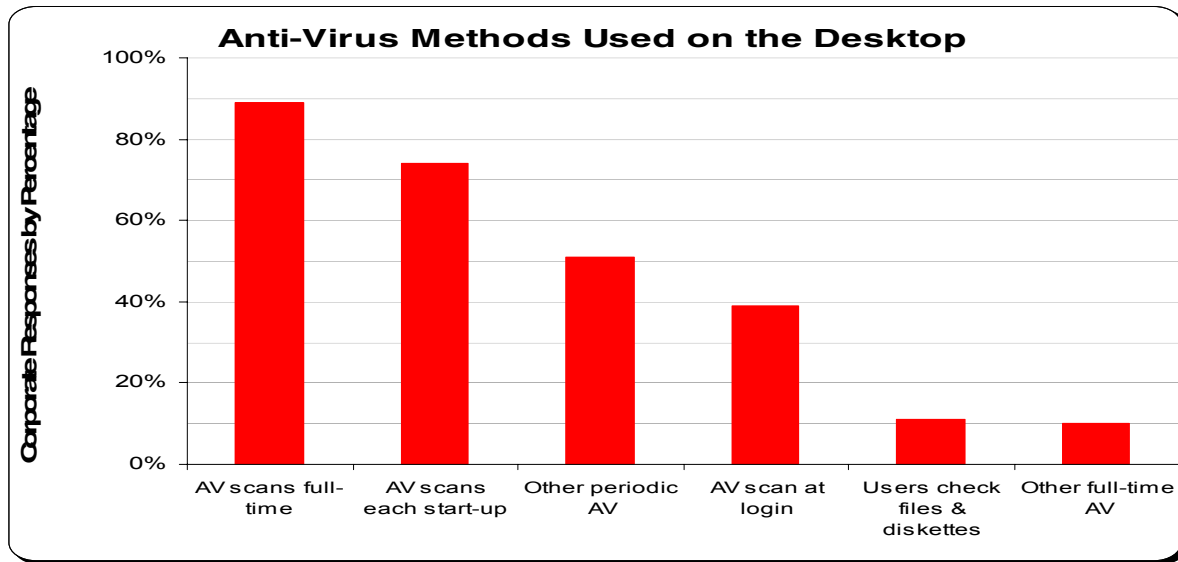


Figure 13: Anti-virus methods used

ICSA Labs Virus Prevalence Survey 2004

SERVER ANTI-VIRUS METHODS

Survey participants were also asked what anti-virus methods they used on file and application servers. Figure 14 shows the response for both the percentage of responding companies and the percentage of servers using particular methods. Again, a clear majority (97 percent) depend on full time background virus protection.

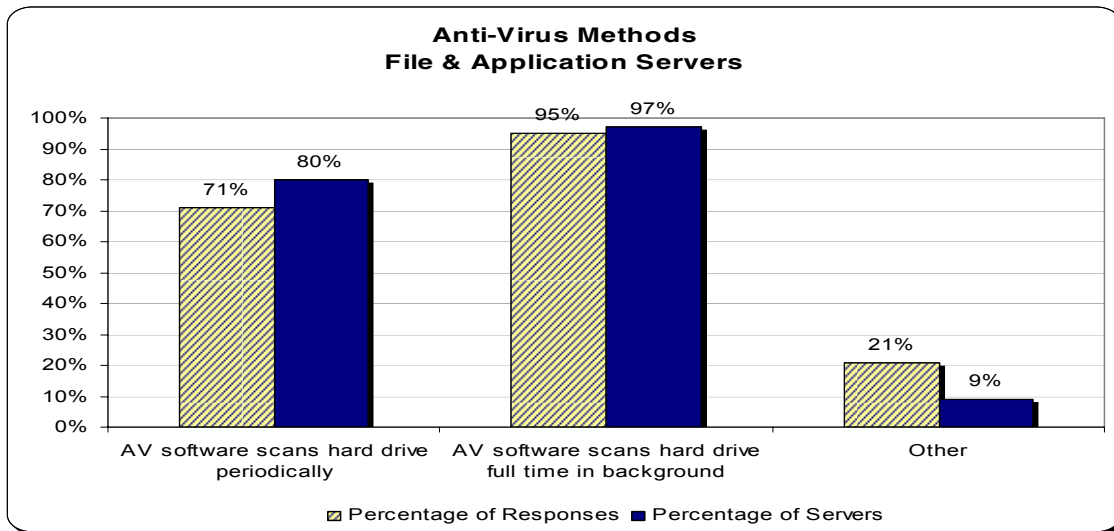


Figure 14: Anti-virus methods used on file servers

ANTI-VIRUS USAGE ON PERIMETER SERVICES

We asked respondents what percentage of their email servers, proxy servers, and firewalls were covered by anti-virus methods. Table 9 shows the results of their responses.

