Legal Issues Alone Are Not Enough to Manage Computer Fraud Committed by Employees

Dr Shalini Kesar
John Moores Liverpool University,
School of Computing and Mathematical Sciences
Byrom Street, Liverpool, UK.
Skesar2@gmail.com

Abstract

The advent of IT has created unprecedented opportunities for the occurrence of computer crime like fraud, committed by employees in particular. This paper focuses upon computer fraud committed by employees because reports claim that it is the employees who pose one of the greatest threats to organisations today. Further it argues that solely relying only on current legalisation and other sophisticated measures alone are inadequate for the managing the occurrence of computer fraud committed by employees. Therefore the onus of detecting and managing computer fraud committed by employee(s) lies within the organisations itself. In conducting the argument it discusses the shortcoming of the current legalisation and the challenges it can pose to deal with such acts. Consequently the main contribution of this paper is to enhance the awareness about management of computer fraud committed by employees.

Keywords: *Computer fraud, Security, Employees and Legalisations.*

1 INTRODUCTION

There is a widespread agreement that the proliferation and integration of Information Technology (IT) into organisations inevitably has increased the occurrence of computer related criminal acts like fraud (for example see Ernest and Young 2004; CSI/FBI 2005; Audit Commission 2001 and 2005). Despite the increased sophistication of preventative measures taken by organisations, summary of the recent Audit Commission Report (2005), for example illustrates that such illicit acts will continue to increase in future. What is even more alarming is that both researchers and practitioners advocate that the reported cases of computer crime only represents the *tip of the iceberg* (for example, Parker 1976; Parker and Nycum,1984; James and Palmer 1994; Icove et al.,1995; Fox, 1998;CSI/FBI 2005; Audit Commission 2005). Although such threats can come from both within and outside the organisations, most reports (Ernest and Young 2004; CSI/FBI 2004; Audit Commission 2005) claim that it is the employees who pose one of the greatest threats to the organisations today. The 2005 report by the Audit Commission, for example, illustrated the majority of intentional computer crime was perpetrated by the organisation's own employees, more specifically operational staff accounting for 37 per cent; administrative/clerical staff 31 per cent and managers around 15 per cent. This could be because employees are more familiar, not only with the organisation's computers, but they also have access to them and they know the 'flaws' in the information systems and the resources that the computers control. Hence employees within organisations are in a better position than outsiders to engage in computer fraudulent activities (see for example, The Barings Bank case in the Bank of England Report 1995; Harrington, 2000; Audit Commission, 2001 and 2005; CSI/FBI, 2005).This is not to say that computer crime incidences committed by outsiders is less serious in nature. It is clear that dealing and managing illicit computer related crime committed by employees is more sensitive since it involves the reputation of the organisation. Yet it is alarming to note that there still continues to be a pervasive misconception that responding to computer fraud originating from outside the organisation is the same as responding to fraud originating from within (Schultz, 2002). This myth has been widely accepted perhaps because few studies have been conducted to understand the problem of computer fraud committed by employees in particular. Despite well documented surveys and reports on the extent of damage caused by

employees (often referred to as *insiders*), remarks from researchers that there is currently "no substantial effort devoted to addressing the problem" (Magklaras and Furnell 2003, pg 26) is a clear indication of the lack of such studies. This is not to say that researchers have not focused their attention on such studies (see Dhillon 2001; Schultz 2002; Magklaras and Furnell 2005). However, limited studies on computer fraud committed by *insiders* and misconceptions concerning such acts (Schultz, 2002). In addition, the growing problem of computer crime is further compounded by the fact that such cases are not restricted to one particular country.

Against this backdrop, the focus of the paper is on computer fraud, one type of computer crime committed by employees. This is based on the argument that such employees plan their acts and take 'calculated risks' to intentionally abuse computers resulting in the violation of safeguards by trusted employees. Consequently this paper argues that onus of detecting and managing computer fraud committed by employee(s) lies within the organisations itself. Therefore solely relying only on current legalisation and other sophisticated measures alone are inadequate for the managing the occurrence of computer fraud committed by employees in particular. For the purpose of this paper, computer crime can result from incompetence, ignorance, negligence in the use of IT or deliberate misappropriation by individuals. Intentional illicit activities such as fraud, virus infections, illicit software, theft of data and software, unauthorised private work, invasion of privacy and sabotage are all examples of computer crime. Computer fraud (one type of computer crime), on the other hand is defined as a deliberate misappropriation by which an employee tries to gain unauthorised access to the organisation's computer systems. The misappropriation itself may be opportunistic, pressured, or a single-minded, calculated plan.

This paper is divided into five sections. After a brief introduction, section 2 reviews some of the main reports and surveys to illustrate the seriousness and complexity of the ever-increasing problem of computer crime. It also discusses various challenges posed in managing computer fraud. This is followed by section 3 that focuses on legal issues in the context of management of computer fraud. In doing so, it identifies the emergent issues of concerns and shortcomings in the existing legalisation. Finally a discussion is presented in section 4, followed by a conclusion in section 5.

