NANDINI VAISH

Nandini Vaish is a Principal Correspondent with India Today where she covers issues allied to Business. Prior to this, she was with Businessworld and CNBC TV18. She graduated in English Literature from Lady Shri Ram College in New Delhi and completed her postgraduation in Advertising and Marketing at The Xavier Institute of Communications, Mumbai.

Nandini won The PoleStar Award for the ‘Best Feature in IT Journalism’ for 2004 for her article, 'Data Security: The Unusual Suspects’, which appeared in Businessworld.

DATA SECURITY: THE UNUSUAL SUSPECTS

The darker side of some of the sleekest gadgets in play

BenQ Joybee music player. Maximum capacity: 256 Mb

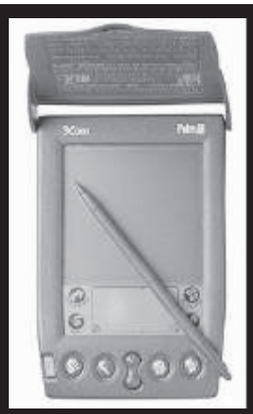
If you thought the latest camera phone your colleague just brought to work is just that - a phone that also clicks pictures - then think again. It can also be used as a deadly weapon of subterfuge. Look at the possibilities: with that device, your colleague can take more than 100 pictures of documents, events and even the office, information that competitors may pay to procure.

Too far-fetched a theory? Not quite. Before you quiz your camera-phone-toting colleagues, you may look at this irony for an affirmation of the threat: Samsung Electronics, the world's third largest camera phone manufacturer, has forbidden the use of camera phones inside its headquarters, factories and research centres.

Samsung is not alone. Automobile and pharmaceutical companies the world over ban such devices from their R&D centres. Government agencies too have banned many such devices. The British ministry of defence has banned the portable music player iPod from sensitive areas. In India, the armed forces headquarters and Defence Research Development Organisation are out of bounds for any outside electronic gadgets. The Saudi government has altogether prohibited camera phones in the country; tourists need to either carry ordinary mobile phones or risk confiscation. The threat to information security is not new. It has been a concern as long as it has been possible to store data, electronically or otherwise. What has changed the field dramatically in recent times is the advent of newer, easier modes of transfer and storage. And in this field, portable storage devices, growing in their ubiquity, are the latest weapons. That's the terrible reality such gadgets have brought about.

Shall we round up the suspects? To begin, thumb drives and memory sticks are a new incarnation of the Trojan horse of Achilles' time. These devices, often the size of a human thumb, plug into universal serial bus (USB) ports that all new computers come with. (USB is an external bus standard that supports data transfer rates of 12 megabytes per second, or Mbps. Another, lesser-used standard is the IEEE 1394, a version of which supports transfer rates up to 800 Mbps.) To the horror of the security-minded, these unassumingly small devices can be 'hot plugged', that is, they can be added or removed while a computer is running without disrupting its regular operations. With memory capacities ranging from a few megabytes to gigabytes, they could form a lethal arsenal.

Then there is the Apple iPod, the largest selling portable MP3 music player, which comes with a maximum storage space of 40 Gb. The space is comparable to that on an average home PC. With data transfer rate of over 10 Mbps, it can download an entire computer's information in minutes.



Palm III personal digital assistant. Maximum capacity: 2 Mb

It's not just the storage space that these devices offer, but their ubiquity, that adds to complications in security policies. Just in the latest reported quarter, Apple sold 860,000 iPods around the world.

It's not just iPods and thumb drives, but a multitude of gadgets ranging from personal digital assistants (PDAs) to laptops that can be plugged into USB ports. And as such devices grow in numbers, so does the threat posed by them. It's a very tangible threat. The loss from data theft every year is counted in billions of dollars globally. In India, a 2002-03 survey by PricewaterhouseCoopers (PwC) and CII (on a sample size of 103 companies) showed that at least 3 per cent of companies lose revenues above Rs 5 lakh each due to breaches. And this is only the tip of the iceberg - only 60 per cent of the thefts get reported.

In 2000, an engineer at erstwhile accounting firm Arthur Andersen who had helped develop a Rs 9-crore enterprise software for Indian Oil Corporation, stole it using his laptop when he moved to another company. Once out, one of the companies he tried to sell the software happened to be Mobil Corporation of US, which had a collaboration with Indian Oil. Mobil recognised the software and he was caught.