Coverage %	Email	Proxy	Firewalls
100%	291	184	149
90%	6	14	24
80%	1	2	0
70%	0	0	1
60%	1	0	0
50%	0	1	1
40%	0	0	0
30%	0	0	1
20%	0	0	1
10%	0	0	0
0%	1	99	123

Table 9: Perimeter coverage by frequency distributions

Figure 15 charts the growth of reported perimeter protection since the 1997 survey. ICSA Labs began recommending full anti-virus coverage on perimeter gateways after the 1997 survey.

ICSA Labs Virus Prevalence Survey 2004

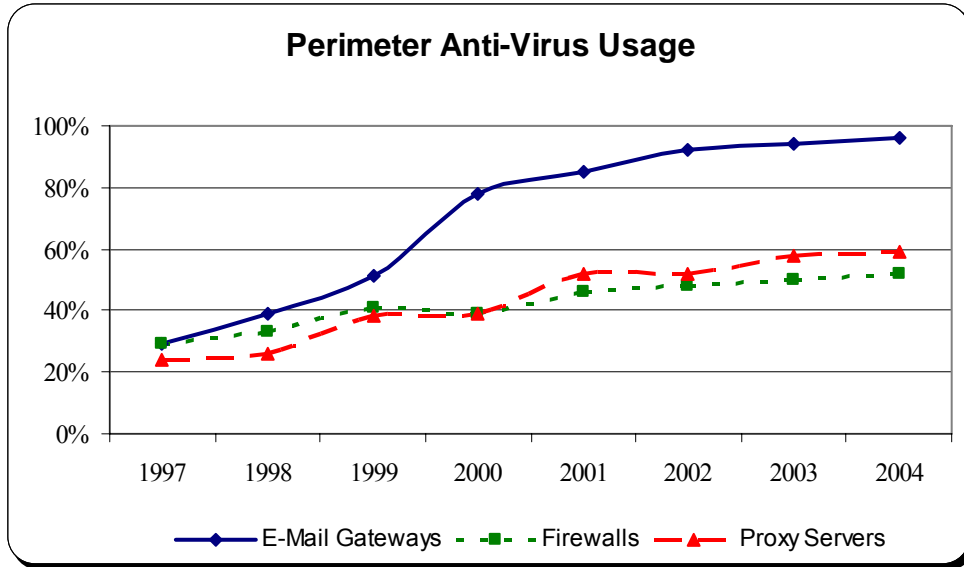


Figure 15: Comparison of perimeter anti-virus coverage, 1997-2004

The 2004 survey again shows an increase in perimeter anti-virus coverage across the board. Email gateways increased from 94 percent to 96 percent. Firewalls and proxy servers showed a similar slight increase, yet remain at lower levels of approximately 50 percent and 60 percent respectively. Perimeter protection is not a replacement for desktop and server protection. However, perimeter protection provides a critical layer of protection and is a necessary component for a complete corporate virus protection strategy.

PERIMETER ANTI-VIRUS METHODS

We also asked respondents about the anti-virus methods used at their Internet perimeter. The following tables and charts represent their answers. Table 10 lists the responses by frequency for email gateways.

ICSA Labs Virus Prevalence Survey 2004

Method	Frequency
Anti-virus software scans all messages in real time?	296
Block, filter, or quarantine email attachments by file type?	280
Anti-Virus software scans message folders and databases?	208
Other anti-virus software protection methods used?	9
Total respondents	300

Table 10: Anti-virus methods in use on email gateways

Table 11 lists the responses for anti-virus methods used on proxy servers by frequency of response. Note, only 209 of the participants responded to this question.

Method	Frequency
AV scans all traffic in real time	149
Block, filter, or quarantine files by file type	130
Other Methods	11
Total respondents used	209

Table 11: Anti-virus methods used on proxy servers

Table 12 lists the anti-virus methods used on firewalls by frequency of response. Note, only 209 of the participants responded to this question.