2 SERIOUSNESS OF THE PROBLEM OF COMPUTER FRAUD WITHIN ORGANISATIONS

Most reports and surveys advocate that figures representing computer crimes are only the *tip of the iceberg*. This could be attributed to perhaps the reluctance of organisations fearing the unnecessary media publicity, in particular, of those crimes committed by their employees (Smith 1988; Icove et al; Fox 1998; Audit Commission 1998, 2001 and 2005). Consequently, any attempts to estimate the actual costs of such offences are speculative. Having said that, the volume of reported cases indicate that the potential impact of computer crime within organisations are indeed large. For example, computer crime costs US organisations more than $400 billion annually. Similarly "2002 Computer Crime and Security Survey" conducted by CSI/FBI reflected that 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months. Although, CSI/FBI survey categories encompass incidents that could potentially have come from either sources (for example theft of proprietary information, sabotage of data networks, and virus), three of them very clearly illustrate the origin. It is evident from the figures highlighted in such reports that although relate to a period over where the proportion of *outsiders* had exceeded *insiders*, the quantifiable losses in the latter case dwarf those attributable to *outsiders*. Similarly the three reports (1998, 2001 and 2005) on computer crime by the Audit Commission illustrated a 38% increase of fraud within organisations. This is far out weighed by the staggering near five-fold increase in the number of reported cases of viruses. Other types of computer crime show significant increase also, albeit frequently from a small base. Another report by the High Technology Crime Investigation Computer Forensics and Digital Evidence Report indicated that over 25% of all

Fortune 500 organisations have been victimised by computer crime with an average loss ranging from $ 42 million to $10 billion.

Against this backdrop, it can be argued that computer crime unlike other traditional crimes tends to defy quantification. Attempts to estimate the actual costs of such offences and what proportion of computer crime is exactly committed by employees are speculative. Nonetheless the extent of damage gauged from the findings of various recent reports and surveys mentioned above indicates that the potential impact of computer crime is large. Consequently the seriousness of the problem cannot be underestimated.

2.1 Complex Nature of Computer Fraud

While trying to understand the occurrence of computer fraud, there has been a tendency in official reports to individualise computer fraud, attributing the blame to the 'rotten apple in the barrel' (for example, see Doig 1984; Kesar and Rogerson 1998). As a consequence, many researchers believe that employees who engage in computer fraud are normally motivated by greed, selfishness and individualism that are inherent in the values of capitalist society which, could turn an otherwise trusted employee into an embezzler or saboteur (see Davies 1990; Croall 1992; Icove et al 1995; Parker 1998). Such issues can be also be associated with complex human emotions and needs such as financial pressure that Croall (1992), for example, considers the initial motivation for computer crime. However, Cressey (1986) adopts a different viewpoint, which is a more individualistic approach to explain the causes of computer crime. He relates activities such as embezzlement to personal, non-sharable and financial problems. There have also been attempts to examine what, if any, characteristics distinguish these individuals. For example, Parker (1984; also see Parker 1998), outlines some characteristics of such offenders (he also focuses on some characteristics of hackers). Similarly Goodwin's (2000) article indicated that disgruntled employees can also be a major threat, particularly if they understand IT. The Barings Bank case, for example, reflects computer fraud committed by a low status 'rogue trader' employee. Nicholas Leeson, a former employee of Barings Bank engaged in computer fraud that allowed him to conduct illicit trading for almost three years with being caught (for details, see the Bank of England Report 1995; case study described in Rawnsley 1995 and Kesar and Rogerson, 1998).

Against this backdrop, it is difficult to determine the different status levels of employees involved in such acts but there is often a tendency in official reports to individualise such activities by attributing it to personality traits or personal problems of individual offenders (Croall 2001). Public media, in the UK for example, tend to focus on cases where the major themes are "fall from grace" of "wealthy and extravagant lifestyle" of the offenders (Levi 1999, pg 48). For example, subsequent investigation into Leeson's illicit trading activities pointed out that the change of flux involving a combination of ambitious internal reconstructing, integration of the bank and brokering operations created *weaknesses* within the Bank. In other words, a primary reason for the collapse of Barings Bank was the absence of appropriate safeguards (such as diffusion of responsibility) that created a situation where Leeson took advantage of the loopholes in management practices to engage in illicit trading. This is not surprising as most reports and surveys also claim that computer fraud is not particularly sophisticated or complex but mostly relies on the lack of basic security procedures (Audit Commission 2001; Ernst & Young 2004; CSI/FBI 2004; CSI/FBI 2004; Audit Commission 2005). Leeson, for instance, was able to circumvent management, who were responsible for internal and external auditors, internal controls and regulatory bodies in both Singapore and the Bank of England (for details, see restructuring of Barings Bank &Co and Barings Securities Limited in the Bank of England Report 1995; also see detailed description of the case in Kesar and Rogerson, 1998.

The example above also provides more complex messages. Whether such acts took place because the offender was motivated by personal gain or by the profitability of the organisation is an important question. In both cases, researchers believe that the characteristics of the offender also play a significant role (Croall, 2001).

Sweeping though these generalisations, it seems that considering the personal traits of the offender may be important; but there is little evidence to support any association between computer crime and individual pathologies (*ibid*). While considering the personality traits of an offender does provide a starting point for investigating the occurrence of such illicit activities, the problem arises when studies tend to be more focused on the "rotten apple in the barrel" (Doig 1984) and aim to chalk out either the characteristics of the offender, or attempt to answer the question "how does such out-of-character" computer crime occur. In their study, Parker and Nycum (1994) outlined some characteristics of such offenders who engage in hacking. Similarly, Cressey (1964) studied the cases of hundreds of embezzlers using symbolic-interaction theory to understand the characteristics of potential offenders. Other studies link computer crime with business success (Box, 1983). However, evidence to suggest that all offenders who engage in computer related crime like fraud within organisations are 'bad people', is an assumption that can be challenged (Punch 1996, pg 84). This is because the relationships between individual, organisational and sociological factors also play an important part in the occurrence of computer fraud (see Schrager and Short 1997, pg 410).

