FEATURE

Through the Administrator's Eye

Phil Crewe
PERA Group

These days it is very easy to put in place a virus scanner which, on the surface at least, will scan for all known viruses (some scanners can scan for unknown ones as well), giving your machine the best protection money can buy. Most also include a monthly update service to ensure that the user stays ahead of the game.

For any reasonably technical person, having a machine without some degree of virus protection must be viewed as almost a dereliction of responsibility. There are, however, many cases that do not fall into this simple reasoning.

If you are an administrator in charge of many machines in a corporate environment, the issue is more than merely providing a degree of virus protection to a technical user. Also to be considered is usability users with a wide range of skills, scalability of protection required, and applicability to potentially multiple client platforms and to different network architecture. Further, there are the normal administration and updating headaches which come from running any piece of software on multiple machines, which are probably also separated geographically.

And this is just the technical side of the problem! Installing software on any machine brings with it a set of problems for the customer support department – virus protection is no exception. The support department will have to field the false positives generated, as well as having to manage the expectations of the users.

These users must accept that installing anti-virus software does not negate their responsibility, but merely provides a degree of safeguard for when they are using data and applications from floppy disks or public service networks. It does *not* mean they have *carte blanche* to bring in software (games or otherwise) from home simply because the virus issue may be being addressed by using a software solution.

At the User Level

Let us look at what is probably the largest sticking point of installing any virus-protection software. The software has to be almost invisible at the user level, except when a virus is detected. It must be quick to scan information, and should never get in the way of what the user is trying to do.

Ultimately, a user is employed by a company to do a particular job. Whatever that is, no software installed on a client machine should interfere with that. Software should enhance users' ability to do their work, not interfere with it.

From many users' points of view, virus-protection software is probably the greatest potential interference on a user machine. It will do nothing to enhance their ability to do the job, but might get in their way with false error messages, could slow the machine down, or even forbid them to use certain devices such as floppy disks. Solutions such as these tend to be acceptable only in certain circumstances (such as on military bases), where the issue is larger than just viruses.

Not Just for Viruses…

When anti-virus software is being considered, it should not be forgotten that installing a corporate virus protection policy may give additional benefits over and above pure virus protection. For example, it could be viewed as an opportunity to ensure that all floppy disks coming into and out of the organization are logged, thus giving the corporation better control over some of the other security issues that it could be facing.

It is also a chance to take additional control over client machines from a management perspective. For instance, it is an opportunity to audit all client machines to ensure that any fixed asset register is up to date.

An administrator might therefore use the opportunity to visit client machines to install virus protection and do a general scan on the machine, thus gaining valuable information for other items such as maintenance contracts or software update planning. If this is the case, it is also a good idea to consider, at the same time as the anti-virus software, the PC management software which is to be implemented in order to do all this.

Since any good strategy re-uses this kind of information to maximum benefit, and since most companies are currently considering their response to the millennium issue with respect to desktop machines, information gleaned from this process may be valuable at many points down the road.

On Handling Updates

It is most certainly neither desirable nor time-efficient to have to visit every desktop machine at regular intervals in order to keep an anti-virus package up to date. Therefore, another issue which must be considered when thinking about which package to implement is how the updates are to be distributed to client machines.

Software distribution packages are available as separate units: if the company has standardized on a particular software update package, it may well be that anti-virus updates can be distributed in this manner. Remember that software distribution can be as simple as a file being downloaded automatically from a file server whenever a user logs on, and need not be based on the more complicated packages available. Note, however, that such packages are specifically written to cater for large corporates and mass software distribution, so their functionality and facilities are much more complete.

Another solution is to implement a client/server solution where both clients and the file server to which they are attached have the same anti-virus package. A careful choice of package will enable the distribution of the updates directly from the server system.

Naturally, even this update process should comply with the general resolution; i.e. not to interfere with the users' work in any way. The user does not need or wish to know that the anti-virus data file has been updated, even if it is just with a dialogue box with an 'OK' button.

Easy as it is to hit that button at that point, the majority of users will find this unacceptable. Most people have a routine when powering up their machine in the morning, and additional dialogue boxes will interfere with this timing. Whatever system is being planned, always bear this golden rule in mind: 'Never disturb the user unless you have something interesting to say.'