Method	Frequency
Block, filter, or quarantine files by file type	178
Anti-virus software scans all traffic in real time	108
Other anti-virus protection methods	10
Total respondents used	182

Table 12: Anti-virus methods used at the firewall

ICSA Labs Virus Prevalence Survey 2004

Figure 16 consolidates the perimeter protection methods listed above by percentage of response. While proxy and firewall coverage is still lagging a bit, it is good to see that when anti-virus products are used, high percentages are scanning traffic in real time. It is also nice to see the percentage of companies that block, filter, and/or quarantine files and messages at the perimeter are increasing as well.

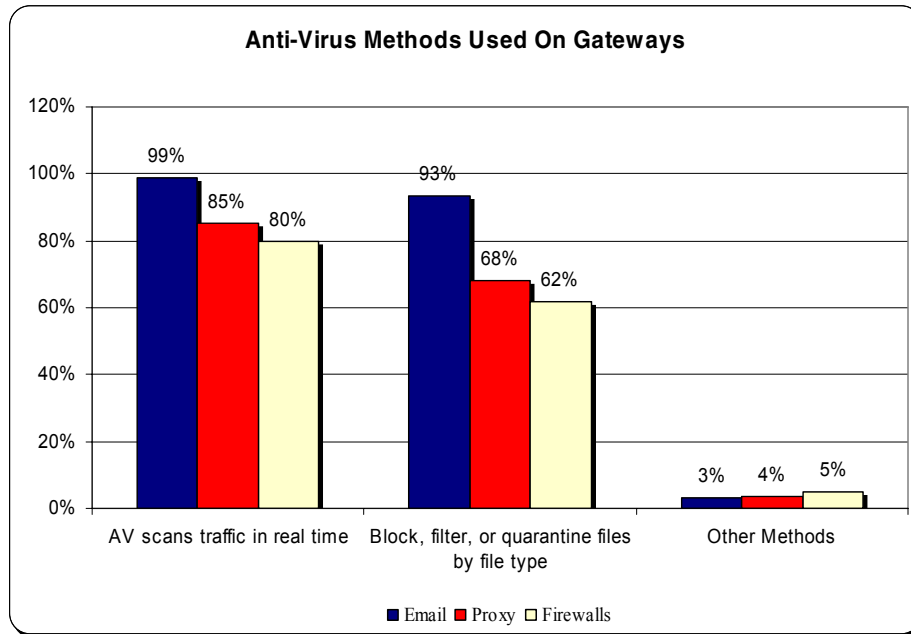


Figure 16: Anti-virus methods used on gateways by percentage

ICSA Labs Virus Prevalence Survey 2004

Discussion Section

THE VIRUS PROBLEM CONTINUES TO WORSEN

Just as 2003 began with a rush, so did 2004. While 2003 began with the Slammer worm, 2004 began with a *virus war*. Beginning in January and running through May, the creators of three different viruses seemed to be in a surreal race. The creators of MyDoom, Bagle, and Netsky each released new variants at record pace. All three worms and variants propagated as attachments. MyDoom and Bagle installed their own SMTP engines for propagation, backdoors, and remote access capabilities, and were no doubt used for spamming. Netsky on the other hand installed its own SMTP engine to construct emails and propagate, but also attempted to remove registry keys to deactivate other malware, specifically MyDoom and Bagle. It was an interesting year.

For the ninth consecutive year, we have seen increases in virus infections, virus disasters, and recovery costs. While virus infection rates were higher this year than the previous two years, it was still somewhat flat. From 1996 through 1999, the virus infection rate approximately doubled. There was a significant spike in the 1999 survey due to the March 1999 Melissa outbreak. After the Melissa incident spike, infection rates slowed to approximately 15 percent per year until 2001. During the period of 2001 – 2003, we saw a minimal increase of only five infections per 1,000 PCs per month. 2004, however, saw a relatively significant increase of ten infections per 1000 PCs per month, or a 12 percent increase over 2003.

In tandem with the increase in infections per month, we saw another significant increase in total virus *encounters*⁵. The survey differentiates between virus *infections*⁶ and virus *encounters*. Reports of encounters more than doubled in 2003 from 1.2 million and in 2002, to 2.7 million encounters reported 2003. While 2004 did not see another doubling, there was greater than a 40 percent increase over 2003 to 3.9 million encounters.