In trying to understand computer fraud within organisations, the above approach tends to serve as an ideological function where the focus diverts attention from the "barrel" (Doig 1984), which include practices and other issues associated with the organisation itself. This strengthens the contention that individual explanations, although often associated with computer crime, is however, limited in explaining the underlying causes of such acts. In this context, Croall (2001) further advocates "Individual motivations must be located in the wider context of the organisations in which the offending takes place and the cultural values that encourage or discourage offending" [Pg 84].

In the light of this, traditional criminology studies that focus on criminal motivations of individuals now have been generally dismissed as superficial and over-generalised by most researchers (for example, see Braithwaite 1984; Nelken 1997). Slapper and Tombs (1999), for example argue that the so called "general theories" do not explain the criminal values or how crimes originate and may therefore explain the perpetuation of crime but not its origin. Researchers like Clarke (1997) believe that two main 'mistakes' are made by traditional criminology. Firstly, criminologists assumed that understanding the crime is the same as understanding the criminal (Gottfredson and Hirschi 1990). Secondly, the misconception relates to the aspect of crime control versus dealing with the criminal (Wilkins, 1990) which asserts that the solution of reducing crime implies a focus on the criminal. Within Information Systems (IS) studies, these types of control to combat computer related criminal acts, such as fraud, general deterrence theory from criminology has been used to predict the use of deterrent security countermeasures such as IS security polices and guidelines, security awareness programmes and preventative security software. These deterrent measures are applied with the idea that they will 'lower' abuse of information systems by convincing potential offenders (employees) that there is too high a certainty of getting caught and that punishment can be severe (Straub and Welke, 1998). Information systems researchers have relied on deterrence theory, which although useful, has been recently criticised for its limitations (see D'Arcy and Hovav 2004). Nonetheless researchers are consistent to claim "Deterrent efforts correspond to certainty of sanctions because the amount of such efforts directly affects the probability that IS abuser will be caught" (Kankanhalli et al. 2003, pg 141). This again is dependant upon the working environment of the organisation. Therefore, an employees' perceptions of threats imposed by 'deterrence security mechanisms' may not be directly proportional to the actual level of controls and safeguards implemented within an organisation (D'Arcy and Hovav 2004). Consequently, researchers argue that it is the perception of sanctions themselves that can lead to deterrence (Gibbs, 1975; Tittle, 1980; Straub, 1990; Kankanhalli et al. 2003). Researchers have also pointed out the need for such studies to take into account the impact of individual characteristics such as gender and age (D'Arcy and Hovav 2004). Overall, the general theory of deterrence does provide a sound theoretical justification for the use of deterrent countermeasures as a means to limit acts of computer related crimes committed by employees it nevertheless, is a partial viewpoint to understand the complex nature of such illicit acts.

Differing in its focus from most criminology studies is a relatively new school of thought, Situational Crime Prevention (SCP), where the emphasis is more on the criminal settings, rather than the criminal (Clarke, 1997). Thus, rather than detecting or sanctioning offenders, the starting point of SCP is to circumvent the occurrence of generic crimes and to reduce criminal tendencies through enhancement of society, like better housing or education. Little attention was given to this new school of thought by criminologists and policy-makers until Clarke's seminal work in 1997. Similarly, Croall (2001) suggests that most of the earlier theories that focus on individual choices to commit crime tend to exclude white-collar offenders, and are therefore considered inappropriate. This is important to note since computer crime, as argued by various researchers is a form of white-collar crime (for different viewpoints, see Perrolle 1987; Johnson 1994; Maner 1996; Hollinger 1997).

From the above discussion so far, it becomes clear that computer crime is complex in nature and encompasses different types of acts. Moreover it can be argued that the complexity associated with computer crime within organisations can be fully understood when personality traits are seen in the context of the wider organisational issues, which is a pre-requisite for participation in such offences (also see Mars 1982; Dhillon and Backhouse 1996; Dhillon 1997; Kesar and Rogerson 1998; Audit Commission 1998; Dhillon 1999). This is because reports and survey indicate that a failure in basic controls is still a problem within organisations. As noted earlier, this manifests itself as the failure of some organisations to implement even the most basic controls, thereby leaving information systems vulnerable. Consequently, some studies link computer crime, fraud committed by employees particularly with wider organisational and structural problems such as diffusion of responsibility within organisations (Audit Commission 2005). Hence, it can be argued that lack of basic safeguards can create an environment in which, employees do not directly feel responsible for the consequences of their actions. In such a situation an employee can perhaps justifiably blame the consequences on another employee (Harrington 1995). Therefore such employees are less likely to suffer from guilt from committing an action that may have been law breaking (for examples, see Gotterbarn 1991; Croall 1992; Nissenbaum 1994; Johnson and Mulvey 1995; Laudon 1995; Kesar and Rogerson 1998). Such a climate created by top management within an organisation can indeed be conducive to computer crime.

