CHAPTER 15

PREVENTING CYBER CRIME

Cyber crime may have disastrous consequences on the economy of a country. Organisations and individuals may suffer extensive losses at the hands of cyber criminals. It is therefore imperative to deal with the various ways in which cyber crime can be prevented.

15.1 EDUCATION AND AWARENESS

Many private and government schools educate students in relation to computers and present subjects in respect of information technology. It is important that young persons should be educated in respect of computer ethics at school level. Many hackers and cyber criminals have some training in the field of computers or information technology. The training of students at universities in these fields should include the teaching of ethics and values.[1] The government should also become involved in educational projects and awareness programs.

Corporations and private persons should be made aware of the risks in relation to information technology and what can be done to prevent cyber crime.[2] Employees of large corporations should be educated in respect of security issues and made aware of all the risks. The safekeeping and

[1] Also see R A Coldwell *Hacking into computer systems, anomie and computer education* (1998) Acta Criminologica Vol. 11 No 1 17-18.

[2] For example see Jason Johnson *Clean up your act (dealing with computer viruses forms a vital component of practice management)* (2001) May De Rebus 33.

secrecy of passwords for instance are essential and should be explained to all employees.

15.2 INFORMATION TECHNOLOGY SECURITY[3]

Security should be directed at organisational level, physical security and information technology security.[4] At organisational level codes of conduct should be implemented that set borders and limits for those who have access to computers and computer systems. The main frame of a computer system as well as important physical areas should be secure against intrusion. Computer systems should be protected by the proper use of passwords. Firewalls are often used to protect computer systems against intrusion. Nowadays there are many products on the market that are designed to protect computer systems and data. Anti-virus software programmes for instance are readily available.[5] Corporations often use the method of *compartmentalizing* data or information by keeping sensitive data on a system that is not connected to the Internet.[6]

15.3 DETECTION, REPORTING AND THE JUSTICE SYSTEM

Corporations are sometimes reluctant to report cyber offences and computer-related fraud.[7] The main reasons for that is that the integrity of

[3] In general see Michael Alexander *The Underground Guide to Computer Security* 1996; Jeff Crume *Inside Internet Security – What hackers don't want you to know* 2000.

[4] See Tony Elbra *A Practicle Guide to the Computer Misuse Act 1990* (1990) 21 – 26.

[5] See Fites et al *The Computer Virus Crisis* (1989) 133.

[6] Michael Fraase *Information Eclipse* (1999) 233.

[7] See Dr Michael Levi *Computer fraud in Britain – some research findings* (1990-91) 1 The Computer Law and Security Report 6.

their data may be questioned and it may cause embarrassment. A “whistle blowing” system to report any cyber crimes should be implemented. To effectively combat cyber crime, a country must have effective laws in place. It would appear from the discussions above that our law has to a certain extent effectively dealt with the advent of cyber crime. The next step would be to ensure that these laws are effectively implemented and that the investigation and prosecution of these cases are successful. All these aspects are discussed in detail above. Police officers and prosecutors should be trained to effectively investigate and prosecute cases of this nature. Police and prosecution units that specialise in these types of offences will assist in the effective investigation and prosecution of such cases. Judges and Magistrates accordingly should also receive lectures and training on the subject. Where necessary and appropriate knowledgeable assessors should be appointed to assist in the just adjudication of cyber cases. A strong and workable legal system can also serve as a deterrent since the criminals are dealt with according to the law and it promotes legal certainty. Appropriate and strict sentences will also have a deterrent effect.

15.4 INTERNATIONAL CO-OPERATION

Finally, cyber crime is a global problem and has a distinct borderless nature. The Internet for instance is accessible all over the world. Cyber crimes often have global implications. The effective co-operation between countries in respect of detection, investigation and prosecution of a cyber crime will be imperative to effectively combating and thereby also preventing cyber crime. The proposals in this regard by the Convention on Cybercrime, are necessary steps in the right direction.[8]

[8] See paragraph 13.1 *supra*.