FEATURE

IT Security Breaches: The 1994 NCC Survey

Chris Hook,
NCC Services Limited

Earlier this year, the *National Computing Centre* (*NCC*), with the support of the *DTI* and the *ICL*, carried out its second UK survey of IT security breaches and failures. Its aims were to provide information on a range of IT security issues, including attitudes to IT security, the incidence of security breaches, and case study examples.

The Participants

Responses were received from 832 organisations of all sizes, and from most industry sectors. Almost 60% were from organisations employing under 500 staff (see Table 1 below), an encouraging indication that smaller companies are beginning to take the problems of IT security seriously.

Over 80% of respondents reported at least one significant breach over the past two years. The most prevalent incidents reported were equipment failure (47%), power failure (47%), viruses (34%), network failure (31%) and theft (29%). In this article, I shall concentrate on those results affecting the logical security of PCs; in particular, those relating to viruses.

In the two years since the last survey, reported virus infections have increased by 250%. Two hundred and seventy-nine respondents (34%) reported a total of 1,029 incidents: in our first survey (published in 1992), 142 respondents (16%) reported 410 incidents.

Part of the reason for this increase may be, one hopes, due to a greater awareness of the disruption a virus infection can cause, although whether this increased awareness has been translated into positive action to prevent incidents from occurring is perhaps debatable.

No of employees	No of respondents	% of total
Under 100	197	23.7
100 to 499	301	36.2
500 to 999	114	13.7
1000 to 4999	151	18.1
5000 to 10000	24	2.9
Over 10000	35	4.2
Not known	10	1.2

Table 1: Responses by size of organisation. As can be seen, most respondents' companies have fewer than 500 employees.

Policy Implementation

An analysis of the survey showed that formal security policy for IT systems was being implemented by 57% of those who responded, and 51% had formal procedures for PC security. A further 37% had ad hoc PC security procedures.

There were notable variations within different industry sectors: two-thirds of the Finance sector had formal procedures for PC security, compared to only 38% of the Education and Research establishments, although 54% of these claimed to have ad hoc procedures.

Similarly, 66% of organisations employing over 10,000 staff had formal PC policies, whilst under 50% of those employing less than 500 had such measures in place. Controls and procedures implemented by various companies are described in the table below.

Control	Automated Procedure	Formal Instruction	Guidelines & training	Monitoring	Any of These
Backup	36%	35%	0%	16%	94%
Anti-Virus	39%	39%	27%	23%	88%
Authorised Software	13%	59%	24%	24%	91%

Table 2: Controls implemented for PC users (percentage of respondents).

The majority of respondents addressed the areas of data backup, anti-virus procedures and installation of only authorised software in some way, though few of them monitored compliance with the procedures.

Even in the very largest companies (those employing over 10,000 staff), the figures for those monitoring compliance with procedures for backup, anti-virus and installation of authorised software were surprisingly low; only 26%, 31% and 40% respectively.

Respondents were asked to indicate which types of incident, in their opinion, presented the greatest threats to their IT systems. Alongside equipment failure, virus infections were rated by all classes of respondent to be the most notable threat, with 31% rating them as a major threat and 53% a minor threat. This view was particularly prevalent amongst larger organisations. Despite this, only a minority of respondents (including the largest) had issued formal guidelines on virus protection, or included anti-virus procedures in their staff training.

It would seem that whilst there is an awareness within organisations of the threat from virus infections, many have failed to take sufficient steps to counter it (the 'It won't

happen to me' syndrome). Ultimately, over one-third of respondents had suffered disruption to their systems due, in many instances, to repeated virus infections (average nearly four per respondent).

Virus Incidents

Further information was given by some respondents about 109 viruses, two-thirds of which occurred during 1993, often at a cost of many thousands of pounds per incident. Networked PCs were affected in 52% of incidents and standalone PCs in 64%. Personal systems were mainly affected in 62% of incidents. Fifty percent of departmental systems were also affected, in comparison with only 9% of corporate systems.

In half of the cases, more than one day was required to recover all facilities fully, with 14% taking more than a week. The majority of respondents' overall assessment of the impact was that it was minimal or easily absorbed, but in 11% of incidents it was considered significant.

In a number of cases, it was found that backup copies would not restore when needed, or were not up to date. For the greater part, investigation costs greatly exceeded the cost of actual damage caused: this is one reason why every virus, no matter how innocuous its payload, must be treated seriously.

Cost	Major	Minor	Not significant
Investigation/checking	22%	70%	8%
Long-term remedies	11%	40%	49%
Reconstruct software	4%	52%	44%
Loss of business	4%	11%	85%
Reconstruct data	2%	42%	56%

Table 3: Major and minor costs arising from virus infections (percentage of incidents).

Only 20% of respondents who reported a virus infection in detail had costed the incident, but of those, investigation costs of between £10,000 and £50,000 per incident were not uncommon. The highest reported cost was £100,000 to investigate and remove a virus which had affected 200 PCs on three networks. The source was an infected anti-virus software disk (presumably not write-protected)!

Where Infections Originate

The sources of infection were many and varied, and by no means confined to end-users loading illicit software from their own disks, although this was common. We found that viruses infiltrated systems in many different ways: for example, a distribution company strongly suspected a small PC interface company, contracted to carry out some work for them, of introducing the Joshi virus. In a construction company, a virus was found installed on a new Spanish-built PC. In a government department, CMOS1 was brought in on a portable PC used by an officer on a visit to Spain, and a disk brought into a training course by a delegate was infected with Form. A PC in a manufacturing company, after being checked by an outside engineer, became contaminated with Michelangelo.

