
Anti-Virus in the Corporate Arena

(version 1.01)

Martin G. Overton

*Virus Researcher and Author of ChekMate.
(Email: Martin@salig.demon.co.uk)*

Abstract

When you are responsible for the security of 1,000 to 100,000 PCs, virus outbreaks are getting out of hand, the users won't scan, can't run the TSR scanner or don't care about viruses, what do you do?

This appears to be the scenario in many large corporates.

Many security officers or support staff are given the onerous task of anti-virus strategy, policy, testing, implementation and support. Of these, few have the in-depth knowledge that *really is required* to understand the problem, let alone the solutions. How do they choose the right solution(s)? What are the options?

For many it's a catch-22 situation. If they ignore the problem, they are wrong. If they do something and it fails, they are also wrong! Management just want results.

Viruses are at the very least a nuisance and no matter how 'safe' and 'toothless' a virus it still hits the corporate support budget. Magnify this by the number of outbreaks within a company and add the cost of anti-virus software, updates and training and the problem becomes more focused and expensive.

This paper aims to answer the question that many corporates are asking 'What anti-virus defences do I choose, how do I implement them and how do I know that they are sufficient'.

This paper was written for, and presented at the 1996 Virus Bulletin conference at Brighton, England on September 19-20th 1996.

*I would welcome any suggestions for improvement, comments on this paper and it's content.
This paper will be updated from time to time.
(Martin Overton 10th October 1996)*

The Problem

Background

According to the Information Security Breaches Survey 1996, the most common security breach reported were computer viruses. The most expensive virus outbreak reported during the survey was estimated at £100,000.

By now most, if not all companies have encountered viruses. Their response to this problem is either panic, confusion, anger or in a few cases a well-gearred machine kicks into action to solve the problem.

Most companies' anti-virus defence consists of a scanner^[VB-1] and in most cases nothing else is used to combat the virus threat. The ability of most companies to defend themselves against the ever-growing numbers of new viruses is practically nil.

Viruses are now an everyday business problem^[VB-2] and that trend will continue to get worse for the foreseeable future.

The Cost

British businesses lost £28 million¹ due to reported virus incidents in 1994. This is just the tip of the iceberg as many companies do not report virus incidents due to the fear of lost confidence, both from business partners and customers and the subsequent affect on the companies' stocks.

Testing

How do you test anti-virus software?

Well, for most corporates, it is simply out of the question. Even if you have several thousand viruses on hand (*unlikely*) how do you know they are *real* viruses? Remember that to be viruses they *must* replicate otherwise they are considered germs or more often damaged files.

Even if you do get a valid virus test set, how do you test anti-virus software without risking cross-contaminating your systems?

Do you want to trust the glossy magazines reviews? Of course they rarely use *real* viruses and the journalist doing the test knows little or nothing about viruses. Nevermind, the winning products got a great user-friendly interface, that's all you're interested in right?

Well, there's always the anti-virus companies themselves. They are bound to give impartial advice, right?

This is the biggest headache for the corporate security officer!

The answer lies in independent² tests carried out by researchers that understand the issues and can in most cases make impartial recommendations on the ability of a scanner or other anti-virus counter-measure.

¹ Source: National Computing Centre Survey 1994.

² Such as Marko Helenius of the University of Tampere. Virus Bulletin also perform regular comparative tests, but some feel that they are a little too close to the industry to be completely objective.

Threats

Floppy disks

Until recently floppy disks infected with boot and partition sector viruses accounted for in excess of 80% of virus infections reported world-wide. Against all logic boot and partition sector viruses spread faster than most file viruses.

Macros (The Latest Threat)

Macro viruses have become the latest threat to corporate security. What was once considered safe, is now seen as just as capable of carrying an infection as executable code. Indeed, the boundary between data and executable code is getting mighty blurred. Currently Microsoft Word for Windows and Lotus Wordpro (*was AmiPro*) can be infected by this new class of viruses.