The reported disasters again increased. After the very small drop in 2002, we have seen our second consecutive increase, this one rather significant – almost 20 percent over 2003. Respondents reported an increase from 80 reported disasters in 2002 to 94 reports in 2003, and 112 in 2004. While disappointing to see the significant increases, it was anticipated. ICSA Labs forecasted that both infection and disaster rates would continue to grow due to new mass mailers and internet worms, expanded connectivity, greater functionality and increased power and available bandwidth. That prediction has proven to be accurate. This past year saw many new viruses of these types and a multitude of variants.

VIRUS TYPES

2004 was an interesting year for numbers of viruses and outbreak incidents. Several trends need to be addressed. Some we have listed for several years, yet they bear mentioning again.

⁵ The survey defines an encounter as an event or incident where viruses were experienced, detected, or discovered on any PCs, diskettes; or files or filtered, block or stripped from email.

⁶ An infection describes an activation of the virus on the machine, media, or network.

ICSA Labs Virus Prevalence Survey 2004

1. There was a higher rate of infections per month over the entire survey period than in previous years. This year's survey showed a surprisingly high infection ration January-June, which then dropped off a bit the rest of the year.
2. The current mass mailers and viruses seem to be staying longer. The individual variants may be shorter-lived, but the families tend to stay with us longer, due to the volume of variants we see.
3. The trend of forging the From: address in emails distributing the viruses continues to be used in almost all of the most prevalent viruses.
4. The most successful viruses continue to install their own email engines for propagation and are used for spam propagation as well.
5. More evidence that Spammers and virus writers have joined forces or use one another's techniques.
6. Corporations are facing increasing numbers of virus incidents, and must devote more time, personnel, and resources to protecting their systems.
7. Infections and disasters are taking longer to disinfect systems and fully recover, which costs corporations more dollars and resources.
8. Boot Sector and 16-bit legacy viruses were not referenced in this year's survey.

PERCEPTIONS OF THE VIRUS PROBLEM

Survey participants again lowered their perception of the virus problem. Ninety-one percent of those surveyed feel that the overall virus problem is either *Somewhat worse* or *Much worse* than 2003, which was considered a very bad year itself. Only nine percent of respondents felt it was *About the Same*.

VIRUS DISASTERS AND COSTS

The severity of disasters continues to increase. Disasters continue to take longer to recover from and cost corporations more each year. The average time for full recovery in 2003 was 24 person days. This was only a very slight increase over 2002. However, 2004 saw an increase of 7 person days or 30 percent increase for full recovery. As time to full recovery is escalating, so is the cost impact over last year. 2003 saw the largest single increase since we have been gathering this data. The 2004 survey eclipsed that. The average reported cost for a disaster this year was reported to be \$130,000 versus the \$99,900 reported for 2003, representing an increase of more than 40 percent!

Those numbers can be daunting themselves, however, when one considers that respondents in our survey historically underestimate costs by a factor of 7 to 10, the results can be overwhelming. Based on the dollars reported by the technical respondents, if costs were to be considered, complete cost of recovery would be in the range from \$900,000 to more than \$5,000,000 (in total costs of recovery alone).

VIRUS DISASTER IMPACT:

For the eighth year in a row, our survey respondents reported that viruses are not only more prevalent in their organizations but are also more destructive, causing more real damage to

ICSA Labs Virus Prevalence Survey 2004

data and systems, and costing more than in past years. All of this, despite increases in their use of anti-virus products, improved updating and upgrading, and better management of anti-virus systems. Corporations are spending more time, energy, and dollars in purchasing, installing, and maintaining anti-virus products without achieving their desired results.

Part of the reason for the increased cost of viruses is the impact they have on the business functions of a company. In years past, viruses were nuisances and caused little real damage. Those days are long past. Today's viruses continue to escalate in all those areas that affect the function of organizations. Loss of productivity is by far the most important consequence of both virus encounters and disasters. At least 50 percent of the respondents list *Loss of productivity, PC unavailable, Corrupted files, and Loss of access to data* as the primary effect that viruses had on their organizations.

The "threatscape" for viruses and worms has shifted toward multifaceted and faster spreading attacks and infection mechanisms. With this shift comes the importance of mitigating the risk of new and previously unknown viruses. Even though the current reactive anti-virus technologies are much faster at providing updates for known viruses, and their heuristics have improved greatly, known virus scanning is only a baseline. Corporations also need to look toward other proactive protection strategies such as better and finer grained heuristics, access controls, behavior blocking, change detection, filtering, and other generic technologies.

