CHAPTER 7

DEVICES

7.1 INTRODUCTION

Cyber criminals often use devices in order to gain unauthorised access to data or to commit cyber crimes. These devices may consist of hardware devices and attachments, and software programs. Many of these software programs can be downloaded from the Internet. *Spyware* or *snoopware* are software programs designed to monitor a host computer or system. Some of these software programmes can actually be "installed" via electronic mail to the victim's computer.[1] Valuable information such as credit card numbers and personal passwords can be obtained in this manner. A *war dialler* for instance is a software program that dials telephone numbers in order to find answering machines connected via modem to the telephone.[2]

The notorious *ABSA hacker* allegedly used a software program called *eBlaster.*[3] This program can be sent via e-mail to the victim and when the victim opens the e-mail, the software program is secretly installed and activated on the victim's computer. All the information that is entered into the computer is sent to the criminal. These include e-mails and keystrokes entered on the computer. The perpetrator would therefore be

[1] John Schwartz *Crossing line between monitoring and spying* Thisday 14/10/2003 page 23.

[2] David J Marchette *Computer Intrusion Detection and Network Monitoring* (2001) 315

[3] Edwin Lombard *Alleged Absa hacker's secrets revealed in court* Sunday Times 21/09/2003 page 7; Bert van Hees *Hacker suspect's 46 charges* The Citizen 17/09/2003 page 3.

in a position to obtain confidential information such as account numbers, pin numbers and passwords.

An electronic card reader or *skimming device* is a physical device that can be used to “read” electronic data from for instance the magnetic strip of a debit bankcard or a credit card. These devices are used at restaurants and other outlets where a cardholder uses a credit or debit card. The card is swiped through the skimming device or card reader by the perpetrator and all the data contained on the magnetic strip is captured and can be downloaded from the device with the assistance of a computer terminal. It was recently reported that certain skimming devices were found at Automated Teller Machines worldwide and also in South Africa.[4] The skimming device is placed over the normal slot for the card and when the card is inserted the skimming device reads the electronic data on the magnetic strip.[5] The information can be retrieved by disconnecting the device and downloading the information. The data can also be transmitted to the perpetrator within reasonable proximity through means of wireless technology. In some of these instances transmitters and aerials were also retrieved. A camera was strategically placed on the ATM in order to capture the entering of the pin number.[6]

Sniffers are programs or devices that are used to monitor networks and to troubleshoot network connections.[7] They are also known as network

[4] Petro Lowies *Skelms se nuwe set by kitsbanke – oorsese bedrogspul nou ook in SA* Naweek-Beeld 10/01/2004 page 1.

[5] Footnote 4 *supra*.

[6] Footnote 4 *supra*.

[7] Shani S Kennedy & Rachel P Flum *Computer Crimes* (2002) American Criminal Law Review Vol. 39 No. 2. 277.

analysers. *Superzapping* refers to a system tool or software program that is used when a computer malfunctions to bypass controls and security measures in order to repair the computer.[8] These programs may assist cyber criminals to gain unauthorised access to data.

Hardware *keyboard loggers* are units that are installed between the keyboard and the computer. This enables the device to record all the keystrokes that is entered on the computer via the keyboard and stores it in the device. These devices have varied storage space and sometimes look very similar to ordinary computer cables or equipment. The device is then connected to a different computer and the information can then be downloaded from the device by the perpetrator. Valuable information can be obtained in this manner. A hardware keyboard logger needs to be physically installed and the perpetrator will need physical access to the targeted computer. Software key loggers are software programs designed to record information on the computer.

7.2 **INTERNATIONAL RESPONSES**

7.2.1 United States of America and the United Kingdom

Section 1030(a)(6) of the United States Criminal Code as inserted by the Computer Fraud and Abuse Act[9] states:

> "(a) Whoever –
>
> (1) – (5)…

[8] Irving J Sloan *The Computer and the Law* (1984) 11 *et seq*. Also see Dana van der Merwe *Computers and the Law* (2000) 169.

[9] 1986.

> (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-
>
> (A) such trafficking affects interstate or foreign commerce; or
>
> (B) such computer is used by or for the Government of the United States;
>
> shall be punished as provided in subsection (c) of this section."[10]

The prohibitions in respect of trafficking in passwords only apply to commerce and government computers. The Act has been criticised because "affects interstate … commerce" is not defined and the definition and scope thereof are unclear.[11] Furthermore a perpetrator should have the intention to defraud. Kevin David Mitnick was convicted of a contravention of section 1030(a)(6) of the Act as well as of a contravention of the Electronic Communications Privacy Act for possession of telephone access codes which he used to bill calls to different accounts.[12]

The United States Code also prohibits the production and use of or trafficking in counterfeit access devices[13], provided that the perpetrator

[10] United States Code, 2000 Edition.