Of course many applications have macro languages built in to them to give even higher functionality to the end-user. Many are mini-operating systems in their own right. What this means to you is that macro viruses are going to become the number one threat to your corporate data. So expect the worst, if you use a widely used application with a macro language expect it to be targeted sooner rather than later.

Macro viruses pose a higher threat than the more conventional viruses for several reasons:

- They spread through any means used to share documents, diskettes, e-mail and groupware.
- They execute on any operating system that runs the application and the macro language that the virus runs under.
- The potential for damage, both from destructive variants, such as Hot and from the ease of creation by disgruntled employees.

STOP PRESS: Excel has now been targeted (currently known as Laroux).

The Internet

Viruses can be freely found on the internet. However, virus outbreaks linked to the internet sites run by commercial companies are quite rare. Most site operators have a good policy of checking files for viruses before offering them for downloading to the public. This is similar to most well run Bulletin Board Systems and similar information systems.

Be more worried about e-mail that contains binary data, such as Word and Excel files (Yes, they are binary files!) to be the biggest threat the internet has to offer corporates. This is of course only true for viruses and Trojan horses, other security issues for internet use need to be similarly addressed.

Support staff

Support staff are frequently guilty of infecting PC's that they are supposed to be fixing, all be it unintentionally. Nevertheless, support staff are a high risk category and should be treated as such.

Engineers

Engineers should also be treated as a high risk category. More so if they are from third party maintainers as the possibility of them encountering a virus is many times greater than those of internal engineers.

Cover disks

The ubiquitous magazine cover disk is still to be considered as much as a viral threat as 'Typhoid Mary'. Don't forget that cover CD-ROMs can also carry viruses and virus droppers, scanning 560MB of CD-ROM can take some time, but at least your staff can't infect them!

Home PC's

Many of your staff, especially your IT staff will have computers of their own at home. These can be another source of virus contaminated files and disks coming into your company. It makes sense to expand your anti-virus protection to include these home systems, as in the long run it will lead to lower instances of viruses being brought in from home.

Solutions

One thing you should be aware of is that there is no 100% solution to the virus problem. Any company that informs you that their product offers 100% protection from viruses are either naive or just don't fully understand the real problem.

However if you approach the problem in the right way, then you can minimise the percentage gap from that perfect 100%. A well-designed approach can be expected to give a 98-99.5% protection from viruses and their effects.

Policy

Use the K.I.S.S.³ approach for your anti-virus policy. The reason for keeping it simple is so that your staff can remember it. Something like the following would be sufficient as a basic template:

Sample Anti-Virus Policy

1. **Use the anti-virus software provided.**
 - *This is part of your terms and conditions of employment.*
 2. **Report any virus detected to security on ext. xxxxx**
 - *Do not use your PC until directed to.*
 - *Do not let anyone use any of your disks.*
-

³ Keep It Simple Stupid

Education

You may think that trying to educate your staff about the risk of viruses is like trying to nail jelly to a wall, and about as rewarding, and in most cases you are right. Your non-IT staff will generally be either blasé, paranoid or simply ignorant about viruses. They simply see it as not being their problem.

Support staff

In many corporates, your support staff are the ones that get the first call from a panicked user who has just been informed by the anti-virus software that the “XYZ123 Virus Has Been Detected”. Therefore they need to know what a virus is, how to remove it correctly, and how not to overreact⁴.

It is also of little use if only one member of the team has “*the knowledge*” as you can almost guarantee that the virus will be found when they are:

1. *Off sick.*
2. *On holiday.*
3. *On a course.*
4. *No longer working for the company.*

To avoid this very common pitfall, simply spread the skill around the team!

Developers

Your application developers can be seen as major players in the league of ‘viral spread’. They must be accountable for the master copies of software that they produce and be fully aware of the disastrous impact of them sending an infected master program or diskette for duplication. This is even more important where external companies may receive the infected application as a law-suit may quickly follow.

