

# **The Real Cost of A Virus Outbreak**

## **Why is antivirus needed?**

A computer virus is a piece of executable code with the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files are copied and sent from individual to individual.

Some computer viruses have a damage routine that can deliver a payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other kinds of damage. If the virus doesn't contain a damage routine, it can still cause trouble by taking up storage space and memory, and downgrading the overall performance of your computer or system network

Several years ago most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email now used as an important business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in productivity loss and clean-up expenses. Antivirus has become a necessity in the changing communication environment.

The Computer Security Institute conducted a survey of 538 computer security practitioners in corporations, government agencies, financial institutions, medical institutions, and universities in the United States. Their results revealed that 85 percent of respondents had detected computer security breaches within a twelve month period. The 35 percent who listed a financial impact, reported \$ 377,828,700 in financial losses. Of these, many cited their Internet connection as the point of attack for hackers.

## **JUST HOW REAL IS THE CYBER-THREAT OF DESTRUCTIVE COMPUTER VIRUSES?**

Viruses won't go away any time soon. More than ten thousand have been identified and 500 new ones are created every month, according to the International Computer Security Association (ICSA). With numbers like those, it's safe to say that most organizations deal regularly with virus outbreaks. No one who uses computers is immune from viruses. With the growth of the Internet and email as the main communication tools, viruses and malicious code are undoubtedly a major concern for many businesses. A single email attachment or execution of a virus from the Internet or email can lead to widespread infection in a matter of hours and result in costly downtime.

## **WHAT RISK IS YOUR NETWORK FACING RIGHT NOW?**

Hackers, with track records of developing sophisticated automated hacking tools, are hard at work creating new types of malware to confound IT administrators. Of 70,000

corporate networks surveyed in January 2001,<sup>3</sup> hackers made 6,000 attempts each month to gain access to corporations.

This is three times the number of attempts made in the previous month. Since January, IT managers have reported a sharp increase in the number of denial-of-service attacks which can freeze an e-business Web site, resulting in a loss of revenue.

## **TYPICAL VIRUS OUTBREAK SCENARIO**

More than 87% of all viruses enter the enterprise via emails. Email has evolved beyond communication to become a business critical application. If email goes down, vital links to customers and vendors go down with it, and business grinds to a halt.

A breakdown of the typical costs involved with detecting, cleaning, and recovering from a virus attack:

In this scenario, the entry point is an infected spreadsheet attached to an email sent via the Internet to 100 recipients at both Company A and Company B. It is assumed that 100% of computers are infected.

Cost for an IT manager to be informed of and take action on one virus incident \$500

Cost for one workstation to be stopped, scanned, and cleaned of virus \$1000

Cost for one workstation to detect and clean a virus infection locally \$100

Average number of times hackers will attempt to crack a network per month 24.

Investing in email virus protection can save an enterprise **\$22,000 per incident** or, calculating the assumed average number of times a hacker will attempt to crack a network, **\$528,000 per year**.

Time Period – Virus Incidents **Company A** Without Email Virus Protection

### **Company B**

With Email Virus Protection

Over One Year -- 24 \$540,000.00 \$12,000.00

Over Five Years -- 120 \$2,700,000.00 \$60,000.00

Over Ten Years -- 240 \$5,400,000.00 \$120,000.00

At one time the corporate safe was hidden behind a picture in the CEO's office, today the most precious assets are information. The concern here is with the loss of confidential or proprietary information due to an uncontrolled virus attack. There is no way to measure the actual value of information rendered unrecoverable by a malware program, but the cost can be high.

According to the ICSA, 36 percent of 300 organizations surveyed reported their servers were down for 1 hour or less, with the median downtime being 21 hours. A few respondents experienced longer recovery times up to 1,000 hours. More than 80 percent of those reporting a virus outbreak required 20 person-days or less to recover. The

average cost was between \$10,000 (median) and \$120,000 (average) in estimated direct costs.

The sooner an infection is detected, the lower the cost of eradicating it and the lower the residual costs due to damage and data loss. Stopping viruses at the server, rather than removing infections from numbers of files on hundreds of workstations, will save thousands of dollars per incident.

The solution probably lies in a service that gives you the power to monitor and filter e-mail traffic to protect your organisation from virus attacks, spam mails and wasted bandwidth right at the Internet level. All the unwanted emails (containing spam and virus) should be filtered at the service provider's servers before they reach your mail server and the intended recipients.

**Desired Features:**

- Double-level Virus Scanning
- Multi-layered Anti-Spam
- Spam Analysis Engine with auto-updates and auto-learning
- Personal Whitelists and Blacklists allow/block emails from specific IDs/domains
- Real-time Blackhole Lists capture data from global spam servers to block spam
- Content filtering
- Reports on email trends, viruses detected, spam volumes, policy violations

**The Service infrastructure:**



\*\*Note – ECM = Enterprise Clean Mail Servers

(Source: The Internet and antivirus sites like Trend Micro)