PROTECTION STRATEGIES:

Again, our survey reports that anti-virus product usage is up at every level from previous years. Only firewalls and proxy servers show less than a 90 percent usage of anti-virus products. More than 95 percent of users report that desktop, server, and email gateway server usage has at least 90 percent coverage. Yet, with anti-virus product usage up, why do we continue to see the increases in infections, disasters, and costs?

Very simply, we must begin to think differently about virus and malware protection. Anti-virus products are and will remain an important part of the virus protection equation, but they are only a part of the solution. It is no longer enough to think of virus protection in terms of reactive technology. The example given above showing the increasing rapidity of viruses being spread is evidence that the use of anti-virus products, while necessary, is not enough.

Corporations need to adopt more proactive and holistic protection philosophy that includes strong leadership, a comprehensive security policy, and intelligent risk management. ICSA Labs and Cybertrust have recommended email gateway filtering and generic virus controls and procedures since 1997. In the last three years we have seen a significant increase in the use of perimeter anti-virus products. However, corporations are still slow in adopting generic protection schemes. Generic controls exist that can be employed with minimal maintenance and manageable infringement on corporate business practices. For a number of years, Cybertrust has published a list of these generic controls in its anti-virus policy guide.

These controls include such protections as file attachment filtering; specific configuration for various email clients, email servers, web browsers, and business applications such as word processors and spreadsheets; and various other controls that are generally easy to implement, require infrequent updates, and go unnoticed by the average user because of their

ICSA Labs Virus Prevalence Survey 2004

transparency. However, their effectiveness is very good, especially when used in conjunction with and implemented within the corporate security policy. Research done by ICSA Labs and Cybertrust has shown that adopting the controls outlined in a two-year-old version of the aforementioned policy guide would have rendered viruses such as Slammer, Blaster, SoBig, and more recently, MyDoom ineffective⁷. Copies of these studies may be obtained by contacting Cybertrust.

Another aspect of intelligent risk management should require users to subscribe to an “early warning” service that warns system administrators as quickly as possible of the outbreak of new malicious code, vulnerabilities in operating systems and networks, and code that exploits these vulnerabilities. However, not all early warning systems are created equal. Ideally, the early warning service will not only advise of the threat or vulnerability, but will give some rating on severity and what actions to take in the short, mid and long term. In conjunction with such a service, it is imperative that organizations update their perimeter virus defenses within minutes of receiving such an alert.

⁷ A copy can be obtained from the Cybertrust website <http://www.cybertrust.com/>

ICSA Labs Virus Prevalence Survey 2004

In summary, ICSA Labs recommends the adoption of an intelligent risk management solution to the virus problem.

1. Develop a comprehensive security policy
 - a. Publish the policy
 - b. Update it regularly
 - c. Enforce the policy
2. Adopt a defense in depth
 - a. Install anti-virus software at all levels: desktop, servers, gateways, and the perimeter.
 - b. Employ generic virus protections where possible: filtering, blocking, AND stripping attachments.
 - c. Employ complimentary security programs such as desktop firewalls, host and network based intrusion detection, and prevention.
 - d. Consider managed security services for email and anti-virus.
3. Subscribe to an alert service
 - a. Commercial
 - b. Online lists: NTBugtraq, Bugtraq, AVIEN to name a few

ICSA Labs Virus Prevalence Survey 2004

Appendix A: Survey Questionnaire

- Q1 How many computers (workstations, desktops, or laptops) are you responsible for in terms of virus knowledge, prevention, and software?
- Q1a Please indicate which Desktop Operating Systems your organization uses. Also, please indicate how many PCs in your organization use each Operating System
- Q2 How many file and application servers are you responsible for in terms of virus knowledge, prevention, and software?
- Q2a Please indicate which Network Operating Systems your organization uses. Also, please indicate how many servers run each system.
- Q3 What percent of virus incidents in your group are you informed of or likely to know of?
- Q4a Please indicate which anti-virus products you are running at the desktop PC level. Also, please indicate how many desktop PCs are running each product.
- Q4b Please indicate which anti-virus products you are running at the server level. Also, please indicate how many servers are running each product.
- Q5a Please indicate which of the following anti-virus software protection methods are used on the desktop level. Also, please indicate how many desktops use each method.
- Q5b What percentage of desktops have NO anti-virus software installed?
- Q5c What percentage of desktop have anti-virus software installed, but not running?
- Q5d Please indicate which of the following anti-virus software protection methods are used on the file server level. Also, please indicate how many servers use each method.
- Q6a What percentage of email gateways have full-time anti-virus software installed?
- Q6b What anti-virus products do you have installed for the email gateway?
- Q6c Please indicate which of the following antivirus software protection methods are used on the email gateway. Also, please indicate how many servers use each method.
- Q7a What percentage of proxy servers have full-time anti-virus software installed now?
- Q7b What anti-virus products do you have installed for the proxy gateway?
- Q7c Please indicate which of the following anti-virus software protection methods are used on the proxy server level. Also, please indicate how many servers use each method.
- Q8a What percentage of firewalls have anti-virus software installed now?
- Q8b What anti-virus products do you have installed on the firewall?
- Q8c Please indicate which of the following anti-virus software protection methods are used on the firewall level by clicking on the appropriate box. Also, please indicate how many servers use each method by typing a number in the box.
- Q9 To the best of your knowledge, has a computer virus ever been discovered in any PC, diskette or file in your organization?
- Q10a-b How many virus encounters did you have during:
a. December 2004