End users

These make up the bulk of most companies, and there lies the problem! The IT staff may understand about viruses, but non-IT staff just want to get on with their work.

Any form of anti-virus needs to be fast and effective or they won’t want to use it and in some cases may actually remove the protection that you have installed.

You need to make the protection as invisible as possible

⁴ Also known as ‘Headless Chicken Mode’.

Anti-Virus Technologies

Let's first look at the technologies currently used by most of the anti-virus products and explain their relative strengths and weaknesses.

Scanners

The main advantage of scanners is that they can detect known viruses before the execution of a file. Therefore they can stop a system from becoming infected⁵. Their main drawback is their in-ability to detect *all* new or modified viruses, and even all instances (generations) of some polymorphic viruses.

On-Demand

This is the archetypal virus scanner that uses a mixture of virus detection strings, decryption and polymorphic detection routines. Files are opened by the scanner to see if they contain the known virus, if they do, the file is flagged as infected by *xxxx* virus and the scan continues with the next file.

So let's do a little calculation as to how much time is wasted scanning hard drives in a year by a single person. Multiply this by the number of employees in the average company, and the 'real' cost of on-demand scanning is very clear!

Working Days (Average per Year)	x Time of Scan (Mins(Average))	Minutes	Hours	Working Days (@ 7 Hours)
260	5	1300.00	21.67	3.10

This example only assumes that a hard disk is scanned once a day.

Strengths:

The plus points of on-demand scanners are:

- *Can detect known viruses before another file is infected.*
- *Useful for vetting new files and disks.*
- *Not memory resident (TSR).*

Pitfalls:

There are a variety of pitfalls to on-demand scanners, these include:

- *Can't detect new viruses that are not in their database.*
- *Can miss some generations (mutations) of polymorphic viruses.*
- *If used properly (from a cold-boot), can be very, very slow.*

⁵ If used properly, otherwise the scanner may actually *spread* the virus.

Memory Resident (TSR)

A TSR (Terminate and Stay Resident) program is one that remains in memory as a background or delayed task. The virus-scanner TSR's have most of the detection capabilities of the main package. This TSR will of course require some memory for it to run in. Anti-virus TSR's will take from 3-50+kb of memory away from DOS (dependent on the protection offered and the product used).

Strengths:

The main advantage of a TSR based virus scanner is the ability to do 'real' time or active scanning (on access). This means that any time the executable file is run, copied or moved the file is then scanned for viruses. This is invisible to the user, unless a virus is found. If a virus is found the user will usually be presented with a menu of options, as below:

*File Infected With XXXX Virus
Run the file or Exit (R/E)?*

This menu of choices will vary from product to product and can be in many cases be configured to only give certain choices and a custom message.

This constant, background detection makes TSR scanning very popular and suitable for systems that want little or no interruptions for scanning for viruses. It also adds an extra layer for the virus to try to disable or fool.

Pitfalls:

There are a variety of pitfalls to TSR scanners. These include:

- **Memory Requirements:**
As mentioned above, the amount of memory required by a TSR can be excessive. This coupled with PC's on a network can cause real and embarrassing problems when programs that used to run fine, no longer do so because the scanner is 'hogging' valuable memory.
- **Compatibility:**
There are compatibility issues with this type of scanner. Many people are aware of the problems with TSR's 'fighting' for the same memory area, or generally being incompatible.
- **Disability:**
Most of the newer viruses can disable, bypass or even unload many of the resident scanners available.
- **Over-reliance:**
Many users may become over-reliant on the resident scanner, and rarely or never use the 'full-blown' scanner, as it is seen as unnecessary. This of course is a very large security risk as a complex polymorphic virus could be running rampant on their system, and of course exposing others to the same risk.

- **Detection:**

Some of the resident scanners do NOT detect the same number of viruses that the 'full-blown' product does. Usual casualties are polymorphic viruses such as Uruguay or MtE/TPE based viruses.

