# Electronic Epidemic:

## The Age of the Computer Virus

*Vanessa Bleyer, Lethbridges Barristers & Solicitors*



***As a consequence of having IT experience, it is not unusual for me to hear cries of distress coming from my colleagues when their computer is not behaving itself. The problem is usually fixed with a few clicks of the mouse! However, on 13 August 2002 when responding to yet another colleague's call for help, I witnessed computer conduct the like of which I had never seen.***

An offensive message appeared on the computer screen directly after emails were sent to each address in the computer's address book, incorporating parts of confidential documents saved elsewhere on the computer. I had no time to gather enough data to understand the source of the problem, as vital operating system files vanished before my very eyes. Within a few minutes, most computer files were deleted and the system crashed. I can only suppose it was either a vicious virus or a malicious attack.

We have become accustomed to emails carrying viruses. They threaten what should be the privacy of our personal computer. An activated virus has the potential to cause either huge damage or very little damage. Governments worldwide have acknowledged the threat. So what is being done in Australia?

Australia's legislative response (which could also be seen as a security reaction to September 11) is the *Cybercrime Act 2001* (Cth). It creates seven new computer offences to "remedy deficiencies in the existing laws".[1]

It is now an offence to cause unauthorised impairment of electronic communications to or from a computer.[2] This offence is particularly designed to "prohibit tactics such as 'denial of service attacks'"[3], where, for example, a website receives a corrupt message causing the computer server to crash. The maximum penalty is 10 years imprisonment.

It is also an offence to possess or supply data or programs that are intended for use in the commission of a computer offence.[4] This offence is designed to "cover persons who possess or trade in programs and technology designed to hack into or damage other people's computer systems".[5] The maximum penalty is 3 years imprisonment.

But are these strict new penalties deterring anyone?

The number of prosecutions for computer crimes is very small. It remains to be seen whether the new penalties will deter anyone, especially as recent figures show that offences are on the rise.

The volume of computer crime in Australia is growing rapidly. Computer crime incidents in 2002 are double the number of incidents in 1999.[6] Eighty-nine percent of recent occurrences were the result of external attack,[7] that is, an attack originating from an extraterritorial source. Indeed, the most renowned strikes emerged from Taiwan in June 1998 (the *Chernobyl* virus), from the United States in March 1999 (the *Melissa* virus), from the Philippines in May 2000 (the *I Love You* virus) and from the Netherlands in February 2001 (the *Kournikova* virus). These incidents caused massive financial loss, with the *Melissa* virus resulting in $80 million damage and the *I Love You* virus causing a less impressive $10 million damage.[8]

Most computer users try to avoid potential virus damage by installing anti-virus software. However, this is not always enough. Viruses are created to exploit vulnerabilities in operating systems or applications. Only daily updated prevention strategies come close to providing protection.

Just as people found they needed locks on the doors of their houses to keep intruders out, the same now applies to computer systems. The problem though is that locks on computers do not last; in fact they are obsolete by the time they are installed. As a result, 43% of Australian organisations are willing to hire ex-hackers[9] to gain insight into their electronic enemy and deploy security strategies.

So what is needed to protect us from computer viruses? Anti-virus software is, of course, a good start. Legislation with some teeth is helpful as it might deter would be hackers and intruders. It may be time to consider combat techniques that roam where viruses roam. Viruses weave their way through the global network that forms the Internet, whereas anti-virus software only creates a barrier at the user's machine. An anti-body that moves through the Internet may assist, however who could produce such technology? Perhaps we need to rely on intruders themselves to work with us in an effort to understand and pre-empt what their contemporaries may unleash!

In the meantime old-fashioned vigilance is best. Be alert to the potential consequences of opening an attachment – no matter how persuasive the text of the email!

For more information, the 2002 Australian Computer Crime and Security Survey can be obtained from the New South Wales Police web site at **www.police.nsw.gov.au**. The *Cybercrime Act 2001* (Cth) can be obtained from the Australian Legal Information Institute web site at **www.austlii.edu.au**. ●

---

**VANESSA BLEYER** is the former Director of the Webology group of Internet Companies. She is currently an Articled Clerk at Lethbridges Barristers & Solicitors, a firm specialising in criminal law.

1 Daryl Williams, Second Reading Speech, *Cybercrime Bill 2001*, 27 June 2001, page 1.
2 Division 477.3, *Cybercrime Act* 2001 (Cth).
3 Daryl Williams, *Op Cit*, page 1.
4 Division 478.3, *Cybercrime Act* 2001 (Cth).
5 Daryl Williams, *Op* Cit, page 2.
6 Australian Computer Emergency Response, Deloitte Touche Tohmatsu and the New South Wales Police, *2002 Australian Computer Crime and Security Survey*, page 1.
7 *Ibid.*
8 Tim Burmeister, Presentation on behalf of the Defence Signals Directorate at the *eSecurity and eCrime* Seminar, 19 July 2001.
9 Australian Computer Emergency Response, Deloitte Touche Tohmatsu and the New South Wales Police Force, *2002 Australian Computer Crime and Security Survey*, page 1.