It is perhaps evident that such a climate, as described above, can provide potential offenders with suitable opportunities for ready misappropriation of information systems within an organisation (for examples, see Angerfelt 1992; Audit Commission 1994; Gapper and Denton 1996; Pearson 1996; Audit Commission 1998; Walsh 2000; Power 2001). The 2001 and subsequently the 2005 Audit Commission Report, for example, characterised organisational problems such as a lack of safeguards, together with ineffective monitoring and lack of internal audits as the basis of opportunities for occurrences of computer crime. Some of the principle weaknesses cited by offenders were poor administrative practices such as inefficient password policies, out of date technical knowledge, and lack of security software within organisations (for examples, see Oz 1994; Forester 1994; Audit Commission 1998; Goodwin 2000; Power 2001). As mentioned earlier, it is difficult to estimate exactly what proportion of fraud is committed by high or low status employees, never the less there are indications that potential offenders can also take advantage of given suitable opportunities where organisations have failed to take the necessary precautions (see, for example, Vitell and Davies 1990; Peterson 1994; Rawnsley 1995). Moreover, depending on the occupations, some organisational structures would provide more opportunities than others (for example, see Mars 1982, who categorises occupations on the basis of various opportunities within an organisation). This perhaps explains why the figures reflecting the occurrence of computer crime committed by employees are increasing in number.

Discussion so far sheds light on the complex nature of computer fraud committed by employees, in particular. Indeed some of the issues classified above cannot be easily explained by irrational impulses or personality problems (Croall 1992). Consequently there are many challenges posed in managing such illicit acts, particularly those committed by employees. These are discussed below.

2.2 Challenges Posed for Management of Computer Fraud

The advent of IT also poses many challenges to organisations in trying to manage computer crime like fraud committed by employees. Traditionally, security has often been associated with locks, barriers and uniformed guards (Parker 1981). However, it was soon realised that tangible technical measures had to be taken to overcome threats like computer crime. Research, so far, has provided conflicting evidence about how far top management is implicated in offences and about how well informed they tend to be. There is probably a considerable variation within top managements, but they do play an important role in influencing the internal structure of the workplace, and that has a direct relationship with the occurrence of computer fraud committed by employees (see Turner 1994). Mintzberg (1983), for example maintains a similar viewpoint that is supported by the notion of a system of ideology. Clinard and Yeager (1980) on the other hand, note that the size and delegation of duties within large organisations, for example, can produce an environment favourable to the commission of computer crime. Consequently this indicates that top management can use their authority within the organisations to circumvent control at the operational level (Croall 1992; Clarke 1990; Braithwaite 1984; Braithwaite 1985; Audit Commission 1998, 2001 and 2005). Hence influence, whether internal or external, on this norm structure can result in the individuals within organisations being divided, thus creating a subculture within an organisation. Such a subculture is often interpreted as a more-or-less organised response on the part of employees to organisational structures, managerial policies or payment systems (Mintzberg 1983; Croall 1992). Indeed this indicates that subcultures can arise in response to particular aspects of the technological and social organisation of work. As mentioned earlier, organisations that rely heavily on IT will become vulnerable to intentional illicit activities committed by employees.

3 LEGALISATION AND COMPUTER FRAUD

Indeed IT offers some new and highly sophisticated methods for law breaking, which in turn, create the potential to commit traditional types of crimes in non-traditional ways. Cases of computer crime that result in computer fraud, theft and sabotage are constant reminders of a growing problem for the international society today. In light of this, this section reflects on some of the major divergent approaches used to manage computer fraud committed by employees, in particular.

Different jurisdictions have tried to tackle computer crime using a variety of instruments depending on the different ways in which, they have been affected by such acts (Jones 1992). Such is the concern for computer crime that the attention of international organisations such as the Organization for Economic Co-operation and Development (1986), the International Chamber of Commerce (1988) and the Council of Europe (1990), amongst many others, have focused on the question. A discussion about various guidelines available for policy makers and legislators in the context of the focus of this paper follows.

The Organisation for Economic Co-operation and Development (OECD) of thirty industrial market-economy nations examines issues involving economic, social and governance challenges of a globalised economy. The Council of Europe has produced guidelines for policy makers and legislators in dealing with computer crime. In 1983, OECD undertook a study of the possibility of an international application of legislation to address the problem of computer crime. As a result in 1986, it published Computer-Related Crime: Analysis of Legal Policy, a report that surveyed the existing laws and proposals for reform in a number of member states. In addition, it recommended a minimum list of misuses that countries should consider prohibiting and penalising by criminal law, such as fraud and forgery, alteration of computer programs and data and copyright violations. The Computer and Communication Policy Committee also suggested that criminal protection should be developed against other types of abuse, including theft of trade secrets and unauthorised access to, or use of, computer systems.

Following the completion of the OECD report, the Council of Europe (1990) initiated its own study to develop guidelines to assist legislators. Hence the recommendations of the Council of Europe on computer crime contained guidelines for nation legislation that in effect was adopted by the Committee of Ministers of the Council of Europe on September 13, 1989. Further, in 1992, the OECD developed a set of guidelines for the security of information systems. The main aim of these guidelines was to provide a foundation on which the State and the private sector can construct a framework for the security of IS. Although a study was conducted by the Council of Europe that concentrated on procedural and international co-operation issues related to computer related crime, much of the international work has so far been centred in Western European and OECD countries. On March 1997, the OECD issued further guidelines to address other information security concerns like Cryptography (Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security). This was adopted by the OECD Council on July 25, 2002.