Device Driver (VxD)

This is the latest incarnation of the virus scanner approach. The VxD scanner is a Windows (3.x or '95) virtual device driver. This *usually* offers the same level of detection as the on demand scanner. The main difference is that the protection is continuous⁶ as offered by the TSR scanners, but without the TSR scanners' downside. This of course will not protect you against new or many modified viruses.

Strengths:

The plus points of VxDs are:

- *It can in most products detect all the viruses known to the full scanner.*
- *Constant protection while within Windows.*

Pitfalls:

There are a variety of pitfalls to VxDs, these include:

- *Only alerted to an active virus when Windows is loading (loaded).*
- *Viruses may be written that can disable or bypass this protection in a similar way to the TSR scanners.*
- *Most can't detect new viruses that are not in their database.*
- *Unlike on-demand scanners, it is not advisable to have competing products loaded at the same time.*
- *Not yet as mature as on-demand scanners.*

Heuristic

Heuristic analysis is a method employed by a growing number of virus scanners. It aims to detect a virus in a file (or area) by the code content. Heuristic scanning analyses the file to see if the code appears to be like a virus or carry out virus-like actions. Such as, if it searches to the end of another file (appends code) and modifies the start (jump instruction) to the new code added. There are of course many of these types of coding to check for. In this way heuristics can be used to detect some unknown viruses (around 60-80%).

Strengths:

The plus points of heuristic analysis are:

- *It can detect unknown viruses (around 60-80%).*
- *Scanners based on heuristics don't need frequent updates (though most are updated monthly or bi-monthly).*

⁶ As long as you are running Windows or a DOS box within Windows.

Pitfalls:

There are a variety of pitfalls to heuristic analysis, these include:

- *False positives (the analysis flags a perfectly innocent file as infected).*
- *False negatives (the analysis is flawed or fooled by an anti-heuristic virus, such as Quicky⁷, therefore the virus is not detected and is free to infect other files, etc., while the scan is continuing).*

Behaviour Blockers

These are similar in nature to the TSR scanners. The difference is that they don't tend to use virus strings or known virus detection routines. Instead they tend to monitor system areas (such as CMOS and the Interrupt Vector Table), memory, track 0 (zero) of the hard disk (where the partition and boot program is stored) and any attempt to modify executable files or for files to go TSR (memory resident).

Strengths:

The plus points with behaviour blockers are:

- *They can trap unknown viruses.*
- *They don't need frequent updates.*

Pitfalls:

There are a variety of pitfalls to behaviour blockers, many are the same as those suffered by the TSR scanners. These include:

- **Memory Requirements: (as TSR's)**
- **Compatibility: (as TSR's)**
- **Disability:**
Many of the newer viruses can disable, unload or bypass (*such as MegaStealth*) behaviour blockers. In fact many of the tunnelling viruses can slip undetected past them.
- **Too Many False Alarms:**
Many users may become irritated by behaviour blockers. Even simple tasks like formatting disks or updating SETVER are fraught with problems. The users will tend to disable this protection as it is often seen as too intrusive.
- Finally, the behaviour blocker relies on detecting a virus by its behaviour, which is in most cases is impossible as proven in ^[Cohen2].

⁷ QuickSilver.1376, this virus was detected by ChekMate 'in the wild' before any scanner was aware of it. It uses anti-heuristic routines to fool heuristic based scanners. It is also encrypted.

Integrity Checkers

The integrity checkers (also known as checksummers) main advantage in the fight against viruses is that it can detect *any* change to a file⁸. This means that a checksummer can detect any virus attack on a hard disk, even if the virus is unknown to any scanner

What is integrity checking?:

Most if not all of the virus scanners on the market at this time have the ability to do some form of integrity checking of files on a system. The checksum routine usually produces a 32, 64 or 128 bit checksum. Some packages use a cryptographic (also known as a one-way) checksum and these are very secure⁹. It was proved in ^[Radai] that a cryptographic checksum is not always required as long as the generator is unknown, user specific and encrypted or otherwise protected from an attacking program (virus).

