DEPARTMENT OF THE PARLIAMENTARY LIBRARY

INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

RESEARCH NOTE

2003–04
No. 6, 11 August 2003

Computer Crime and Compromised Commerce

Computer Security

Computer security has become a growing problem, with crime and viruses and hacking reportedly reaching epidemic proportions. The Insurance Council of Australia estimates that cyber-crime costs companies worldwide around about $3 trillion each year, with around 67 per cent of computer users affected in some way. The areas of greatest impact are laptop theft, data or network sabotage, virus and Trojan infection, computer fraud, denial of service attacks and excessive network resource consumption through external scams.

Electronic or E-security is concerned with areas of:

- confidentiality – information should only be available to those who rightfully have access to it
- integrity – information should be modified only by those who are authorised to do so, and
- availability – information should be accessible to those who need it when required.

The Parliamentary Joint Committee on the Australian Crime Authority is inquiring into cyber-crime, pornography and infrastructure threats. There are other aspects:

The Threat Within

While there is no doubting the size and severity of the security problem facing the IT sector, a lot of counter action can come from within the industry and computer users. A large part of the security threat comes from disgruntled or former employees with the means to access computer systems in order to perform their criminal deeds. The screening and education of staff is an important process in helping to ensure security as is regular password changes and system access evaluations. Technology can assist the process with new security systems offering biometric or fingerprint identification but the weakest link remains those with access to the control of these very techniques. Identity theft has become a fast growing crime too.

A relatively new threat has arisen from the growth of wireless technology that may expose corporate networks to external eavesdropping and entry. While flexible and cheaper than cabled systems, wireless systems can be vulnerable to external attack.

E-crime Policies

Under the e-security national agenda, the Commonwealth Government has stepped up efforts to protect the national information infrastructure and increase public confidence in the security of the on-line environment. This involves key agencies such as the Attorney-General's Department, the Australian Federal Police, the Australian Security Intelligence Organisation, the Defence Signals Directorate, and the National Office for the Information Economy (NOIE) in joint operation.

These agencies support the Critical Infrastructure Protection Group, the Gateway Certification Guide and other policy initiatives.[1] The new Australian High Tech Crime Centre, representing all law enforcement agencies, may help to combat cyber-crime and fraud. It is also understood that the Office of the Federal Privacy Commissioner will act to uphold the National Privacy Principles with respect to the collection of personal and consumer information. This relates to the distribution of unsolicited e-mails to individual consumers.

Standards Australia have recently launched new national guidelines to help organisations combat electronic crime.[2]

Spam

Unsolicited bulk or junk e-mail, known colloquially as spam, has become as familiar and pernicious to Internet users as telemarketing calls over the home telephone or pamphlets and unaddressed materials in our private letterboxes. Perhaps one difference is that spam is more readily and cheaply spread worldwide and does not face cost barriers of printing and physical distribution or of employing call centre staff to market and advertise goods and services.

A more sinister aspect is that much spam involves black market scams, fraud and unedifying activities. Spam has also become a traffic burden on the Internet, taking up capacity and with pop-up messages that are annoying. Major spam categories are promotions for sexual sites, finance and products.

Now it seems that between a third and a half of all e-mail traffic may be spam! In April this year, NOIE estimated that the volume of spam had reached 35 per cent of e-mails and that this was increasing by 300 per cent each year. In May, the IIA (Internet Industry Association) reported that figures from the USA suggested the volume of spam was increasing at a rate of 18 per cent per month. Other reports suggest that the volume of spam is approaching 50 per cent of all e-mail.

NOIE reported that the worldwide cost of spam had been estimated as $18.4 billion. The costs fell across all sectors of Internet usage, from the businesses with employees and systems managers frustrated at the ever increasing task of reading and filtering spam, to the Internet Service Providers themselves attempting to filter spam and shield their customer from the nuisance.

There has been a suggestion that charges apply to e-mail senders. This would make the distribution of bulk e-mail a costly exercise and help thwart its spread. However, committed Internet users oppose any such cost imposition and spammers may ignore payment demands.

Technical means to control spam include blacklisting, payment, filters and authentication. A technical mechanism might be the wide use of TEOS (trusted e-mail open standard). TEOS is a system that imposes some levels of trust on e-mail senders. The local IIA has offered a free trial of anti-spam filters.

Put Spam in the Can

Local action against spam includes a new program by the Australian Competition and Consumer Commission teaming up with foreign law enforcement agencies to attempt closure of open relays in many countries. Relays are servers that allow unregistered computer users to send e-mail through them. There have supposedly been few open relays found in Australia.

While this may help control the 2.5 per cent or so of spam created in Australia, the bulk originating overseas may prove elusive. Notably, there is a suggestion that Australia produces a volume of spam that is proportionately higher per person than in the USA and so this deserves local action.

The ACCC advises consumers not to open messages from unknown persons, never to respond to unsolicited e-mail (including unsubscribe options), to delete all spam e-mails immediately and to use a spam filter and anti-spam tools.

The American State of Virginia now has legislation banning spam activity while California requires all bulk e-mail to have the word ADV in the subject line field. Meanwhile, special Internet listings such as that found at www.spews.org attempt to out known spam locations.

Australia's existing content-based and privacy legislation may form a basis for further anti-spam measures. The federal government has announced its intention of creating new anti-spam legislation, better enforcement, industry collaboration, filtering software and consumer education. Note that separately, Parliament has passed two pieces of legislation that expressly address the issue of 'cyber-terrorism' or 'cyber-crime'.

In a related move, a new industry code now exists to help protect mobile telephone users from SMS (short messages service) spam content. The code seeks to address industry and community concerns about the delivery of unsolicited and intrusive SMS information.

Anti-virus software and anti-hacking firewalls also form part of the modern computer users' armour against intrusion and crime. There are many effective programs around for little if any cost at all to install.

Anti-Spam Legislation

The federal government proposes measures to control spam such as:

- national laws banning the sending of commercial e-mail without end–user consent
- a requirement for all e-mail to contain the senders name and physical and electronic addresses
- implementation of industry codes of practice
- Internet Service Providers to make available client filtering options at reasonable user cost
- international collaboration to develop anti-spam guidelines, and
- information campaigns to raise spam awareness and how to deal with it.

Legislation may be expected in Parliament by late 2003.

Tips to Avoid Spam

Here are some hints to help computer users cope in the meantime:

- guard personal e-mail addresses and do not provide them on forms or surveys unless warranted
- do not respond to spam at all, even to ask for removal from the mailing list
- choose a unique e-mail address perhaps with random numbers and letters rather than a more standard form
- in posting to newsgroups, disable your e-mail address by adding words to it
- use a false e-mail address in web-based news groups
- report spammers to your Internet Service Provider, the ACCC or authorities, and
- use e-mail filter software.

Consumers may find it difficult to distinguish between spam and more legitimate forms of marketing on-line. Public education and industry initiatives will win the spam battle. Software giant Microsoft has now committed to legal actions against spammers. And in a curious twist, even hackers are joining the war, cursing the barrage of spam.

---

1. See: http://www.cript.gov.au/ & http://www.dsd.gov.au/infosec/.

2. See: https://www.standards.com.au/NEWSROOM/NEWS%20RELEASE/2003-08-12/2003-08-12.HTM

Matthew L James and Brian E Murray, Science, Technology, Environment and Resources Group, Information and Research Services.

ISSN 1328-8016