ICSA Labs Virus Prevalence Survey 2004

- b. November 2004
 - c. October 2003
 - d. July-September of 2004
 - e. January-June of 2004
- Q11a-h Which viruses have affected your groups's PC during:
- a. December 2004
 - b. November 2004
 - c. October 2003
 - d. July-September of 2004
 - e. January-June of 2004
- How many times?
- Q12 Has your group had a virus disaster anytime since January 2004?
- Q12a When was the month and year of your most recent disaster?
- Q12b What was the name of the virus in your most recent disaster?
- Q12c1 How many Desktops were initially suspected of having the virus?
- Q12c2 How many Desktops actually were found to be infected?
- Q12d1 How many File/Print SERVERS were initially suspected of having the virus?
- Q12d2 How many File/Print SERVVERS actually were found to be infected?
- Q12e How long were any servers "down" while dealing with the disaster? (total server hours)
- Q12f How long did it take for your group to completely recover? (total person hours)
- Q12g How many person days did the disaster cost your group? (total person hours)
- Q12h How many dollars did the disaster cost your group? (as much as possible include all costs - employee downtime, lost opportunity, IT costs)
- Q13 Which of the following effects occurred in your group with the most recent virus disaster or encounter? (Check all that apply)
- a. Loss of user confidence in the system
 - b. Threat of someone losing their job
 - c. Loss of productivity (machine, applications or data not available for some time)
 - d. Screen message, interference, or lockup
 - e. Lost data
 - f. Corrupted files
 - g. Loss of access to data (i.e. on Server, Host, Mainframe, etc)
 - h. Unreliable applications
 - i. PC was unavailable to the user
 - j. System Crash
 - k. Trouble saving files
 - l. Trouble reading files
 - m. Trouble printing
 - n. None
 - o. Don't know
 - p. Other
- Q14 How did your most recent virus disaster or encounter come to your site?
- Q16 What department are you in?

ICSA Labs Virus Prevalence Survey 2004

- Q17 What is your job title?
- Q18 What is your organization's primary line of business?
- Q19 Compared to this time last year, do you feel virus problems in the computing industry are
- a. Much worse
 - b. Somewhat worse
 - c. About the same
 - d. Somewhat better
 - e. Much better
 - f. No Opinion

ICSA Labs Virus Prevalence Survey 2004

Appendix B: Possible Biases

As with all surveys, there are potential biases that may affect the results of this report. We have taken all possible steps to reduce the effects of these.

RETROSPECTIVE STUDY

The most important bias is that this study is retrospective. That is, we asked respondents to answer questions about past events. Though most sites claimed to have formal tracking mechanisms in place, we believe that respondents describe the older events less reliably than they do when providing information about more recent events. Moreover, older events are often under-represented (forgotten) compared to more-recent events.

Finally, it may also be true that unpleasant events are less easily remembered than pleasant events, so that the past seems more positive than it actually was.

This bias might enhance the perception that things are getting worse.

CORRECTNESS

Some questions referred to issues with well-known right answers, such as questions about policy and virus protection. Other questions asked respondents about the correctness of their estimates (e.g. comparisons of actual virus infections to initial estimates).

In such cases, it is possible that respondents consciously or unconsciously adjusted their responses to look good to the interviewer or to reduce discrepancies between their actual behavior and the normative behavior they felt they ought to display.

This bias could overestimate correctness in such questions.