The tales are endless, but others worth recounting include that of an organisation which had made 34 of its IT staff redundant. It was subsequently discovered that a number of blank disks had been infected with Form and replaced in their boxes. Nine PCs out of 40 on a network were affected when the disks were used and the company estimated that the cost of lost business, investigation and disruption over a twelve-day period amounted to £50,000.

"probably more than with any other threat to IT, protection from viruses lies first and foremost in the hands of the end user"

A major retailer was continually re-infected over a four month period by Form. The source of the infection was eventually traced to a software house which was supplying the company with a bespoke system. In total, about 70 'man-days' of effort were expended in investigating the outbreaks at the company's computer centre and at its head office, and a disk scanner had to be hired. The cost was put at £10,000, in addition to the considerable ill feeling amongst staff who were blaming each other for the continual re-infection. The company now has a mandatory disk authorisation system installed.

In a similar case, a virus was introduced to several machines in the area office of an insurance company from a master floppy disk purchased from a software supplier. The virus was then transferred from the original machines to several other machines via floppy disks. Several thousand of these disks then had to be checked. Whilst most people could start work again within a day, some users had to wait up to a week before being able to use their systems. The incident cost the company between £1000 and £5000. The software supplier's only concession was a letter of apology.

Overall Costing

Respondents who had not costed an incident when it occurred were asked to estimate its likely cost (under £1000, £1000-£4999, £5000-£9999, £10,000-£50,000, or more than £50,000). The majority of incidents were estimated to have cost under £1000, but 23% were thought to be between £1000 and £4999, and 2% at over £50,000, although costs had not been itemised at the time. In addition to immediate costs of disruption and investigation, the long term costs (e.g. installing anti-virus software and training users) were estimated at over £5000 in nearly 20% of all incidents.

Based on details of the actual and estimated immediate costs supplied, most virus infections (approximately 70%) cost less than £1000. However, 20% of incidents detailed cost between £1000 and £5000, and 10%, over £5000. The average immediate cost was £3922. If the results of respondents are representative of the United Kingdom as a whole, we estimate that the annual cost of virus infections could be circa £128 million.

Standards and Procedures

What, then, is going wrong? We asked those respondents who had reported details of virus infections whether or not they had relevant standards and procedures in place: 87% said they had, and 76% said that their staff were adequately trained in their use. However, when asked if these staff were adhering to the standards when the infection occurred, 75% said they were not.

This seems to be a common problem with all types of logical breaches of security. End users appear to be able to grasp the physical dangers to their PCs (fire, theft, equipment failure for example), but are totally unable to understand the concept of these invisible things called 'data' or 'software' and the threats which endanger them. This is reflected in the type of incidents encountered.

"investigation costs (for virus infections) of between £10,000 and £50,000 per incident were not uncommon"

In one case, a company made regular backups of its free-standing PCs by taking a portable tape drive to each workstation in turn. The backup software was loaded from a floppy disk each time. The disk was not write-protected and became infected with a boot sector virus which was present on the PC of a senior manager, whose cavalier attitude to virus protection was well known. Over the following three-day period, other PCs became infected, as the backup software was loaded on each in turn. Once the infection was discovered, it took a further three days to clear the infection from all PCs in the company.

In another example, Form infected a disk fax and was unwittingly distributed to multiple sites of a government department. It was picked up by one site immediately, but at another, a machine was infected as the user booted up his PC with the disk in the drive. That user then posted disks to eight other sites before going on leave for three days; no one else knew to which other sites disks had been posted! Two of the sites were infected. The major impact of this incident was growing acrimony amongst staff.

A common source of infection is illustrated by the member of staff of an educational establishment who was studying at a local college. He brought back a disk infected with Cascade, which he loaded without permission onto a stand-alone PC used for maintaining accounts at the establishment where he worked. It took two days for the local authority's technical support team to clean up the infection, during which time it was not possible to deal with account and telephone enquiries. A clerk then had to work overtime to catch up on the backlog of work. The total cost of the incident was estimated at £2000.

According to two-thirds of the virus infection reports, standards were revised following the incident. Disciplinary measures were taken in 15% of cases.

Which Solution?

What can be done to counter the problem? Probably more than with any other threat to IT, protection from viruses lies first and foremost in the hands of the end user. Unless mandatory control systems are implemented, or floppy disk drives are locked or removed, with all software and data downloaded from a file server, ignorant or careless actions by staff will increase the risk of infection.

Every employee must receive proper IT security awareness training. This should cover all aspects of PC security (i.e. backups, theft, data protection, copyright and viruses). Such training should be designed so that staff understand fully the impact which all breaches may have on the operation of the business for which they work.

In particular, it should cover how viruses can be introduced, what to do if an infection is suspected, and how every individual must be responsible for the protection of their PCs from the threat which viruses present.

Unless measures such as those described above are consistently introduced and implemented, the security breaches and virus attacks which are being experienced in businesses throughout the UK (and indeed internationally) will not only remain but increase.

Chris Hook, MCBS, ACIB

Chris Hook is a Managing Consultant with the *NCC Business Technology Group*, and has particular responsibility for IT security consultancy assignments for clients, and for presenting security awareness seminars to IT end users.

Prior to joining the *NCC*, he was Computer Auditor at *Rochdale MBC* and was Chairman of the Greater Manchester *Local Government Computer Audit Group*. He is a member of the *British Computer Society* and an associate of the *Chartered Institute of Bankers*.

The *National Computer Centre* (*NCC*)

The *NCC* is an independent provider of advice on every aspect of IT, a role it has held for nearly 30 years. Its consultancy service provides risk analysis of IT security, contingency planning for IT systems, network security and audit, general IT security reviews, and assistance with corporate IT security awareness programmes.

The *1994 IT Security Breaches Survey* is available from the *NCC* at £145 + £4.00 p&p. For further information, contact Jayne Howell on +44 (0)161 228 6333.