Computer viruses

2001 was the year of the virus. The popular press has reported now-familiar virus names – "ILoveYou", "Melissa", "Code Red", and more recently "Nimda" ("admin" spelt backwards). Computer viruses are the electronic equivalent of vandalism. However, they weren't always that way – originally, they were humorous pranks. An example that dates from the late 1980s was an Apple Mac virus that activated itself by having a small man run across the computer screen, grab your mouse pointer and then run off with it.

Although computer viruses once inhabited only program files, they now can be found in system files, word processing documents, read-only published (PDF) documents, and emails. There are also viruses that can be activated merely by accessing infected Web homepages. Practices that use Microsoft's Web server software solution – IIS – will be well aware of the large number of faults in this software that allow viruses to infiltrate and damage file servers.

There are more than 55,000 known viruses, and new ones appear daily. Viruses have two predominant characteristics – they jump from one computer system to another in the absence of any deliberate action by a computer user, and they most often wreak havoc when activated. Common types of viruses include "Trojans", which hide themselves in other programs, and "worms", which burrow into systems through holes in security. There are "sleepers" which find their way onto a computer and lie dormant until some identified event or significant date, and "denial of service" viruses, which find their way onto a large number of different computers and then send a stream of uninterrupted garbage communication data to one specific organisation.

Technology "To do" List

- Assign responsibility for keeping virus "definitions" up-to-date on all practice computers.
- Confirm that staff are aware of the virus dangers of opening unsolicited emails, especially those with attachments.
- Ensure that your practice is protected from incoming email viruses.
- Acquire virus protection software that automatically updates itself, performs regular unattended scans, and traps viruses in any sort of document.
- Keep your virus software maintenance paid up.
- Have a strategy in place for easily restoring files or computers that have been damaged by viruses.

TYPES OF DAMAGE

In most practice environments, viruses can carry out damage at a number of levels. Firstly, they can cause files or whole hard disks to be deleted. This is sometimes referred to as the virus "payload". Secondly, there is financial damage as a practice burns up valuable staff time in detecting and eradicating a virus, and in possibly repeatedly paying for IT consultant time in virus removal. At a third level is the damage done to a practice's reputation as it unintentionally sends some or all of its clients virus-infected files. Reminding a client of the disclaimer that appears at the bottom of each email does nothing for client relations when the client has suffered avoidable business disruption.

A TYPICAL STORY

A practice recently received a number of phone calls and emails from clients indicating that they had received virus-infected documents from one of the associate solicitors. The phone calls ranged from helpful to irate. The staff member responsible for the practice's computer systems was baffled. The email server had appropriate virus protection, protecting incoming emails. The firm's file server had a similar level of protection. The associate's computer had resident virus protection software. So what had gone wrong? It transpired that the staff member responsible for manually updating virus protection for the associate had not done this for about two weeks and, in the meantime, the associate had used a diskette on her notebook that had also been used on her son's computer at home. The diskette contained a virus that was less than a week old.

THE FOUR PILLARS

The good news is that minimising virus damage is relatively straightforward. There are four "pillars" of a structured comprehensive virus protection plan. The first is ensuring that each computer, including the practice file server, has current virus protection software installed, which is resident at all times, checking documents and programs as they are used. This software should scan all files for viruses on a frequent, regular, unattended basis. The second pillar is to ensure that this software updates itself without manual intervention on a daily basis from the software vendor's website. Each update should also be propagated automatically to all practice computers daily. The third pillar is the additional implementation of protection software that sits at the email "gateway" of the practice to trap viruses, or even suspected viruses, before they make their way through the firm. The final and most important pillar is ensuring that there is a high level of staff awareness and vigilance in relation to virus prevention. This includes ensuring that files don't enter the practice on diskettes without being virus-checked first, or via unauthorised notebook usage. ■

itcolumn@liv.asn.au

Adam Reynolds is a principal of Proficio, an independent IT consulting firm.

For more I.T. in practice information, see the contributions of the Law Institute Legal Practice Management Committee and IT special projects department at www.liv.asn.au/sections/lpms_it/.