Further expanding work undertaken by the OECD, and the European Committee on Crime Problems of the Council of Europe developed a set of guidelines for national legislators that enumerated activities that should be considered as a subject of criminal sanction. Rather than attempting to define the term 'computer crime', they left individual countries to adapt to the functional classification of their respective legal systems and historical traditions. In addition, The Council of Europe's European Committee on Crime Problems 1990 proposed a three-step approach towards addressing international computer crime that included measures to improve international collaboration. More recently, the Council of Europe has been addressing the problem of the increasing number of computer crimes linked with the Internet. Most countries have directed their attention towards legislation as a treatment to combat computer crime, in consequence some form of legislation exists in each country to address such activities (see, BloomBecker 1986; Shackelford 1992; Hollinger 1997; Reed and Angel 2000). In formulating legislative responses to computer crime, three alternative approaches have been identified in the literature (for details see, Jones 1992; Shackelford 1992; Walden 2000): The evolutionary approach; Amending existing statutes; and Enacting computer-related statutes.

The first approach, the evolutionary approach, deals with the application of the general criminal laws by expanding concepts and definitions to include certain types of computer crime. The second approach, amending existing statues, is when countries actually amend their existing laws to include additional offences such as computer fraud (for example, West Germany, amended its 1987 Penal Code to include an additional fraud offence of 'computer fraud' and the Swedish Data Act 1973 was amended in 1982). The solution of enacting computer-related statutes is a third approach, which large jurisdictions either adopted or proposed (some of the legislation such as the Computer Misuse Act and The Computer Fraud and Abuse Act will be discussed in later sections). In Europe, countries such as Austria, Denmark, France, Germany and Greece, for example, had made extensive amendments to their existing criminal law by 1990. Since then, however, countries such as Spain, Portugal and the United Kingdom have introduced laws dealing with computer crime. Other countries such as Japan, Canada and the United States of America (both at a state and federal level) have introduced new statutes (Note that because countries such as Canada, United States and Australia, are federal states, the position is further complicated). In light of this, many countries, in aiming to prevent unauthorised access to and tampering with information systems, have adopted or amended their existing legislation. In response to increasing incidences of computer related crime, Hong Kong, for example developed their first legislation that specifically addresses such issues (see Kennedy 2001). Further the changing nature of computer crime (computer fraud in particular), Australia introduced the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill on 24 November 1999, which proposes the implementation of the Model Criminal Code offences on this topic. The policy was updated in July 1999, and since then consultations have been taking place with relevant Commonwealth agencies in Australia. The United States and Great Britain are just two of the many countries that have enacted national legislation in response to the growing problem of computer crime (also see introduction on key developments regarding European Computer Law, see edited book by Reed and Angel 2000). As mentioned earlier, two main pieces of legislation that were developed directly to deal with computer related issues are: The Computer Fraud and Abuse Act of 1986 and The Computer Misuse Act of 1990. Given

the focus of this paper, brief discussion of these Acts will provide useful insight into the approaches adopted to manage computer fraud within organisations. The Computer Fraud and Abuse Act of 1986 (CFFA) became the first piece of legislation specifically targeted at deterring and punishing computer crime at the federal level in the United States, while the Computer Misuse Act became a law in the United Kingdom to deal with cases primarily linked with computer crime. A brief discussion of the contents follows.

3.1 The Computer Misuse Act

The seeming inability of current legislation to cope with hackers was one of the main reasons to set up a Royal Commission to look at the whole area of computer crime. As a consequence, to halt computer crime, the United Kingdom promulgated the Computer Misuse Act of 1990. It is believed the primarily motivations for the government support were similar to the reasons given when the Data Protection Act (DPA) was first introduced into Parliament in 1983 (Walden 2000). In an attempt to encompass a wide range of computer related crime, the Act's eighteen sections employs broad language to define these substantive offences (Shackelford 1992). When the British Law Commission analysed computer related crime statutes in other jurisdictions, it found that each had approached the issue from different perspectives, resulting in substantially different offences, where most of these statutes attempt to criminalise the same basic activities. The Commission also found that countries generally adopted one of three alternative approaches, mentioned above, to computer crime. Based on the Commission's recommendations, Parliament adopted a half-way approach whereby "new offences are created only when necessary to encompass computers" (Shackelford, 1992). Further Shackleford acknowledges the several advantages that this half-way offers. At the same time, he points out that the computer-specific enactment, if drafted properly, and in turn adopted by many countries, would serve as a "basic mechanism for addressing the international aspects of computer crime". Again the three offences of the British Misuse Act (also see Elbra 1990) are: Intentional and knowing unauthorised access to any computer, or the programs or data contained therein, or any attempts to gain unauthorised access, including exceeding authorised access; Unauthorised access as defined above, with the intent to commit or facilitate a further offence and intentional and knowing unauthorised modification of the contents of any computer.