[11] Christopher D Chen *Computer Crime and the Computer Fraud and Abuse Act of 1986* (1990) Computer Law Journal Vol. X No. 1 79.

[12] A BNA Special Report *Computer data security* 104 – 105.

[13] Section 1029(e)(1) provides "the term 'access device' means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)". In addition section 1029(e)(2) provides that "the term 'counterfeit access device' means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device" (2000 Edition).

acts with the intention to defraud.[14] The intentional trafficking in and use of unauthorized access devices within any one-year period and by such conduct obtaining anything of value in excess of $ 1, 000 is also criminalised.[15] It is reported that Andrew Miffleton, a hacker from the group known as *the Darkside Hackers*, pleaded guilty to contravening section 1029(a)(3) of the United States Code which prohibits the possession of unauthorised access devices.[16] Miffleton *inter alia* possessed a list that contained the root level passwords to certain computer systems as well as individual user level passwords.

In the United Kingdom the Computer Misuse Act[17] does not criminalise the possession or distribution of devices used or intended to be used in the commission of computer crimes.

7.2.2 Canada

The Canadian Criminal Code contains an interesting provision in respect of devices that are used in the commission of cyber offences:

> "Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the

[14] Section 1029(a)(1) of the United States Code (2000 Edition)

[15] Section 1029(a)(2) of the United States Code (2000 Edition).

[16] Press release by the US Department of Justice entitled *Computer hacker sentenced in federal court* accessible at http://www.usdoj.gov/criminal/cybercrime/miffle2.htm

[17] 1990.

> instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
>
> (b) is guilty of an offence punishable on summary conviction."[18]

The provision is very widely defined and will encompass all types of devices that are used or intend to be used in the commission of cyber crimes. The possession as well as the distribution of such devices are criminalised.

7.2.3 The Convention on Cybercrime

Article 6 of the Convention on Cybercrime[19] deals with the misuse of devices and states that the signatory countries should criminalise the "production, sale, procurement for use, import, distribution or otherwise making available of" devices and passwords with the intention that it be used in the commission of cyber offences. A device would include a computer program and is a device that is designed or adapted for the purpose of committing cyber offences. A computer password or access code or similar data that is used to access data will also fall within these provisions. The possession of a device or password with the intention to use same in the commission of a cyber crime should also be criminalised by the signatory countries.

It is clear that these types of devices, software programs and passwords should be directed at the commission of a cyber crime. If these devices

[18] Section 342.2(1) of the Canadian Criminal Code.

[19] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001.

are sold or used for authorised testing or protection of a computer system it is lawful and should not be criminally sanctioned.

7.3 SOUTH AFRICAN RESPONSES

Before enactment of the Electronic Communications and Transactions Act there were no provisions in either common law or statutory law that prohibited the possession of or trafficking in devices that are used in cyber offences. The South African Law Commission recommended that the development and trafficking in devices or applications that are primarily used to obtain unauthorised access[20] as well as trafficking in passwords[21] should be criminalised by way of legislation.[22] These proposed offences were criticised by a computer security consultant on the basis that these devices are often used and developed in order to test vulnerabilities in computer systems and security measures.[23]

Section 86(3) of the Electronic Communications and Transactions Act states:

[20] The following draft was recommended: "Any person who, without lawful justification, develops, manufactures, produces, imports, exports, procures for use, or makes available, a device or application designed or adapted to make it primarily useful for accessing or for modifying, destroying or erasing or otherwise rendering ineffective an application or data held in a computer system without authority to access, modify, destroy or erase or otherwise render ineffective that application or data, is guilty of an offence" – Section 4 of the Proposed Computer Misuse Bill, SA Law Commission Report 65.

[21] The following draft was recommended: "Any person who makes available any password or similar information by means of which an application or data held in a computer system can be accessed without authority to access that application or data, is guilty of an offence." – Section 5 of the Proposed Computer Misuse Bill, SA Law Commission Report 65.

[22] SA Law Commission Discussion Paper 99 Project 108 *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural matters* (2001) 58.

[23] This letter is accessible at http://www.2600.co.za/articles/computermisuseresponse.html .