Integrity checking involves computing a mathematical value (CRC) for the content of the file, this is then stored along with size, date and time, and attributes of the file¹⁰, this information is stored as values next to the files name and path in a database, or attached to the end of the executable itself. The database may be encrypted in an aim to prevent the values being manipulated by a virus.

The database entry and CRC is checked at user generated intervals¹¹ when the integrity checker is activated. A new CRC is generated from the file and this is checked against the stored CRC. As long as the two remain the same, then all is supposedly well. Otherwise a message informing the user is displayed letting them know that the file has been modified and MAY contain a virus!

Some of the newer products also take a snapshot of the start and or end of the executable code/file. You may ask why? The answer is that most viruses have to modify the start and/or end of the code/file it is infecting to ensure that it runs its own code before that of its host. This method is secure as long as care is taken to ensure that a stealth virus is not active in memory.

Strengths:

- The vast majority of viruses can easily be detected with an integrity checker, even new, unknown and modified viruses that may well slip past a conventional scanner.
- As stated in ^[Bontchev] “The integrity checking software is the currently strongest line of defence against computer viruses” it goes on to say “In fact as demonstrated by ^[Cohen], they are currently the most cost-effective and sound line of defence against the computer virus.”

⁸ Under clean boot or simulated clean boot conditions.

⁹ MD5 is a 128 bit cryptographic hash function from RSA Inc.

¹⁰ Not all of these details are stored by all products.

¹¹ Unless the checksummer is a resident (TSR) product.

Pitfalls:

- Some viruses have been specifically targeted against checksumming techniques used by many scanners. These include: *StarShip* - This gets past checksummers by only infecting floppy disk files (no integrity checker checks floppies). Also *Groove* and *Peach* will delete some products checksum databases. These badly designed products will not flag that the database has been deleted, it will simply re-create the database and of course the checksum for the now infected files.
- In an area that regularly updates or changes the configuration of PC's a conventional checksummer is irritating and useless. The user would disable it within a few days.
- Self-modifying executables, such as SETVER will frequently be flagged as possibly having been infected by a virus.
- Checksummers that do not check to see if a stealth virus is active in memory *before* checksumming files may well not see any modification even if a file is infected because of the way that the stealth virus is showing the file as it was *before* it was infected. This could then cause all the possible target files to be infected¹².

Targeted Integrity Checking

This method uses the strengths of checksumming (the ability to detect any modification, to a file or other protected areas) without the downside of quite lengthy checking times. What it does do, instead of trying to check the whole system, only targets that are frequently attacked by viruses are tested. This allows very fast checking times with a very good level of confidence that the system is currently clean or not as the case may be.

This needs to be used with other techniques to ensure that a fast infector is not active in memory.

So let's do a little calculation as to how quick a targeted integrity checker is when compared to the scanners or a conventional integrity checker (checksummer).

	Working Days (Average per Year)	x Time of Scan (Mins)	Minutes	Hours	Working Days (@ 7 Hours)
Targeted Integrity Checker	260	.5	130.00	2.17	0.31
On-Demand Scanner/ Checksummer	260	5	1300.00	21.67	3.10

You can clearly see that the time that is taken by a scanner over a year is excessive when compared to a targeted integrity checker. Remember that this is just a single use per day, per employee.

Byte-for-Byte Comparison

This is a simple yet very effective way of detecting non-stealthed or limited stealthed viruses in files, boot sectors and partition tables. It simply compares a stored code 'snapshot' or 'fingerprint' against a new runtime 'fingerprint' for a file or area. The easiest way to describe how it works is to say that it works in a very similar way to the COMPARE command under DOS.

¹² Of course this is as much a problem for a virus scanner as a checksummer, in many cases more so as a scanner tends to be executed more frequently.

Any change¹³ will be detected using this approach.