3.2 The Computer Fraud and Abuse Act

The Computer Fraud Act of 1986 was signed as a law to clarify definitions of various computer related crimes. It was a culmination of several years of discussion and research among legislators. The Computer Fraud and Abuse Act of 1984 (CFFA) was amended with the Computer Fraud and Abuse Act of 1986 (the '1986 Amendment'). This Act extended the scope of the previous Act and clarified some of the ambiguities in the original piece of legislation. Consequently, the Act enhanced and strengthened an intermediate Fraud and Abuse Act established in 1984. Subsequently, it also complemented the Electronic Communications Privacy Act of 1986, which outlawed the unauthorised interception of digital communications. Further, the CFAA provides additional penalties for fraud and related activities with regard to access devices and computers. This legalisation is related to federal privacy protection to computerise information maintained by financial institutions and clarifies unauthorised access of computers used by the United States government. The three new offences this particular legalisation describes are: unauthorised computer access with the intention to defraud, malicious damage via unauthorised access and trafficking in computer passwords with the intent to defraud.

A wide ranging definitions of 'computer' has been given in the US Federal Computer Fraud and Abuse Act, 1984: The term 'computer' means an electronic, magnetic, optical electrochemical, other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Many jurisdictions have

provided similar definition to the term additional to that of 'computer' (for example, see California statues for the definition of 'computer network' or the Canadian Criminal Code for the definition of 'computer program').

Various pieces of legislation have been used to prosecute offenders who commit crime. Perhaps the two most prominent cases to 'test' the new legislation of The Computer Fraud and Misuse Act are Robert Morris (a twenty two old graduate student at Cornell) and the Herbert Zinn (a high school drop out). Both these cases involved unauthorised access into computer systems (for details, see for example, Johnson 1994). Purging the 'worm' (Morris created a 'worm' that crashed computer systems) from computer systems cost organisations several days of production and millions of dollars.

3.3. Legal Challenges in the Context of Management of Computer Fraud

Most researchers and information security practitioners agree that with the advent of IT, one of the main threats relates to corporate data. It is often assumed that organisations are future oriented, concerned about their reputation and 'quintessentially rational' (for example, see Braithwaite and Geis 1982). The lack of boundaries and physical constraints, combined with both the speed in which transactions takes place and the magnitude of intentional harm, have indeed changed many of the traditional paradigms of criminal law. As mentioned above, the two Acts discussed above were specifically developed to deal with computer crime. This is not to deny that other existing Acts can be used in dealing with the issues associated with computer crime. Consequently what has been observed is that in the past few years, due to IT, change resulted in revisions of the existing laws and development of new ones necessary to combat the increasing problem of computer fraud.

International organisations, such as OECD, the Council of Europe, and the United Nations have a key role to play to help organisations combat computer related crime, nonetheless they are dependent upon the actions of national governments in passing appropriate laws and seeking international agreements. Also the private sector has a part to play in persuading national governments to take the necessary steps in combating computer crime. Consequently just to rely on such bodies can indeed be time consuming. The debates associated with 'Cyber Crime', for example, continues to shows signs of no consensus reached due to the very complex nature of computers (for examples, see the CERT report). In addition, the existing English laws, like the Theft Act 1968, Walden (2000), for example, states that either the legislation was drafted in an era before the emergence of such technology was envisaged, or because statutory drafting has failed to be robust enough to appropriately address information technology. He compares fraud, criminal damage, obscenity and forgery cases that involve computers with the traditional existing criminal legislation to prove his point. Thus broadly speaking, we have seen legislative attention to computer crime grow dramatically in the early 1980s, as computers became increasingly central to organisations to the conduct their business. In their paper, "The process of criminalisation: the case of computer crime laws", Hollinger and Lanza-Kaduce (1997) analyse the process by which recent laws related to computer crime have been formed. They state: "Individual reformers, rather than widespread grass roots social movements of economic interest groups, have been the principal force behind the passage of computer crime legislation…those who were most influential in the formation of computer crime laws have been computer abuse 'experts' and legislators". Furthermore Hollinger and Lanza-Kaduce believe that computer crime laws possess a significant symbolic component. Andeneas (1987), on the other hand believed that computer crime laws are symbolic in that they 'educate', 'moralise', or 'socialise' computer users. He justifies his statement by giving an example of the development of occupational codes of ethics by data management professional organisations after criminalisation was virtually completed (see Johnson and Snapper 1985; Johnson and Nissenbaum 1995). No doubt the analysis of Hollinger and Lanza-Kaduce (1997) does provide a useful insight, however, as pointed out by Raymond (1997), it does not identify any methods through which media presentations about the harm of uncontrolled computer access resulted in computer crime legislation. Consequently, if computer crime legislation is symbolic, then it leaves several important questions

unanswered. Subsequently it is important to understand and identify the roots of this symbolism (for details, see Raymond 1997).