SITE SELECTION

The survey can be biased in favor of companies that have “computer virus experts” due to the initial site screening. Consequently, it might be true that sites that do not have such a person were under-represented in the survey.

It may also be true that these sites did not have such a person because the virus problem was minimal there.

This bias could show the problem as worse than it really is. Unfortunately, it could also be true that under-represented sites were worse off than the sites in the sample.

FAMILIARITY

The survey tried to estimate the chance that the respondent would actually know about every virus encounter at their site. Respondents were asked the question, “What percent of virus incidents in your group are you informed of or likely to know about?”

However, based solely on anecdotal experience of what happens to anti-virus reporting in organizations, we surmise that a remote employee who encountered a virus for which the appropriate actions were already well known (because of past experience) would be less likely to report the incident to the respondent.

Therefore, we think that common viruses may be under-reported compared with newer or less familiar viruses, or those that have recently hit the headlines at the time of questioning.

ICSA Labs Virus Prevalence Survey 2004

Appendix C: Glossary of Common Terms in Anti-virus Discussion

The following are common terms used in discussions of anti-virus software:

- Background Scanning:** Automatic scanning of files as they are created, opened, closed, or executed. Performed by memory resident anti-virus software. Synonyms: online, automatic, background, resident, active.
- Behavior Blocking:** A set of procedures that are tuned to detect virus-like behavior, and prevent that behavior (and/or warn the user about it) when it occurs. Some behaviors that should normally be blocked in a machine include formatting tracks, writing to the master boot record or boot record, and writing directly to sectors. Synonyms: “dynamic code analysis”, “behavioral analysis.”
- Boot Record:** The program recorded in the Boot Sector. All floppies have a boot record, whether or not the disk is actually bootable. Whenever you start or reset your computer with a disk in the A: drive, DOS reads the boot record from that diskette. If a boot virus has infected the floppy, the computer first reads the virus code in (because the boot virus placed its code in the boot sector), then jumps to whatever sector the virus tells the drive to read, where the virus has stored the original boot record.
- Boot Sector:** The first logical sector of a drive. On a floppy disk, this is located on side 0 (the top), cylinder 0 (the outside), sector 1 (the first sector.) On a hard disk, it is the first sector of a logical drive, such as C or D drive(s). This sector contains the Boot Record, which is created by FORMAT (with or without the /S switch.) The sector can also be created by the DOS SYS command. Any drive that has been formatted contains a boot sector.
- Boot Sector Infector:** Every logical drive, both hard disk and floppy, contains a boot sector. This is true even of disks that are not bootable. This boot sector contains specific information relating to the formatting of the disk, the data stored there and contains a small program called the boot program (which loads the DOS system files). The boot program displays the familiar “Non-system Disk or Disk Error” message if the DOS system files are not present. In addition, the program is infected by viruses. You get a boot sector virus by leaving an infected diskette in a drive and rebooting the machine. When the program in the boot sector is read and executed, the virus goes into memory and infects your hard drive. Remember, because every disk has a boot sector, it is possible (and common) to infect a machine from a data disk.
- Boot Virus:** A virus whose code is called during the phase of booting the computer in which the master boot sector and boot sector code is read and executed. Such viruses either place their starting code or a jump to their code in the boot sector of floppies, and either the boot sector or master boot sector of hard disks. Most boot viruses infect by moving the original code of the master boot sector or boot sector to another location, such as slack space, and then placing their own code in the master boot sector or boot sector. Boot viruses, which also infect files, are sometimes known as multipartite viruses. All boot viruses infect the boot sector of floppy disks; some of them, such as Form, also infect the boot sector of hard disks. Other boot viruses infect the master boot sector of hard disks.
- Companion Virus:** A program that attaches to the operating system, rather than files or sectors. In DOS, when you run a file named “ABC”, the rule is that ABC.COM would execute before ABC.EXE. A companion virus places its code in a COM file whose first name matches the name of an existing EXE. You run “ABC”, and the actual sequence is “ABC.COM”, “ABC.EXE”
- File Virus:** Viruses that attach themselves to (or replace) .COM and .EXE files, although in some cases they can infect files with extensions .SYS, .DRV, .BIN, .OVL, OVR, etc. The most common file viruses are resident viruses, going into memory at the time the first copy is run, and taking clandestine control of the computer. Such viruses commonly infect additional programs as you run them. However, there are many non-resident viruses too, which simply infect one or more files whenever an infected file is run.
- In the Wild Virus:** A term that indicates that a virus has been found in several organizations somewhere in the world. It contrasts the virus with one that has only been reported by researchers. Despite popular hype, most viruses are “in the wild” and differ only in prevalence. Some are new and therefore extremely rare. Others are old, but do not spread well, and are therefore extremely rare. Joe Wells maintains a list of those he knows of to be “in the wild.”