Interrupt Vector Analysis

Most memory resident viruses modify the interrupt vector table in one of two ways:

1. Actually 'hook' the interrupt by re-directing it to its own virus code.

e.g. No Virus

Original Int 21 entry in IVT	0C1D:027C
------------------------------	------------------

e.g. Virus Resident

Redirected Int 21 entry in IVT	093A:9EF2
--------------------------------	------------------

2. Follow the interrupt table entry and patch the interrupt code that the IVT entry points to. This now will jump to the virus code, which does its stuff, and then it may return control to the 'original' interrupt code.

e.g. No Virus

Original Int 21 entry in IVT	0C1D:027C
Original Code at 0C1D:027C	904C203D0020

e.g. Virus Resident

Original Int 21 entry in IVT	0C1D:027C
Patched Code at 0C1D:027C	EB9EF2CD2190

Either way the virus gets control of the interrupt and can do whatever it wishes to do.

Testing for this sort of modification is fairly easy and quite accurate in detecting viruses.

Top-of-Memory

Most boot sector (DBR) and partition table (MBR) viruses as well as many resident file infecting viruses will create a 'hole' in base memory (the first 640Kb) and place it's code there. Usually this 'hole' is 1-4Kb¹⁴ although some use as much as 12Kb.

This can be a very effective way to detect boot sector and partition table viruses active on a system.

Decoys

This is a fairly new approach. Many anti-virus researchers use Decoys (also known as Bait or Goat files). Very few virus detection systems use this approach, even though it is very successful (as long as a suite of suitable files is generated). These files simply exist only to act as a target for a virus.

¹³ Assuming that an advanced stealth virus is not active in memory. A good AV product would detect it's presence in memory and warn the user.

¹⁴ Form, AntiCMOS, Parity Boot.B, Sampo, Michelangelo and Monkey amongst many others

Some viruses are fussy about files they will infect and this needs to be taken into account. Tremor for example will not infect files under 10Kb in size and Quicky won't infect files over 300Kb (this is probably to avoid infecting AV programs).

These 'decoys' are files with constant known state. This means that they should *never* change. Using this fixed state of these files allows them to act as a 'viral smoke alarm'. To work correctly the files need to be checked *before* and *after* execution to spot modifications that should only ever be due to a virus active on the system.

This approach, amongst others described in this paper, has allowed ChekMate to detect unknown viruses¹⁵ before any scanners on the market were able to detect them.

Why Multi-Layered?

A multi-layered approach involves the use of multiple technologies for virus detection.

"But why do I need to implement a multi-layered approach?"

Below are the main reasons for using a multi-layered approach:

- *New viruses appearing more rapidly on business PCs. (200-250 new viruses every month!)*
- *Virus GLUT (many virus scanner producers are finding it tough to keep up).*
- *Scanners can only detect viruses that are known to them.*

Any one anti-virus technology will not offer 100% protection from all viruses and other malware. A Multi-layered approach would include at least several, and in some cases most of the following anti-virus technologies:

- *Signature scanning*
- *Code emulation*
- *Integrity checking*
- *Heuristics*
- *Interrupt tracing*
- *Decoy launching*
- *Diskette authorisation*
- *Behaviour blocking*
- *REGULAR BACKUPS*

Multi-layered protection is the '*belt-and-braces*' approach to the virus problem. Caution must be exercised as each extra layer can carry an increased support burden if the wrong products are chosen.

Yes, regular backups of DATA on your system is still very important, you can replace program files easily enough from master disks, but corporate data is worth a lot more to your company and is very hard to replace if damaged or destroyed.

Even with this '*belt-and-braces*' approach you will still only get 98%-99.5% protection from viruses.

¹⁵ Unknown by scanners at the time of initial detection at the customer sites. The viruses include: QuickSilver.1376, Dalian and Jerusalem.HK.2880 amongst others.

Why Multi-Level?