Informing the End-user

This last issue raises the next point – how to tell users when you have something interesting to say. The only time the user should be informed is when a virus (or a suspected virus) has been found. In all other cases (no matter what they are), a message could be generated back to a systems administrator, where it can be interpreted properly, and further action implemented, if necessary.

Triggers for a message to the administrator could be a failure to load part of the software, or the fact that the data file is out of date, or that a user is doing something outside the security policy. In all cases, the administrator should be informed directly: reliance should not be placed on the user informing the administrator. Thus, another 'requirement' of an anti-virus system should be integration with the internal electronic mail or alerting procedure used in the company.

When a virus has been found, what should the user see? Primarily, the user should be prevented from infecting anything else. This is the first point at which user productivity can legitimately be interrupted. At the least, the user should be prevented from logging onto the network, if the machine itself does not lock up.

Whatever takes place, the user now needs to be told exactly what is happening. There is no point in locking the machine so the user cannot do anything, if you do not give the reason for such action. This may sound obvious, but there have been circumstances where the first a Help Desk knows about a virus problem is when several users from a department ring to say that they are completely fed up with the network, as no-one can get on to transfer their files.

In several such cases, it transpired that whenever they turned their machine on, the anti-virus software locked their machine as it had detected a virus. Since the users did not know what was happening, they talked to their departmental 'expert', who advised them to boot with a floppy disk. This circumvented the normal booting procedure of the machine and did not load the anti-virus software.

The employees continued to work without network or email facilities, and passed data around on floppy disk. Naturally, all of the machines were infected by the time the administrator found out what the problem was, and a significant amount of time and energy was needed to resolve the problem.

The upside of this is that the virus outbreak was contained to within a department. If floppy disks had been exchanged outside that department, however, this may no longer have been the case. If the anti-virus package had been configured to inform the users why the machine was stopping working when it did, the administrator would have been able to take action much earlier.

> *"there should also be another method of routine scanning whereby viruses are detected proactively"*

It is also recommended that error messages generated by anti-virus software are personalized to the company concerned. Most anti-virus software allows this, at least enabling additional information, such as 'call the Help Desk on extension 4431', to be displayed in any error dialogue boxes. If this is the case, the user will know what to do next.

Once again: do not get in the users' way unless you have to, and when you *do* have to, tell them what to do next, clearly and simply. Alerting the administrator directly via internal email or messaging is very advantageous, as the administrator will know when anything out of the ordinary, although not necessarily fatal, has occurred.

Pick a Package, any Package

When considering what type of anti-virus scanner to put in place, it must always be remembered that, when dealing on a corporate scale, one false positive for a given package could lead to a call to query it from every user in the corporation. Therefore, it is just as important that the package chosen generates a minimum of false positives as it is to detect the viruses required and to have a good update program.

Implementing any of these systems is naturally going to cost the company, both in financial terms and as regards time and effort in installation and maintenance. This needs to be considered against the question 'What happens if we don't do it?'

First, there *is* no correct answer to this. We all have a feeling that implementing virus protection software is going to help us in the long run: in general this is correct, in that we will all come across a virus outbreak at some point. However, if we are taking considerable pains to ensure our users' activity is not disturbed, we should at least think about what we would do if we implement nothing, thereby not disturbing the user at all, and a virus outbreak occurs: how then would we recover from the situation?

Recovery and Consequences

At a detailed level, the cost of recovering from a virus outbreak will rather depend on the virus concerned and the number of machines affected. If the outbreak is restricted to only a few machines then the cost of clearing up will be small. It will nevertheless involve time and effort in backing up data, reformatting hard disks, re-installing software from supplied floppy disks, and replacing the data. The more machines are affected, the greater the cost.

The question is, however, how will you know when you have a virus infection? Without some degree of virus protection available within the organization, it could go unnoticed for some considerable time, either until a machine starts to malfunction or (and in my opinion worse) a customer tells you that a floppy disk you sent them has infected their machines.

If a customer, as the result of such an incident, loses confidence in your supplies to him, it could mean a loss of business. This would have much larger financial consequences than the potential cost of early virus detection on your system. How do you know that it is you who has infected those client machines? You could spend time trying to track down a virus which does not even exist on your machines, and you might still lose the client.

