CHAPTER 9

EXTORTION

9.1 INTRODUCTION

Extortion by means of computers and information technology can be very serious. For instance a cracker may threaten to release a virus into a computer system of an airport unless his demands are met. The actual location of the perpetrator may be extremely difficult to locate and the demands may rather be adhered to, to avoid disastrous consequences or loss of life. Since a great level of anonymity can be achieved through computers and information technology, it is extremely difficult to identify and locate the perpetrator. An extortionist may even be situated in a different part of the world. Acts of extortion may be directed at government, corporations and individuals. Terrorists may demand the release of imprisoned patriots and money. It could happen that certain data of a corporation are encrypted by the perpetrator and that he demands money in turn for the key to decrypt the data. A cyber criminal could release a virus into a system and then extort money in turn for the programmed "vaccine" to "cure" the system.[1]

The British authors *Grabosky et al* identified five basic forms through which information technology could affect extortion:

- Information systems is the *medium* of the threat i.e. the Internet is used to communicate the threat;

[1] See Martin Wasik *Computers and the blackmail threat* (1989-90) 4 Computer Law and Security Report 22.

- Information systems as the *target* of the threat, for example the electric power distribution computer system or the airport computer system (air traffic control) could be targeted unless certain demands are met;
- Information systems as *media for the disclosure* of embarrassing personal details, for example embarrassing information can be posted on a website in the extortion scam;
- Information systems as the *means of facilitating payment*, for example the extortion money is electronically transferred to some foreign bank account;
- Information systems as *incidental* to the offence (the extortionist can compile a profile on his target through means of electronically obtained information).[2]

9.2 INTERNATIONAL RESPONSES TO COMPUTER-RELATED EXTORTION

Section 1030(a)(7) of the United States Code deals with cyber-related extortion and provides that whoever with the intent to extort any money or other thing of value from any person, firm, association, educational institution, financial institution, government entity or any other legal entity, transmit in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer.[3] The USA PATRIOT Act however limited the scope of application of this provision

[2] Peter Grabosky *et al Electronic Theft – Unlawful Acquisition in Cyberspace* (2001) 38 – 43.

[3] See Shani S Kennedy & Rachel Price Flum *Computer Crime* (2002) American Criminal Law Review Vol. 39 No. 2 283.

to the extortion from individuals.[4] Some individual States in the United States also criminalise computer-related extortion such as North Carolina.

9.3 SOUTH AFRICAN RESPONSES TO COMPUTER-RELATED EXTORTION

The Convention on Cybercrime did not specifically deal with computer-related extortion neither did the South African Law Commission. According to Snyman the common law crime of extortion is committed when:

> "a person unlawfully and intentionally obtains some advantage, which may be of either a patrimonial or a non-patrimonial nature, from another by subjecting the latter to pressure which induces her to hand over the advantage."[5]

Section 87(1) of the Electronic Communications and Transactions Act provides in respect of computer-related extortion that:

> "A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence."

The act consists in the performing or threat of performing any of the acts described in section 86 of the Act such as unauthorised modification of

---

[4] Kennedy (footnote 3 *supra*) 283.

[5] Snyman *Criminal Law* (2002) 386.

data.[6] This will include instances where an extortionist threatens to release a virus into a critical data network or to open the computerised floodgates of dams unless his demands are met. Pressure is therefore exerted by threatening to perform any of the acts criminalised in section 86 of the Act such as the releasing of a virus in order to obtain an advantage. A perpetrator may have modified data and be able to restore the data to its original form. He now exerts pressure for the purpose of obtaining an advantage because he has the ability to restore the data. A hacker locks legitimate users out from access to a computer system and undertakes to stop with his actions or restore access to the system with the purpose of obtaining a proprietary advantage.

The common law crime of extortion is directed at any form of advantage including proprietary as well as non-proprietary advantages.[7] It is therefore interesting that the legislator limited section 87(1) of the Act to a proprietary advantage. This means that the advantage can be expressed in terms of or converted to money or economic value.[8] This limits the scope of application of the offence.[9] The common law crime of extortion requires that the advantage must be handed over to the perpetrator before the act is complete.[10] If the perpetrator is apprehended after the threat has been made but before the acquisition of the advantage, he can only be convicted of attempted extortion.[11] However section 87(1) of the Act

---

[6] Discussed in chapters 3 – 7 *supra*.

[7] Section 1 of the General Law Amendment Act 139 of 1992.

[8] Snyman *Criminal Law* (2002) 387 *et seq*.

[9] M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) 2 TSAR 244.

[10] Snyman *Criminal Law* (2002) 388.

[11] Snyman *Criminal Law* (2002) 388.

states that pressure must be exerted for the *purpose of obtaining* any unlawful proprietary advantage. It would appear that it is not necessary for the perpetrator to actually receive the advantage and would widen the scope of application of the offence.[12] It is sufficient that the perpetrator has the intention to obtain an unlawful proprietary advantage by means of pressure. Section 88(1) of the Act makes provision for the criminalising of an attempt to commit the offence in section 87(1) of the Act. If the threat or pressure with the intention to obtain a proprietary advantage without actually receiving the benefit constitutes a completed crime, it is difficult to imagine what would constitute an attempt under section 87(1) of the Act. Watney is of the view that it was unnecessary for the legislator to create the offence in section 87(1) of the Act, since computer-related extortion would fall within the ambit of the common law crime of extortion.[13]

It was recently reported that two people were convicted in the Randburg Magistrate's Court of a contravention of section 87(1) of the Act.[14] It appears that the two men hacked into the computer system of Vodacom and contacted them in order to claim money in return for the database that contained client information.[15] The Beeld reported that the perpetrators admitted that they demanded payment of R10 million from Vodacom in order not to release the personal information of clients nationwide.[16] It was reported that Michael Bafatakis and Andrew Michael Stokes were

---

[12] Watney (footnote 9 *supra*) 244.

[13] Watney (footnote 9 *supra*) 244.

[14] *First ever conviction for computer hackers* The Citizen 20/11/2003 and Sarie van Niekerk *Kuberkrakers skuldig ná Vodacom-afpersing* Beeld 20/11/2003 page 11.

[15] Footnote 14 *supra*.

[16] Sarie van Niekerk *Kuberkrakers skuldig ná Vodacom-afpersing* Beeld 20/11/2003 page 11.

sentenced to a fine of R 24 000 or 3 years imprisonment which were suspended for 5 years on certain conditions.[17]

[17] Footnote 14 *supra*.