The threat

- Many new, small devices can steal data
- They can also be used to introduce viruses and Trojans into systems
- Camera phones can steal drawings, blueprints or layouts
- Devices can secretly record conversations

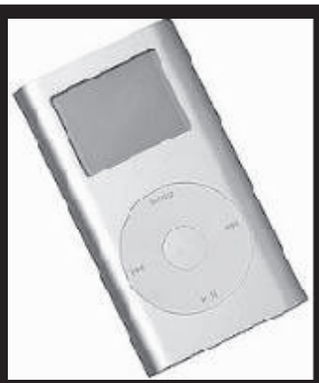
Bollywood has always been a haven for intellectual property thieves, but few have been as brazen as Canadian film editor Troy Niemens. Unhappy with some pecuniary issues at his employer Kaleidoscope Entertainment, Niemens decided to flee with an unreleased version of the film 'American Daylight', which he had been editing on his Apple iBook. He and his wife were arrested at the IGI airport in Delhi a few minutes before they were to board a flight to Canada. Is it technology that is spawning a new breed of corporate crime? Sivarama Krishnan, executive director, PwC, doesn't think so. He argues: "Data theft is not encouraged by technology, but by unprincipled competition. Technology is merely an enabler. USB devices per se do offer a threat, but are also tools for performance and productivity enhancement." While often it's corporate rivalry that encourages theft, the trigger may lie within the company. In the survey, former employees and competitors accounted for 5 per cent and 6 per cent of thefts, respectively. (Computer hackers were responsible for 46 per cent of the breaches.)

Analysis and advisory firm Gartner highlights the risks companies expose themselves to by allowing USB devices within the office. While it is difficult to stop employees from using these popular tools, it is imperative that companies have safeguards to prevent misuse. One of the first things is to have a security policy that spells out the organisation's stance on the use of such devices. Training should ensure a security-conscious workforce, which will be less likely to unwittingly put out sensitive information.

Preventive Measures

- Establish a security policy that encourages whistle-blowing
- Train employees on detection of different kinds of fraud
- Control access to USB ports, through centralised server, for example
- Enable smart card logins to prevent unauthorised users

A 'desktop lockdown policy' disabling universal plug and play functions and allowing access by only authorised devices may not be feasible to implement on all machines. Consultants even advise companies to classify users and usage, as many banks and insurance companies do. At PwC itself, good corporate governance is stressed over technology protection. Palmtops, camera phones and pen drives are allowed in the premises, but access to sensitive documents is restricted.



Apple iPod, whose storage equals that
on a regular home PC, is one of the latest threats

Newer challenges are prompting some to think afresh about solutions. The South Korean government, for one, is planning to regulate the use of camera phones in public places by ensuring that it's evident when someone is clicking a photograph. Visibility of the camera lens could be one solution, an audible 'click' sound another. Companies in India too have certainly recognised such threats. Some, whose business depends on data security, have taken severe measures. At process outsourcing firm Wipro Spectramind, employees are watched through surveillance cameras. The terminals on the process floor are all 'dumb' - they have no hard disks. Employees have to leave all gadgets, even paper and pen, in a locker room outside. The company conducts regular internal audits and monitors emails at random. "Violations, if any, are severely dealt with," says Tamal Dasgupta, CIO of Wipro Technologies, of which Wipro Spectramind is a subsidiary. Policing aside, the company has developed an internal awareness project called Security Srinivas. A small website has been dedicated to this and employees receive regular updates on the company's security policy.

The world's largest pharma company, Pfizer, follows its own information protection management guideline (IPMG), which states that information and programs stored on portable computers must be adequately protected from modification and disclosure. Only those USB memory devices that fully support passwords and encryption are allowed. These too are formatted and configured with passwords that comply with Pfizer's IPMG standards.

Says Jasminder Gulati, manager (enterprise marketing), Microsoft India: "To safeguard against data theft using external devices, it is important to ensure that the data in itself is protected. This can be done by either encoding or encrypting the data." Microsoft has been working closely with the National Association of Software and Service Companies to get a Data Protection Act in place.

But laws do not ensure that thefts are not attempted. The best way to avert being hit is to know well about the threat and keep up surveillance. It is also a great excuse to check out the latest gadgets of your colleagues.