



Remote Workers' Security: your IT's Achilles Heel?

*Extending effective virus
management to employees
beyond the firewall*

by
Mark Lillycrop
Chief Analyst
Arcati Research
mark@arcati.com
www.arcati.com/ml.html



Remote Workers: the Corporation's Achilles Heel?

Remote working has radically altered employment practices within the new economy, but the benefits (such as employee flexibility and increased productivity) need to be balanced against the problems of managing teleworkers. In particular, companies need to make sure that remote PCs remain properly protected against computer viruses and other security exposures. Software tools such as Sophos's new Remote Update are tackling this problem head-on.

Remote working and telecommuting are growing fast. The simple fact is that more and more office-based knowledge workers want to work from home, and their employers are generally happy to let them do it. This creates an enormous challenge for the IT departments that manage remote workers' computer resources and virus protection, an issue that needs to be addressed urgently.

Nearly 30 million Americans (around 20% of the workforce) now work from home at least one day a week. Two-thirds of *Fortune 1000* companies reportedly have telecommuting programs, half of which were instituted in the past two years. What's more, this is an international phenomenon, and in many countries the teleworking population is growing fast:

- In the UK, the Office of National Statistics recently reported that teleworking is up 70% from five years ago, with 7.4% of the entire workforce working from home at least one day a week. Although this is less than in Germany and France, other European countries have an even higher proportion of the workforce working from home.
- The Australian Bureau of Statistics claims that around 8% of the New South Wales workforce are teleworking.
- In Japan, the Telework Association estimates that the number of employees working at least one day a week from home has risen from 0.81 million in 1996 to 2.46 million in 2000 (expected to hit 4.45 million in 2005).

The benefits are clear to see: for the employee there is less mind-numbing commuting, less stress, less pollution of the environment, a more comfortable working environment, more job satisfaction and increased flexibility for childcare. For the employer, the advantages are equally clear to see, with productivity at the top of the list. JD Edwards reckons that its teleworkers are



Arcati Research Bulletin

20-25% more productive than its office workers, while American Express claims that teleworkers can produce 43% more business than office workers.

Productivity increases are always important, but so is reducing property costs. International telecommunications company BT has 7,500 employees without a desk, and the company has calculated a cost saving of £180 million (\$290 million) since its homeworking strategy started in 1992. In view of the current economic climate, savings of this size are difficult to dismiss.

Of course, a large proportion of remote workers are not home-based. Many companies have teams of mobile workers who spend much of their time on the road or in the air, based in hotels or temporary accommodation. Many 'road warriors' rarely see the office where they are officially based. Indeed, there is an increasing trend for employers to offer 'hot-desking' facilities to mobile workers, allowing them to use space at the nearest branch office for as long as they need it. Hot-desking provides exceptional economies for large organizations, and many have been able to achieve dramatic improvements in desk occupancy (and corresponding reductions in the amount of office space required) in this way.

The challenge of supporting remote workers

What most remote workers share is a need to access the corporate IT resources that their office-based colleagues take for granted. In recent years, teleworkers have been equipped with fast laptop PCs, network-enabled PDAs, and the latest generation cellphones, all to help them communicate more effectively with their employers, customers, and business partners. Those who have the use of hot-desking facilities can usually access company networks and data relatively easily, but those who work from home and do not have a company-configured computer often use their own equipment, sharing non-standard PCs and phones with other members of the household. Home-based employees are also more exposed to security problems: they rarely have a firewall in place, and they are particularly liable to attract viruses introduced through chat rooms, peer-to-peer computing, Web-based e-mail, and other technologies that are strictly controlled (or restricted) within the corporate setting.

For the IT manager and network administrator, the sheer diversity of technology in use by remote workers presents a real challenge. Quite apart from being able to access the information they need, and maybe update centrally held records, these employees also need similar technical support to office workers – they need the same software updates, applications, security utilities and corporate documents.

But with unpredictable network access and line speed, keeping remote workers in sync with corporate systems can be an uphill struggle. Because of the time and effort involved in finding a fast, reliable network connection, teleworkers will



Arcati Research Bulletin

often delay software updates until the next time they can bring the laptop into the office; or they put off the upgrade indefinitely, until their job becomes impossible without the necessary software.

Anti-virus: software that just won't wait

In many cases, delaying a software update will have little impact on the business or the employee. Lacking the latest features of a new application release, for example, may not matter in the short term. But one software update that is time-critical is virus protection.