The Computer Misuse Act, on the other hand, has been criticised for the notable omission of an actual definition of the term 'computer' (Hollinger 1997). Although the Law Commission felt is was not necessary to include the definition, Hollinger believes that was perhaps an unwise decision since: "All the attempted definitions that we have seen are so complex, in an endeavour to be all-embracing, that they are likely to produce extensive argument and thus confusion for magistrates, juries and judges involved in trying our proposed offences". According to Walden (2000) it is potentially extending its scope to "everyday domestic appliances and cars that incorporate computer technology". Having said that, the Law Commission found support for a general view not to define terms like 'computer', since they believed that if defined, they would be "so complex, in an endeavour to be all-embracing, that they are likely to produce extensive argument". This viewpoint also has been adopted by other jurisdictions, such as France and Germany, the United States being an exception, where they have actually defined 'computer' in the Computer Fraud and Abuse Act. Although improvements were made in the Computer Fraud and Abuse Act (CFAA), as pointed out by Hollinger (1997) it nevertheless lacks a clear definition of important terms such as 'access', 'effects', and 'use'. In spite of the writer trying to simplify the language of CFAA, it seems difficult to comprehend (for example, see Johnson 1994). The Computer Misuse Act was essentially designed to make 'computer hacking' an offence (Rigby 1994), however it mainly deals with computer crime specifically related to government and financial institutions. With regard to CFAA, many argue that it has loopholes and ambiguities that make it difficult to prosecute (Kluth 1990). Prosecution of Robert Morris for the "Internet worm" (as mentioned above), for example, and the ensuing debates illustrate the loopholes and ambiguities in legislation that was developed to deal with computer crime in the first place. In addition, legalisation addressing cybercrime is further complicated from such Acts can be subject to state and federal level (or different countries). In fact, multiple prosecutions are possible for various offences arising out of the same computer related criminal act. Regardless of the nature of computer crime, in US the enforcement and prosecution for all crimes are covered by federal and criminal statues. This requires two elements. First the government must prove a criminal act (*actus reus*)-that is the government has to make the act a crime before the offender may be charged with a criminal act. Second, the government must prove a criminal intent (*mens rea*). The main challenge with this element is that the so-called criminal intent is not clear. Indeed both these elements, particularly in the context of computer fraud committed by employee(s) poses many challenges.

Against this backdrop, the lack of any international agreement for addressing computer related crime and the mechanism for dealing with international computer fraud would be in place but inoperable (for details, see Shackelford 1992; Rigby 1994). No doubt many countries have addressed the increasing incidences of computer crime but like other legislation, it too has been criticised for its ineffective implementation. For example, in March 1992, the Hong Kong Government passed for the first time a bill on computer crime (Kennedy 2001). Lee's 1995 paper critically examines the provisions of this law and their implications for information systems security, in particular). Consequently investigations involving cases of computer crime cases, and in consequence the gathering of appropriate evidence for a criminal prosecution, can prove to be extremely difficult and complex not to mention time consuming. This is primarily due to the intangible nature of data, especially in networked environments within organisations (see Shackelford 1992). Walden (2000), for example, believes that IT renders the process of investigation and recording of such cases vulnerable to claims by the defence of "error, technical malfunction, prejudicial interference or fabrication". This viewpoint can lead to a ruling from the court against the admissibility of evidence. Further researchers also have pointed out that existing laws cannot be applied easily to deal with computer related crime and so additional substantive legislation is required (for example, see Bainbridge 1996). The question is whether any useful lessons can be learned from such Acts (for example, the Computer Misuse Act). Although in theory many forms of computer crime could be dealt with using existing legislation, in practice prosecuting people who are involved in computer misuse is hard and demanding (see the case of Craig Neidorf in Spinello 1997). This problem is further

exacerbated as most organisations for various reasons are reluctant to report computer crime cases, particularly those involving their own employees.

In discussion the shortcomings of existing legalisation, Harrington (1996), for example, compares the Codes of Ethics and law, since she believes that they are "formal sanctions studied as part of deterrence research". She justifies her analogy by stating that codes have the same underlying mechanisms as laws and other legal sanctions, as both aims to reduce incidences of illicit activities such as computer misuse. In the context of computer fraud, Harrington found that codes of ethics do have an effect, but they are related only to certain abuses. Oz (1992), on the other hand used a framework to compare different codes of ethics. Furthermore, Johnson and Snapper (1985) question the use of the codes and their implications for professional behaviour and the real meaning of their ethical demands. Thus they believe that such codes leave a number of questions unsettled. No doubt codes of ethics have been developed to provide guidelines for computer professionals, but these codes have certain inherent limitations since they do not necessarily make a person behave ethically (for example, see Johnson 1985; Forester and Morrison 1994; Harrington 1996). It is beyond the scope of this paper to discuss the critique on such codes. However the lack of positive findings for the effects of codes in the context of management of computer crime acts like fraud occurring from within the organisation does strengthen the argument that laws and other measures alone are not enough to combat this serious growing problem.

4 DISCUSSION

Employees at all levels of the occupational hierarchy can have many opportunities to misuse their occupational roles that can result in computer fraud. Indeed different jobs provide a different 'illegitimate opportunity structure' within organisations for employees to exploit. However, it is important to note that not all employees exploit opportunities within organisations. Whether they do or not may well be related to other aspects of the social organisation of work (Croall 1992). Nonetheless, employees can profit economically if they have access, which can readily be used. These opportunities are in turn related to the way in which a particular occupation is organised and to the level of supervision that exists within the organisation. In light of this, when considering effective measures to manage computer fraud committed by employees in particular, perhaps the first thing that comes to mind to an organisation as a means of protection is the development of 'security' techniques and legalisation. However organisations cannot rely solely on technical or legal measures to protect their businesses from threats that occur due to violations of safeguards by trusted employees. This is because employees who intent on gaining unauthorised access through deception usually discover the weaknesses and vulnerabilities of new technology long before the agents of society and law enforcement (see Croall 1992; Hollinger 1997). When the offender is an employee of the organisation, the difficulties of prosecuting them is further exacerbated, for relatively few employees have been brought to the court. Such a paucity of prosecution has been attributed to a range of reasons (also see Parker 1976; Bequai 1983; Parker and Nycum 1984; Croall 1992; Walden 2000). Firstly, fear of adverse publicity makes organisations hesitant to report the cases of computer crime committed by their employees. Secondly, lack of adequate training within prosecuting authorities. Thirdly, the trans-national nature of computer related crime and the associated jurisdictional problems (for example, complexity of collecting, investigating, and prosecuting the offender). Finally networked environments within organisations can exacerbate the problems of obtaining evidence and subsequently presenting it before the courts. Indeed unfavourable publicity and long investigations, prosecutions and trails can, to some extent, act as deterrents. Consequently, it is often assumed that the major aim of sentencing offenders is deterrence (Croall 1992). This reflects a general view that offenders are deterrable, since the focus here is on those employees who take 'calculated risk' to take advantage of the weaknesses of IS. Nonetheless, this deterrent potential can be undermined by the low rate of actual detection and prosecution of employees who engage in computer fraud within organisations (for example, see Bainbridge 1996). Consequently it can be argued that preventive measures taken within an organisation have a better preventive effect than penal laws, as we can see from the

