NSA's future Infosec plans

Wayne Madsen

On 23 April 1997, the National Security Agency (NSA) hosted the first Information Systems Security Education Colloquium at the Maritime Institute of Technology, Linthicum, Maryland, USA. The conclave, which attracted representatives of government, industry and academia, was designed to create a national approach to information security education and training. Although the subject matter was relatively innocuous, the opening remarks by Thomas McDermott, NSA's Deputy Director for Information System Security, revealed some of NSA's expansionist plans for the future.

McDermott pointed out that the Information System Security Organization of NSA was providing "leadership, products, and services necessary to enable customers to protect national security and sensitive information in information systems pursuant to federal law and national policies".

Although NSA does, in fact, have a mandate to provide security for national security information, the Computer Security Act of 1987 specifically assigns the National Institute for Standards and Technology (NIST) responsibility for the protection of sensitive unclassified Government information.The 1987 Act does not assign any government agency responsibility for securing private sector 'sensitive' information.

McDermott, not surprisingly, stated that NSA "strongly" supports the information warfare initiatives of the President's Commission for Critical Infrastructure Protection (PCCIP) and the Department of Defense Science Board. Both groups have called for significant amendments to or complete abrogation of the Computer Security Act. In any case, the NSA would achieve greater authority over civilian government and private sector information systems security.

McDermott conceded as much when he said "if someone messes with a banking system — that is a national security issue". Underscoring his belief that NSA's role was expanding, McDermott saw an evolution away from the organization's past and present roles in providing communications security and information systems security. He felt that NSA must assume a wider role in providing "defensive information operations" for a vast range of systems environments, both in the government and the private sector. The Deputy Director saw NSA's role as being similar to the government providing for civil defence in the nuclear age. "We [NSA]", McDermott said, "must provide civil defence in the information age". While conceding that an 'electronic Pearl Harbor' is still some time off, McDermott believes that "the means and motives exist today for smaller electronic World Trade Center and Oklahoma City events".

"protect national security and sensitive information"

To combat such occurrences, McDermott promoted the notion of "zones of cooperation" between the government sector, US law enforcement and national security, international law enforcement and national security, and the private sector. Future zones of cooperation initiatives described by McDermott include "releasable cryptographic solutions" and "aggressive protection of Defence Information Infrastructure and crucial parts of the National Information Infrastructure".

Lastly, McDermott pleaded with industry to accept NSA's technical expertise to "satisfy national needs".

Computer viruses — the current state in Italy

Silvano Ongetta

During 1996 an average increase of 6.7% of new computer viruses was registered in Italy. This resulted in an increase of 285% over 1995 in the total number of businesses infected with computer viruses. The total number of cases increased by 1195 over the total for 1995. Off-setting this, the number of computers

damaged and the number of hours lost have declined on the previous year.

The increase in computer viruses represents 89 different viruses including 13 more than the previous year. This is equivalent to 0.89% of the total number of viruses currently known worldwide.

The most relevant data is revealed upon examination of a homogeneous sample composed of approximately 1000 PC distributors in Italy. This study indicated that 3% of PCs and support mechanisms were infected or detected viral contamination. In Italy it is estimated that 150 000 viruses exist on PCs or disks out of a total of five million.

This information was obtained from the sixth annual report of the anti-virus service and criminal prevention prepared by Security Net and collated by Fulvio Berghella. The sample obeserved consists of 100 banking services, industrial services and public administration affairs representative in Italy. The cases reviewed in the sample were 2991 which infected 6642 magnetic systems resulting in the loss of 1139 working days or 9000 work hours. The most prevalent viruses were:

Form	33.9%
Bye	7.5%
170X (Cascade)	5.9%
Junkie	5.8%
RRPS2	5.6%
Yankee D	4%
November 17 (V855)	3.6%
NYB	2.8%
PG3	2.7%
Peter II	2.6%
AntiExe	2.3%
Parity B	2.2%
Concept	2%
HLLC	1.4%
Craven	1.4%
GenB	1.4%

These 16 viruses infected 84% of the sample and are present throughout the entire country. Viruses are detected throughout the year, though the most infections occurred in December (14%), November (13%), October (10%) and January (9%). This confirms that the winter season is the most dangerous.

The businesses with the highest risk of exposure to computer viruses are those in the public administration sector where each incident represents an average lost time of 1.3 days. The most severe incidents have been found in the service sector, particularly banks. This has resulted in the development of preventive measures in this sector.

Researchers at Istinform interviewed 100 personnel in charge of security to confirm the method of infection of viruses into businesses (it is acknowledged that such information is fundamental to a better understanding and prevention of the phenomena). The causes of the spread of viruses are classified as programs brought in by employees (22.8%), by suppliers (22.5%), from client floppy disks (22.5%), on floppy disks from other businesses (10.1%), from intercompany exhanges (7.9%), by video games (7.1%), over the Internet (3.4%), by floppy disks installed for maintenance (2.6%) and via new software (1.1%).

Some of the incidents which occurred in 1996 raised legal issues. Two significant cases are as follows: one business in the service industry which was oblivious to computer security, accidentally transmitted to 250 clients a dangerous and complex virus with some updated software. One large firm requested the intervention of a magistrate and police specialists after discovering the presence of the new virus on computer files containing strategic data.

1996 was characterized by the appearance and the immediate expansion of new methods of infection including macro viruses for Winword as well as hoax viruses. The first exploits a macro on a well known word processing program. The latter has the objective of alarming users with hoax messages via E-mail whereby the users are instructed to not read certain files and asked to distributed the warnings to fellow users. The hoaxes take advantage of the sense of responsibility of the users by producing a chain letter type reaction of messages over the Net, which results in lost time and increased traffic and, in certain cases, site paralysis.