> “A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence”

The act consists in the production, distribution or possession of any device which is designed primarily to overcome security measures that protect data. This will include software programs as well as hardware devices. Programs such as *eBlaster* and keyboard loggers[24] would fall within the ambit of these provisions. The Act criminalises the production, distribution or possession of software programs or hardware devices that are designed to contravene the rest of the provisions criminalised by section 86 of the Act (such as unauthorised access or modification). Similarly the unlawful trafficking in or possession of passwords and access codes will also fall within the ambit of this section. A disgruntled employee could for instance sell passwords and access codes of company computer systems to a cyber criminal who in turn could use them to gain unauthorised access to the computer systems.

The perpetrator should act unlawfully. It is possible that these types of programs and devices are used lawfully by persons for instance by security consultants to test and improve security. The perpetrator must act intentionally. The intent to unlawfully utilise such an item to contravene an offence in section 86 of the Act is required. Designers and retailers

[24] See paragraph 7.1 *supra*.

that sell some of these software programs and devices will not usually have the specific intent as required.[25]

Section 86(4) of the Electronic Communications and Transactions Act states:

> "A person who utilises[26] any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence"

Section 86(4) of the Act criminalises the actual use of such a software program or device to overcome security measures or to contravene any of the rest of the actions criminalised in section 86 of the Act. The use of a software program or hardware device to unlawfully access, intercept or modify data will fall within the ambit of the offence envisaged by section 86(4) of the Act. It is interesting to note that in subsection 4 no reference is made to passwords and access codes. It would appear therefore that if a password or access code is used to gain unauthorised access to a computer system it would not constitute an offence in terms of section 86(4). It would however constitute an offence in terms of section 86(1) of the Act. It could be argued that the use of the words *any device or computer program mentioned in subsection (3)…* is wide enough to encompass the use of passwords and access codes.

A person who possesses, designs or actually uses a *port scanning* software program may avoid criminal liability in terms of the provisions

[25] In terms of section 332 of the Criminal Procedure Act 51 of 1977 a corporate body could be prosecuted through its directors or members.

[26] My underlining.

of section 86(3) and 86(4) of the Act. Port scanning establishes which communication channels or ports of a computer are open.[27] It may happen that this information will be used in order to facilitate later unauthorised access. The main problem with these two subsections are the requirements that these devices must be possessed with the intention to gain unauthorised access or actually used in order to overcome security measures for the protection of data. It may be argued that the mere scanning of ports will not constitute unauthorised access to data and do not necessarily overcome security measures for the protection of data. It is therefore doubtful whether these subsections are contravened.

Section 88(1) provides that a person that attempts to commit the offences referred to in sections 86(3) and 86(4) of the Act is guilty of an offence. The aiding and abetting of a person to commit such offences is criminalised in section 88(2) of the Act. An accused convicted of contravening section 86(3) of the Act may be sentenced to a fine or a term of imprisonment not exceeding 12 months.[28] The Act provides for much stricter penalties upon conviction of contravening section 86(4) of the Act. A perpetrator may be sentenced to a fine or a term of imprisonment not exceeding five years.[29] I am of the view that the persons that design, produce and distribute these software programs or devices should be more severely punished and that the penalty provisions in this regard is too lenient.

[27] In general see G J Ebersöhn *Internet law: Port scanning and ping flooding – a legal perspective* (2003) 66 THRHR No. 4 563 *et seq*. The same argument could be used in respect of *war diallers.*

[28] Section 89(1) of Act 25 of 2002.

[29] These types of offences are seen in a much more serious light by the legislator. See MM Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) 2 TSAR 243.

The Act has now been in operation for more than a year and several cases have been reported. One such case involves the installation of a hardware keyboard logger to a Standard Bank computer system in order to obtain information that is entered into the computer.[30] The accused pleaded guilty to malicious injury to property (in order to install the device the physical casing of the computer had to be forcefully removed thereby causing damage). The accused also pleaded guilty to contravening section 86(3) of the Act in that he unlawfully and intentionally possessed a device that was designed to overcome security measures for the protection of data in that he possessed a hardware keyboard logger. The device, however, did not retrieve any data. In respect of the contravention of section 86(3) of the Act the Accused was sentenced to a fine of R 20 000 or imprisonment for a period of one year.

[30] State v Innocent Mbongeni Madlala Case number: SCCC 160/2003 held at the Specialised Commercial Crime Court, Johannesburg. See *Internet banking hacker sentenced* The Star 12/12/2003 and *Innocent found guilty of attempted Net theft at bank* The Citizen 15/12/2003