Do all you users have the same shoe size, dress sense or sense of humour? Of course not. Likewise their exposure to viruses are also different.

How do I categorise my staff?

Your highest risk users are frequently your support staff and your system and application developers. Don't forget your business critical departments in this risk category. Why? Well, what happens if you get a major virus outbreak in a department that brings in a large slice of the revenue for your company? Can you afford to lose business for hours or days?

Well, What Should We Use?

Products

Do you really expect me to tell which suppliers' products to use? Well just have a look at some good independent reviews to help you choose a brand. Don't forget to check out the support structure for the company that you choose. Do they cover all 365 days of the year? How often do you get updates? Can they handle new viruses that you find and supply a detection and cleaning method promptly?

Below are the major categories of anti-virus software that you might want to include in your multi-layered virus protection.

- ***Scanners***
- ***Integrity Checkers***
- ***Behaviour Blockers***
- ***Diskette Authorisation***
- ***Access Control***

Example Multi-Layered Approach Product Table.

Platform	Criticality			
	High	Medium	Standard	Low
DOS	<i>1a or 1c 2a or 2b or 2c 3a</i>	<i>1a or 1c 2a or 2b</i>	<i>1a</i>	<i>1d</i>
Windows 3.x	<i>1b and 1f 2a or 2b or 2c 3a</i>	<i>1b and 1f 2b or 2c</i>	<i>1b</i>	<i>1a (Scheduled)</i>
Windows 95	<i>1b and 1f 2a or 2b or 2c 3a</i>	<i>1b and 1f 2b or 2c</i>	<i>1b</i>	<i>1a (Scheduled)</i>
Windows NT	<i>1a or 1b or 1c and 1f 2a or 2b or 2c 3a</i>	<i>1a or 1b and 1f 2b or 2c</i>	<i>1a or 1b</i>	<i>1a (Scheduled)</i>
OS/2	<i>1a or 1c 2a or 2b or 2c 3a</i>	<i>1a 2b or 2c</i>	<i>1a (Scheduled)</i>	<i>1a (Scheduled)</i>
Novell Netware	<i>1e 2b</i>	<i>1e</i>	<i>1e</i>	<i>1a (Scheduled)</i>
IBM Lan Server / Microsoft Lan Manager	<i>1a (Scheduled)</i>	<i>1a (Scheduled)</i>	<i>1a (Scheduled)</i>	<i>1a (Scheduled)</i>

1a. On-demand scanner*1b.* VxD scanner*1c.* Heuristic scanner*1d.* TSR Scanner*1e.* NLM scanner*1f.* Macro scanner*2a.* Diskette Authorisation*2b.* Integrity checker*2c.* Behaviour blocker*3a.* Access control

Below are some examples of how to categorise your staff:

High Risk

Support staff, Engineers, Developers, Critical business areas, Staff with a history of virus outbreaks and areas with large diskette or document throughput.

Medium Risk

Users not in the above category, but that have a high throughput of diskettes (>10 a day) or files from applications that use macro languages.

Standard Risk

This is your standard level of anti-virus protection.

Low Risk

The level of protection for PC's that are rarely changed, such as print servers or gateways.

Free Protection!

Novell Netware

There are some very simple but highly effective ways that you can limit the spread of a file infecting virus on a Novell server. These are:

- Do not use CREATE and WRITE permission for any directory that contains executable files. This is especially true of PUBLIC and SYSTEM shared directories. Try to default user access to shared directories as:

May Read from File	(R)
May Scan for Files	(F)

- Do not allow your support staff to use the SUPERVISOR or ADMINISTRATOR id for normal daily use of the server. Restrict its use to tasks that really require *full* access to the server, otherwise if they introduce a virus onto the server it will probably spread very rapidly to the whole network and even infect the workstations. Of course allow their *normal* user id to have full server READ access, but on no account allow them WRITE access outside their own user area ^[Sophos].
- Do NOT use the EXECUTE ONLY Novell attribute for files as although this is very secure, it will even bar file access to a virus scanner.

