## DATA SECURITY

Security threats can present themselves in direct form, through hackers (and as far back as 1997 it was estimated that the Internet is hacked into every 20 seconds) and through indirect information systems penetration (Mitchell et al. 1999). These indirect threats occur in four major types:

- **Worms:** a worm is a program that, once established, can spread copies of itself throughout a network
- **Trojan horses:** these are also programs that appear to be carrying out a non-malicious activity which, when activated, reveal their true destructive intent
- **Logic bombs:** these are programs activated by a specific event
- **Viruses:** like a medical virus, these 'infect' other programs.

A popular route in for these invaders is via e-mail — and they don't always come in as attachments. The header message is usually friendly and intriguing, encouraging the user to believe that it is a message from a friend or admirer.

The results of these attacks can range from the irritating and embarrassing to the devastating and can include the destruction of data or its modification, interception or fabrication by unauthorized personnel.

### The Melissa virus

Melissa was an e-mailed virus that emerged from nowhere to overwhelm commercial, government and military computer systems, leading the FBI to launch the biggest Internet manhunt ever.

Melissa affects Word 97 and Word 2000 documents. If launched, this virus will attempt to start Microsoft Outlook to send copies of the infected document to up to 50 people in  Outlook's address book as an attachment.

Viruses often spawn ever more dangerous variants. The ‘I Love You’ virus, which appeared in Spring 2000, had 50 variants by October that year.

The growth of e-commerce has seen a surge in opportunities for business fraud and other security issues.

## METHODS OF DATA SECURITY

There is a range of methods of varying complexity that organizations can use to protect themselves from unauthorized access. See Table 1.

**Table 1. Data security method**

| *Method* | *Description* |
|---|---|
| Data encryption | Scrambles the data before and during transmission. Use this method when data protection is important |
| Key management | Acts like a 'key' to access encrypted data. Maximum protection to protect data from unauthorized parties. Use in conjunction with data encryption |
| Digital certificate | Like a watermark on a bank cheque – this is an electronic ID card that establishes your credentials when doing business on the Web |
| Firewalls | The first line of defense from the outside. Acts as a security guard for the company's internal network, filtering all incoming traffic from the Internet. A good tool for networks connected to the Internet |
| User authentication | Verifies the identity of the user. Could also be used to restrict access to certain resources within the network. A requirement for any user accessing a corporate network |
| Intrusion detection system (IDS) | Scans the network for abnormal activity and security breaches. A minimal requirement for any corporate network |
| Virus detection | Scans the network data for viruses, providing both prevention and cure if updated regularly. One of the best defenses for data protection |
| Virtual private networks (VPN) | A secure private data network developed on a public data network like the Internet |