ICSA Labs Virus Prevalence Survey 2004

Macro Virus:	A virus which consists of instructions in Word Basic, Visual Basic for Applications (VBA), or some other macro language, and resides in documents. While we do not think of documents as capable of being infected, any application that supports automatically-executing macros is a potential platform for macro viruses. Because documents are now more widely shared than diskettes (through networks and the Internet), document-based viruses are likely to dominate our future.
Master Boot Record:	The 340-byte program located in the Master Boot Sector. This program begins the boot process. It reads the partition table, determines what partition will be booted from (normally C:), and transfers control to the program stored in the first sector of that partition, which is the Boot Sector. The Master Boot Record is often called the MBR, and often called the "master boot sector" or "partition table." The master boot record is created when FDISK or FDISK /MBR is run.
Master Boot Sector:	The first sector of the hard disk to be read. This sector is located on the top side ("side 0"), outside cylinder ("cylinder 0"), first sector ("sector 1.") The sector contains the Master Boot Record.
Master Boot Sector Virus:	A virus that infects the master boot sector, such as NYB, spreads through the boot sector of floppy disks. If you boot or attempt to boot your system with an infected floppy disk, NYB loads into memory and then writes itself to the master boot sector on the hard drive. If the disk is not bootable, you see the DOS error message, "Non-system disk or disk error...". If the disk is bootable, the system boots to the A: prompt. Either way the system is infected, and there is no indication on the screen that this has happened. Once the hard drive is infected, NYB loads into memory each time the system is booted. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy DOS accesses.
On-Demand Scanning:	Synonyms: offline, manual scanning, foreground, non-resident scanning, scanning.
Polymorphic Virus:	A polymorphic virus is one that produces varied, yet fully operational, copies of itself in the hope that virus scanners will not be able to detect all instances of the virus.
Remove:	To remove or clean a virus means to eliminate all traces of it, returning the infected item to its original, uninfected state. Nearly all viruses are theoretically removable by reversing the process by which they infected. However, any virus that damages the item it has infected by destroying one or more bytes is not removable, and the item needs to be deleted and restored from backups in order for the system to be restored to its original, uninfected state. There is a gap between theory and practice. In practice, a removable virus is one that the anti-virus product knows how to remove. The term "clean" is sometimes used for remove, and sometimes used to refer to the destruction of viruses by any method. Thus deleting a file that is infected might be considered cleaning the system. We do not regard this as an appropriate use of the term "clean."
Resident:	A property of most common computer viruses and all background scanners and behavior blockers. A resident virus is one that loads into memory, hooks one or more interrupts, and remains inactive in memory until some trigger event. When the trigger event occurs, the virus becomes active, either infecting something or causing some other consequence (such as displaying something on the screen.) All boot viruses are resident viruses, as are the most common file viruses. Macro viruses are non-resident viruses.
Stealth Virus:	A virus that uses any of a variety of techniques to make itself more difficult to detect. A stealth boot virus will typically intercept attempts to view the sector in which it resides, and instead show the viewing program a copy of the sector as it looked prior to infection. An active stealth file virus will typically not reveal any size increase in infected files when you issue the "DIR" command. Stealth viruses must be "active" or running in order to exhibit their stealth qualities.
Trojan Horse:	A program that does something unwanted and unexpected by a user, but intended by the programmer. Trojans do not make copies of themselves, as do viruses, and seem to be more likely to cause damage than viruses.
Worm:	Similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all. Once a worm is executed, it seeks other systems to infect, then copies its code to them.
Zoo Virus:	A virus which is rarely reported anywhere in the world, but which exists in the collections of researchers.

ICSA Labs is the security industry's central authority for research, intelligence and product certification for over a decade. ICSA Labs sets performance standards for information security products and certifies over 95% of the installed base of firewall, anti-virus, cryptography and IPSec products. ICSA Labs also leads security consortia that provide a forum for intelligence sharing among the leading vendors of security products.



ICSA Labs

1000 Bent Creek Blvd., Suite 200
Mechanicsburg, Pennsylvania 17050
717-790-8100 www.icsalabs.com