PC's

- To provide simple but very effective protection from true boot and partition sector viruses, simply change the BIOS boot sequence from **A: , C:** to **C: , A: .**

Now even if an infected diskette is left in the drive during a reboot or power-up then the system is unlikely to become infected.

- Otherwise, removing or disabling the floppy drive will help, but this is probably overkill.

Implementation

Network

Installing anti-virus tools on to a network and then getting the workstation to run them from there is a sensible solution. It enables central control of both updates and where required installation of anti-virus software for all the users of the network server that they login to.

The example below assumes a Novell Netware server and a mixture of OS/2, Windows (3.x, '95 and NT) and DOS workstations.

The directory structure on the server looks like this:

VOL1 : \ANTIVIR	
	\DOS
	\WIN3
	\WIN95
	\WINNT
	\OS2

For each of these directories a Novell Group would need to be created and all the users of each operating system would need to be added to the relevant group. This can then be used to run the correct software automatically when the user logs in to the server.

The system login script would then be edited to check to see which group a user is in, as below:

```
IF MEMBER OF "WIN95" THEN
    #COMMAND /C WINSCAN.EXE
END
```

Some of the better products have utilities to make installation and updating of files easier. This is especially useful where a VxD scanner is used as the files will almost certainly need to be installed / updated on the local workstation's hard drive. A test for the presence and version can be automated in a similar fashion to the example above for calling a scanner directly during the login script.

A central code server needs to be created so that other LAN Supervisors or Administrators can login and copy the software or updates at regular intervals. The copying of updates to the other satellite servers could also be automated. Once setup this is a very efficient solution with a very low total cost of ownership compared to individual workstation updating via diskettes.

Similar automation routines can be used for other network operating systems such as Lan Manager or Lan Server.

Standalone

This covers the shrinking number of isolated (un-connected to LAN) PC's. These could be handled in a number of ways:

- An automated floppy installation.
- Via E-Mail attached as a binary attachment, such as Lotus Notes, CC: Mail, MS Mail or Internet¹⁶ Mail.

What's Next?

Well, you have now installed your chosen anti-virus software, all your staff are running them and you are surely fully protected from viruses now?

Yes, you are now protected from known viruses and if you have implemented a multi-layered approach then also from most new or modified viruses that the scanner doesn't yet know about. Now though, is not the time to think that the war is won. This is just the first skirmish in the never-ending war against viruses

To continue winning as many rounds as possible, these are the points that you must consider:

- Frequency of scanner updates.
- Pro-active approach.
- Review your strategy and products at least yearly.
- Evaluate new technologies as they appear.

¹⁶ This requires converting the file to MIME or UUENCODED format for internet transmission.

Conclusion

Conventional virus scanners are still needed for identification of known viruses. However, they are no longer strong enough to offer protection from the ever increasing numbers of new viruses that are appearing 'in-the-wild' *before* scanners can detect them. A multi-layered approach for protection from viruses *is* the way forward.

Virus scanners should still be used for checking floppy disks, CD-ROM's and downloaded files before they are used, or a VxD based scanner should be used to give similar automatic protection. Other technologies must be used to help strengthen the defences, especially in answer to the macro virus problem as this has the greatest scope for impact in corporates.

-
- [VB-1] Editorial, Virus Bulletin February 1994.
- [VB-2] Editorial, Virus Bulletin April 1994.
- [Cohen2] Fred Cohen, Computer Viruses - Theory and Experiments.
- [Radai] Yisrael Radai, Checksumming Techniques for Anti-Viral Purposes.
- [Bontchev] Vesselin Bontchev, 'Possible Attacks Against Integrity Programs And How To Prevent Them'.
- [Cohen] Fred Cohen, A Cost Analysis Of Computer Virus Defences.
- [Sophos1] J. Benjamin Sidle and Dr. Jan Hruska, Viruses and Anti-Virus Measures on Netware.