Computer Crimes

Asgar Hussein

In this era of information technology, unscrupulous individuals are increasingly cashing in on the world's fastest growing crime wave computer frauds.

A computer fraud can be perpetrated in a fraction of a second the time it takes to blink,' thus claimed two British computer experts who formed a company advising firms on the dangers of computer assisted crime.

Fortunately, the incidence of computer crime in developing countries such as Sri Lanka is very much less than in the west and other advanced Asian nations.

Nevertheless, it is quite probable that this menace would reach dangerous proportions in Sri Lanka too in the future unless strong measures are taken to curb its spread.

The present laws in Sri Lanka are sadly inadequate to bring computer crooks to justice, because information and service crimes are not covered in the penal code which is over 100 years old.

It was to remedy this situation that the Information Technology Law Centre of the Computer and Information Technology Council of Sri Lanka (CINTEC), recently proposed legislation on computer crime.

The basis of the draft Computer Crimes Act for Sri Lanka is to recommend the prohibition of unauthorized access and attempts to access a computer, computer program, data or information. It also contains a provision to deal with unauthorized use, regardless of whether the offender had authority to access.

According to this proposed legislation, unauthorized modification, alteration or deletion of information is an offence. So is denial of access, which means that one cannot program the computer in such a manner as to prevent authorized persons from accessing it.

Other offences mentioned in the draft Act include:

- Causing damage or harm to the computer, computer program, data or information. For example, the introduction of viruses and logic bombs would be considered a computer crime.
- Unauthorised copying of information
- Falsifying computer information.
- Unauthorised use of a computer service.
- Interception of program, data or information while they are being transmitted

The proposed legislation was drafted by deputy solicitor general Kolitha Dharmawardena, who heads the CINTEC IT Law Centre. He was helped by research assistant Jayantha Fernando and other members of the Working Committee on Law and Computer of CINTEC. This project was conceived and accomplished under the overall supervision and guidance of CINTEC Chairman Prof. V K Samaranayake. Dharmawardena believes that this legislation, once imposed, will prove effective in bringing computer crooks to book and act as a deterrent, provided detections and investigations are carried out smoothly.

He pointed out that it will enable authorised specialists or technically competent persons to take part in the investigation of computer crimes. It would also permit authorised officers investigating an offence to access, inspect and examine the operations of any computer, computer program, data or information.

Dharmawardena expressed confidence that the draft Act will be approved by parliament, either in its present or modified form.

He told ‘Business Today’ that there could be many intelligent white collar computer criminals in Sri Lanka who are ingenious enough to cause serious financial losses to companies.

‘As yet we don’t know how serious the computer crime problem is in Sri Lanka, but one thing is very clear society is becoming information dependent’, he said.

In fact, as technical know-how increases, so does the risk of computer crime.

Reports of computer crime in this country are slowly trickling in. However, many companies which face computer frauds don’t report to the authorities because they fear it will erode public and shareholder confidence. They also feel the legal system may be unprepared to handle such cases.

It is learnt that several banks in the island have experienced computer fraud, though few have reported it.

Banks are quite vulnerable to computer crime. For example, an employee can program the computer to transfer a part of the interest generated from savings accounts to a fictitious account or that of an accomplice. Manipulation can also occur during electronic fund transfers, including transactions on automated teller machines.

In one leading private bank. here, a clerk fraudulently credited a large sum of money to the account of an accomplice who later withdrew the cash and got away.

There was also a case reported where an employee of the Lotteries Board had manipulated the computer to generate a fictitious winning number to claim the winner’s purse. Fortunately, the deception was uncovered in time by sleuths.

As things stand now, investigating a computer crime may disrupt the operations of the affected firms as the case may drag on for a long period, because investigators and others involved in the legal process lack the expertise to handle complex high-tech crime.

Further, computer crooks often go unpunished because the long delays in the criminal justice system and the high cost discourage companies from reporting frauds which don’t involve very large sums of money.

Dharmawardena believes that to minimize or prevent computer crime, companies should establish proper security systems, and access to the main computer sections must be limited only to those employees who necessarily require it.

Also, it should be ensured that at least two persons, each having a different password, must get together to secure access to sensitive operations so that sensitive information cannot be processed merely by one individual.

Institutions should also periodically change the passwords to access sensitive information. Another safeguard would be to scrutinize the background of persons involved in critical operations, and to maintain a sense of vigilance.

According to Dharmawardena, investigators will face much difficulty in detecting computer criminals because of the lack of tell-tale evidence or clues such as those found in murder and robbery scenes. ‘In the years to come, it would be essential to establish minimum security standards in the computer systems in Sri Lanka.’

Since critical operations are increasingly being computerized, there is a constant danger that misuse can result in very serious consequences. For example, Bearings Bank in London collapsed sometime back due to the dubious activities of its Singapore branch manager Nick Leeson. The computerized system enabled Leeson to continue incurring various obligations on behalf of the bank by trading in futures. This bank. would never have run into huge debts in such a short period without detection had it not been for the modern computerized environment.

In the west, there have been instances of unscrupulous companies engaging in computer manipulation to obtain sensitive information, trade secrets, formulas and names of high-value clients of rival firms.

Some computer crooks are ruthless, and others are less ambitious. There was a case reported of a programmer employed in a cigarette company who rigged the computer and got credited with free savings coupons which he then exchanged for gifts.

Others are far more ambitious, and what better example to cite than Stanley Rifkin, who has been called ‘the master of computer frauds’. This man gained access to the wire room of a Los Angeles Bank he once worked for, and memorized the day’s

codes. Then he transferred US$10 million to his own account by plugging into the computer terminal. However, Rifkin’s crime was later uncovered by the FBI, and he was caught.

According to Deva Rodrigo of Partner, Coopers & Lybrand, chartered accountants, the computer crimes reported in Sri Lanka represent merely the tip of the iceberg, as in other countries.

He told ‘Business Today’ that the risk of a computer fraud is very high in this country due to the lack of awareness of computer controls and application controls.

He noted that serious computer crimes can especially occur in operations where the computer generates cheques and approves suppliers invoices for payment.

Frauds can also take place when credit control procedures are performed by the computer. Because people expect computers to accurately process data and authorise transaction, the level of checking is less. As a result, opportunities for production of misleading financial statements in a computerized environment are greater.

Rodrigo stated there are three dangers specific to computer processing, which would not be risks in manual systems.

The first is that since data is kept in a magnetic form, it can be changed or erased without even a trace. Therefore, protection of data held in computer files from unauthorized changes is a critical area.

The second danger is that if standing data is not kept current and correct, the company. faces the risk of financial loss.

The third danger is that when all functions are carried out by computer programs and if the program development and computer operations are not segregated functions, there is a high risk of unauthorised changes being made to computer programs.

Rodrigo pointed out that a computer fraud survey in the US showed that 8% of computer users have faced serious fraud, 24% experienced a virus out break, and 5 percent suffered hacking.

He said most computer crimes are undertaken by employees mainly in the clerical

and supervisory levels, as well as by programmers and other computer staff.

‘Data diddling’ (Which involves subjecting data in a computer file to unauthorised changes) is the most common type of computer fraud. Next come the frauds connected with program development and maintenance.

‘Trojan horse’ is another type of computer crime. In such cases, those involved in programming introduce a program step that could result in a total break- down of the system when it is triggered by some action (for instance, the deletion of the programmer’s name from the payroll after he is sacked).

Most computer frauds however are detected due to the effective operation of internal control, or by audit.