A policy of virus detection and protection which is known and understood within a company will not only help you to trap a virus earlier, and therefore not send out an infected floppy disk to a client, but it will also enable you to have some authority to say to the client 'it cannot be us' when they report a virus to you – you will be able to point to the virus detection systems you have.

Costing the Clean-up

Purely in clean-up terms, and assuming an infected machine uses, maybe, four applications, the cost per machine to clean up after a virus will probably approach £250. This assumes all the software is readily available for a technical person to re-install on the machine, and that a tape streamer is available for backing up all the data from the machine.

The PC needs to be backed up (probably twice), the hard disk reformatted, the applications re-installed from floppy disk (which should include the operating system) and the data re-installed from the back-up tape. All being well, a good technician can probably do this in one day.

So, to fix one machine will take £250 worth of a technician's time. Add to this the loss of productivity of the person who normally uses that machine, which could be up to another £250. This does not take into account the fact that, if that person happens to be one who usually deals with clients, there could be potential problems filling client requirements, which may lose you the client. Further, invoices and payments may go out late, which may have additional consequences.

Multiplying this by a typical fifteen-person workgroup, and assuming an IT department of five working on the systems, it will cost nearly £4000 for the IT department, £4000 for the fifteen people in the department who cannot use their computers for one to three days, plus the opportunity cost to your organization of having this workgroup idle for that length of time. This could run to between 10 and 100 times the cost of the £12,000 (approximately) in core business costs for having the virus outbreak.

At that point, it becomes easy to justify spending considerable time and effort on the right hardware and software combination to help your organization remain in control of the virus problem.

How Much is Enough?

An added degree of complexity comes into the equation when we consider that, to be adequately protected from a potential virus attack, we should not put all our trust in one software product. This is because, in the ever-changing complexion of the virus world, we can best protect ourselves by having more than one source of virus information and protection.

On more than one occasion, I have seen a virus outbreak in an organization with a virus strategy in place, simply because the software on which the organization relied, across all machines and servers, came from a single vendor. This particular software had an engine which could not detect one specific virus type well; therefore, when this virus was introduced into the organization it was able to spread easily before it was caught.

This begs the question that, if we assume that more than one product should be available as the solution to the problem, how do we reconcile this with maintaining an environment which is easy for users to use and at the same time easy to maintain for the administrators?

The first step along this route is to provide IT staff who are likely to be visiting machines with a different virus protection tool from the one already installed on the machines being visited. We can assume that, if a virus is on a machine where virus protection is installed, the same piece of software on a floppy disk will probably fail to detect it the second time. Having a separate tool available to IT staff will reduce the chance of this happening. This will certainly highlight a new virus when problems are reported to IT staff, and will give the company a greater degree of confidence that viruses will be detected.

Alternative Routes

There should also be another method of routine scanning whereby viruses are detected proactively rather than reactively, with more than one piece of software. The best way to do this is to have scanning of the file servers done by software different from that in use on the desktop.

In order to maintain virus signature information in an up-to-date way, we will probably have to install the same scanner engine on the server and the clients to gain the benefit of downloading new signatures automatically.

The solution to this paradox is to have more than one scanner available to the server, which is then triggered manually or semi-automatically to scan at longer intervals than the core product in use on both the client and the server.

One way of achieving this would be to have the core product scanning on a nightly basis, and scanning all files which are saved and opened from the disk drives, but to have a secondary product which is brought into play manually on a regular basis, when the primary product is disabled, for example over a weekend.

“any users who copy applications to the file server should have their machines thoroughly tested on a regular basis”

Thus, the primary product will be in use day to day, and will maintain virus signatures at the client workstations, but during Friday evening the primary product is disabled and a secondary product on the server is enabled, which progressively scans the disk drives and alerts the administrators to any anomalies which it uncovers.

If a good secondary product is chosen and this is also installed on all servers across a network, the additional administration is small. The overhead on the file server is also small, since it is disabled for most of the time.

Virus detection using the normal tools available will scan local hard disks and floppy disks for suspect files, and server versions of the product will also scan server disks. However, most off-the-shelf packages in their native form will not scan files transferred between users over email (though naturally they will scan files as soon as they are saved to the hard disk).