Virus control has become a way of life for commercial organizations. With some 80,000 individual viruses in circulation, and 800 new ones appearing each month, it has become essential for every company desktop to be protected, to ensure that the business does not suffer a major security incident or lose critical data. Virus outbreaks almost always involve considerable cost and disruption to their victims and they can cause irreparable damage to the company reputation and brand. Moreover, with legislation such as the Health Insurance Portability and Accountability Act (HIPAA) in the USA coming into play, virus outbreaks can lead to criminal charges against senior managers if sensitive data is damaged or malevolently passed into the wrong hands.

Remote workers (who often have a less than desirable approach to system maintenance) are particularly exposed to virus threats. Most companies have a procedure in place for updating their anti-virus software regularly, and many make efforts to ensure that teleworkers treat virus protection seriously. If access to the corporate LAN is impractical, for example, remote workers are

	Local workers	Remote workers
Firewall protection?	Yes	Rarely
Fast, predictable connection speed?	Yes	Rarely
Secure e-mail?	Yes	Sometimes
PC admin rights?	Rarely	Usually
Sole use of target PC?	Usually	Sometimes

Common differences between local and remote PC environment



Arcati Research Bulletin

often referred to the Web site of the anti-virus software provider, so that they can download new identity files directly. However, this process can be somewhat hazardous. Apart from the size of the downloads (sometimes more than 4MB, not practical over a 56K dial-up line), a virus update file can be incompatible with other applications on the end user's machine, or the wrong download can be initiated from the vendor's Web site.

Unless the corporate network administrator can monitor the state of virus protection software on remote workers' machines in the same way that he or she manages permanently network-attached PCs, and can oversee the progress of all updates directly, there is scope for serious errors to occur. But now we hit another problem. Home workers generally have administrator rights over their own home machines, and may even have similar rights on company-sponsored machines; and the chances are that they also have a non-standard configuration. This makes life very difficult for the administrator attempting to update security settings for all end users.

Remote workers: responding to new requirements

Clearly there is a real need for suppliers of anti-virus software to adapt to the changing needs of the marketplace, and to make their products as accessible to road warriors and teleworkers as to office-based employees. For some suppliers, this represents a real challenge, as many existing offerings are optimized for a tightly managed LAN/WAN environment with fast and predictable line speeds.

Re-engineering anti-virus tools for the remote workforce is no small undertaking. In particular, products must offer:

- flexible access to updates, via both Internet and corporate LAN/WAN, so that files can be obtained via the most appropriate route.
- frequently issued virus update files with 24 hour, 365 days a year availability.
- small file sizes, allowing teleworkers and hot-deskers to obtain updates with a minimum of fuss and delay.
- a single, corporate repository of virus information and downloads, to avoid the need for remote workers to obtain (possibly incompatible) update files from the vendor's Web site.
- a wide range of supported clients, to mirror the requirements of heterogeneous enterprises.
- sophisticated management tools for the network administrator, so that he or she can monitor the status of any connected client device, local or remote.

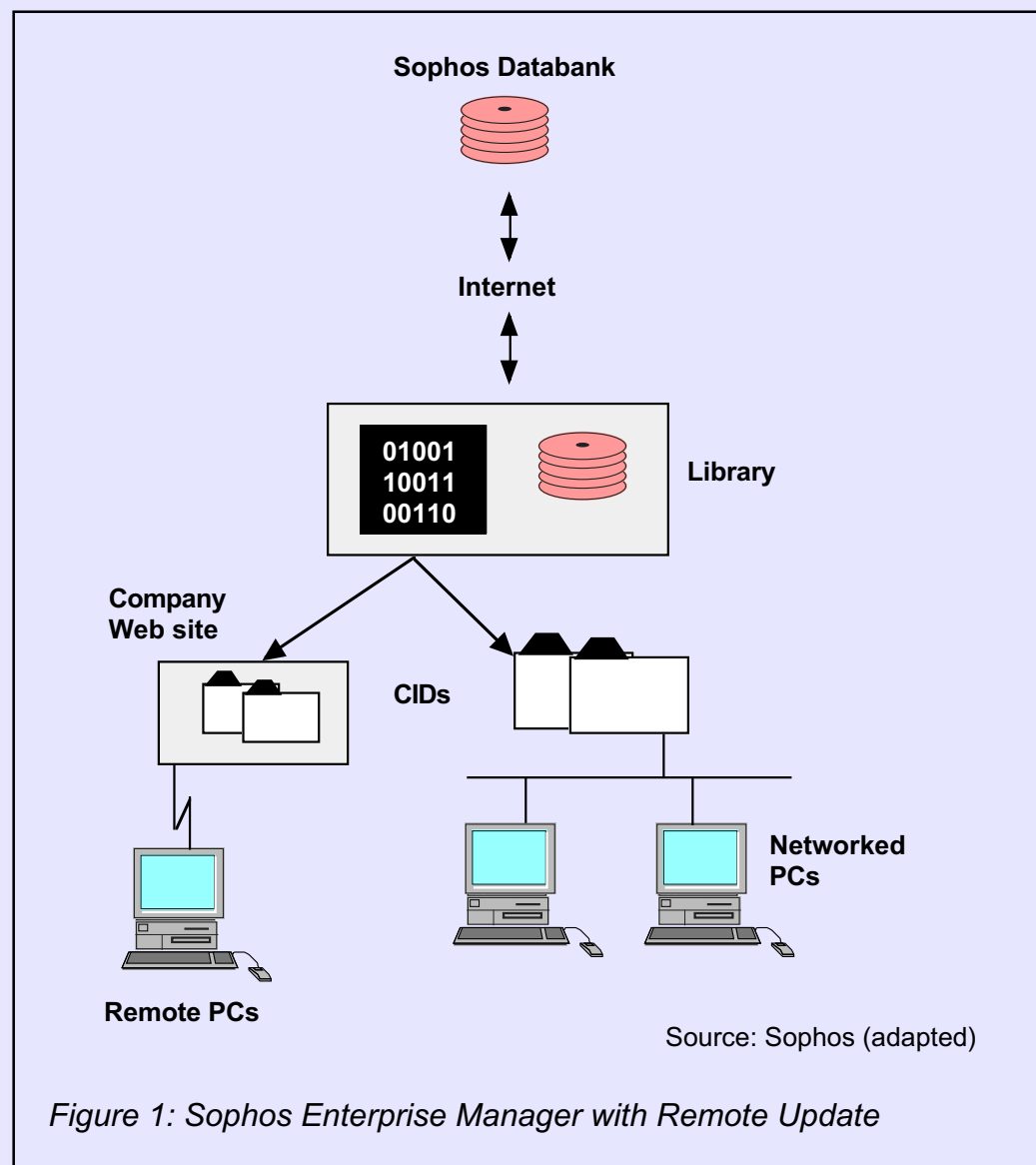


Arcati Research Bulletin

Remote Update: returning control to the network administrator

One company that has recently addressed these issues is Sophos, with the new Remote Update tool. Remote Update extends the function of Sophos's well-established Enterprise Manager for distributing Sophos Anti-Virus (SAV) software and virus identity files. The benefit of Remote Update is that it puts control of remote virus management back into the hands of the network administrator, and gives teleworkers a variety of ways to download regular updates from a corporate server, with a minimum of time and effort.

Once Remote Update is installed on the user's PC, he or she can access the employer's Central Installation Directory (CID) via a simple Internet connection (or via the company LAN/WAN – if one type of connection fails, the other will be attempted automatically). A CID is a repository of anti-virus software





Arcati Research Bulletin

updates and new virus files, automatically downloaded from the central Sophos Databank and stored in a library maintained by Enterprise Manager for updating the CIDs. The remote PC updates directly from a local CID, and the process can either be initiated by the remote user when convenient, or can be set up to occur automatically (see Figure 1).

This choice of HTTP Internet or LAN/WAN connections makes Remote Update equally suitable for the remote user on the move or the teleworker restricted to Web access by home working. Likewise, the small update file size offered by Sophos is a great asset to remote workers. With virus identity files coming out at 1 to 2KB, and even the monthly SAV product upgrade amounting to no more than 200KB on average, few teleworkers could justify a delay in downloading the necessary files on the grounds of slow line speeds.

Not only are the Remote Update downloads small; the application itself can also be configured to restrict the amount of bandwidth it uses, to limit impact on other applications. Indeed, manageability is one of Remote Update's great strengths. When connected to the LAN, the status of individual Remote Update users can be monitored via another Enterprise Manager tool, SAVAdmin, so that the network administrator knows immediately if there are any deficiencies in the connected user's virus protection.

The use of the CID as a central download repository is a real asset. As explained earlier, it is often undesirable to direct remote users to a vendor's Web site; standard access to the company's own Web site or network is a far better approach in managing software distribution to employees.

Finally, Remote Update is available for a broad range of client devices – Windows 95/98/Me, and NT/2000/XP are all supported. This gives it an admirably wide desktop reach, and should make it suitable for the needs of the vast majority of organizations.

Bottom line

In view of the burgeoning number of remote workers worldwide, and the pressing need to keep anti-virus tools up-to-date on employees' PCs, we would recommend that all businesses with staff working outside the firewall look very closely at their requirements for remote management products. Remote Update would be a good place to start.

Mark Lillycrop is Chief Analyst of Arcati Research Ltd and an Associate of Valley View Ventures, Inc. For further information on this paper or Arcati services, visit www.arcati.com/ml.html or e-mail mark@arcati.com.