Many packages are now addressing this issue, and providing engines running on the post office machines which inspect all email attachments, and scan them using the standard virus protection engine to determine whether they are virus free. There are also several stand-alone products which use a third-party virus-scanning engine to achieve the same aim; specifically, to protect an Internet connection.

These third-party products are a good system to consider. You can choose your virus-detection strategy based on your other requirements as an organization along with the ability of the virus detector to detect viruses, then leave the handling of email attachments to a third-party product which uses your chosen detection engine and which fits with your email strategy.

Make it Tough!

There are other measures that could and should be taken to ensure that viruses do not have an easy life within a corporation. These should be in place in any large company, with full-time network support, but it is worth reiterating a couple of simple measures which will help.

First, ensure the security on your network server is as tight as possible around all areas which contain shared applications. If users run applications off the server, and one user with the ability to write to the server has a virus which infects those applications, that infection can soon be prevalent on the executable file and therefore infect all machines which run it.

Any users who copy applications to the file server should have their machines thoroughly tested on a regular basis, since an executable with a virus copied to the file server can cause rapid spread of infection around an organization. It is normal to find an area of the network shared amongst workgroups, and it is very easy for someone in that workgroup to copy a file into that area for other users of the workgroup to run, especially if that user is reasonably technical and has a machine at home. Maintain a ‘weather eye’ on all these areas of the network, to ensure they do not pass viruses around unwittingly.

The security on a file server can, of course, be circumvented by the supervisor account. The supervisor account will have (in general) total and full access to all parts of the network file server. Thus, a virus-infected machine being used by the supervisor (or somebody logged in as a supervisor equivalent) could easily infect a file server.

It is good practice for a supervisor to have more than one login, and for the second login only to have standard user-equivalent rights. Thus, the supervisor can work most of this time, maintaining security, and only when necessary to do supervisory functions, would he log in with the full supervisor logon.

Backups and Other Safeguards

Of course, one of the best protections against a virus outbreak, apart from anti-virus software and monitoring, is a good backup system. This should be in place whether or not a company is thinking of the virus problem *per se*, and also for any issue which may involve recovering from a potential disaster. A virus outbreak is one of these issues in just the same way as fire or flood, and, like these, should have a good backup system as its core.

The backup system should be automatic and should be regularly checked and tested, or (a) it will not get done, and (b) when it does get done the data may not be valid.

In general, viruses will infect application files rather than data (although some of the recent viruses prove this is not always the case); therefore, as well as a good backup, the administration department should have access to the applications in order to re-install them from floppy disk or CD onto users' workstations as necessary.

Having this available and, better still, having tested it, will make recovery a much cleaner and quicker operation. The faster you can recover from any disaster, the less exposed you will be as a company.

Another commonly-used technique is to have a 'dirty machine' which is off the network, and on which no company business is carried out, on which to try out new software or test floppy disks coming in from outside the company. Whilst a useful tool, especially in situations where software is coming in from the outside on a regular basis, it should not replace rigorous anti-virus procedures on client machines.

In instances where there are multiple machine types such as PCs, *Macintoshes*, and UNIX platforms, the issue becomes yet more complicated; however, the same principle still applies. More than one anti-virus package should be used wherever possible, and the method for maintaining virus signatures should be easy. Finally, the anti-virus solution should not get in the way of users until it is necessary.

Conclusions

In mixed environments, it will probably not be possible to resolve all these issues with a single package as a core product – some issues may have to be resolved outside the scope of anti-virus software. For example, it may be possible in a mixed PC and *Macintosh* environment to use the same scanning engine on both machines, and to have them both connected to servers such that the virus updates are sent to the different machine types automatically.

However, using commonly-available distribution tools, this issue can be addressed quite simply, and indeed may give increased flexibility throughout an organization which may wish for a different scanning engine on the server from that on the clients. This obviously addresses the problem of multiple virus scanners to minimize the potential of one scanner missing a virus.

Finally, it is imperative that you keep up to date with information available regarding the latest threats and virus prevention techniques. Any corporate virus strategy needs at least one subscription to *Virus Bulletin*!

Phil Crewe has been a member of *VB's* advisory board since its inception in 1989, and has written many articles in the past.