difficulties and complexity involved in prosecuting offenders. Some researchers believe that a lack of prosecutions under the CFAA could also be attributed to issues unrelated to the Act (Bainbridge 1996). As a result, these can create significant challenges for organisations. In addition the cost involved in the process of prosecuting an offender can be very high. Indeed there is a paradoxical tension between the benefits that computers can bring to society and the potential for serious abuse, and this presents a rudimentary dilemma for organisations. Given the ambiguities and loopholes existing in computer laws perhaps explains why some of the computer related crimes are dealt with as 'theft' by organisations (Lloyd 1990).

Against this backdrop, it is clear that it is not just flaws in computer criminal acts that lead to a lack of prosecution, but issues, which simply cannot be dealt with by legislation and other technical measures. Many questions are also raised to and whether threats from computer fraud and sabotage are amenable to effective treatment just by applying technical approaches (for example, Loch et al 1992; Dhillon 1997; Parker and Nycum 1984; Dhillon and Backhouse 1995; Dhillon 1999, Dhillon 2000). No doubt risk evaluation or determination of security policies and procedures will enhance the effectiveness of security within an organisation. At the same time, it is important to be aware that management of computer fraud committed by employees in particular warrants a consideration of self-regulation where sophisticated security measures do not contain only technical issues but also consider issues related to the underlying causes of such intentional illicit acts. In other words, the onus for preventing and managing such acts committed by employee(s) lies within organisations themselves. This is because opportunities for computer misuse may well be spread within an organisation, but different responses arise from various pressures and working conditions which may originate within organisations or from outside. Consequently, such factors have a profound significance for analysing and understanding the complex nature of computer fraud.

Neumann (1991), for example provides a good argument that is particularly worth noting in the context of management of computer fraud within organisations. He advocates that management needs to consider security as both a functional and behavioural issue. In addition, it has been suggested that steps could be taken within organisations to educate employees about the dangers that both the employees and the organisation can face from such threats. This is because when employees are aware of the consequences of their behaviour, they become "part of the security program" (Spafford et al 1989).

5 CONCLUSION

The management of computer fraud committed by employees in particular is a multi-faceted problem that is being addressed by researchers and practitioners alike. Indeed it looks quite different from different points of view: the victims, the perpetrators, law enforcement officers, prosecutors, computer professionals and criminologists. Nevertheless, the discussion in this paper reveals that by far one of the greatest threats to an organisation comes from within, where employees may gain unauthorised access to information systems and intentionally committed computer fraud. No doubt the advent of IT has created unprecedented opportunities for the occurrence of computer fraud, particularly those committed by employees themselves. With this in mind, the main contribution of this paper has been to enhance the awareness about management of computer fraud committed by employees in particular. Critical reflection on various laws about computer related crime illustrated two main problems: establishing jurisdiction over alleged offenders and establishing identities of the alleged offender.

To conclude, it can be seen that management of computer fraud is not so straight forward. Neumann's (1991) highlights three gaps that he believes may permit such illicit activities. The first gap he identifies as a 'technological 'gap', which stresses technical deficiencies in both hardware and software. The second gap, the 'socio-technical gap', refers to the gap that divides computer-related policies and other issues such as computer crime laws, codes of ethics and standards of good practice. Finally the third is the 'social gap', which relates to social policies and actual human behaviour. Neumann goes on to explain the significance of such gaps and

developments and methods that could be applied to narrow them. Addressing computer related crime specifically, Patrice Rapalus, CSI Director (Source: http://www.gocsi.com), remarks in the "Computer Crime and Security Survey," indeed strengthens the argument presented in this paper:

"Over its seven-year life span, the survey has told a compelling story. It has underscored some of the verities of the information security profession, for example that technology alone cannot thwart cyber attacks and that there is a need for greater cooperation between the private sector and the government. It has also challenged some of the profession's 'conventional wisdom,' for example that the 'threat from inside the organization is far greater than the threat from outside the organization' and that 'most hack attacks are perpetrated by juveniles on joy-rides in cyberspace.' Over the seven-year life span of the survey, a sense of the 'facts on the ground' has emerged. There is more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace. Post-9/11, there seems to be a greater appreciation for how much information security means not only to each individual enterprise but also to the economy itself and to society as a whole. Hopefully, this greater appreciation will translate into increased staffing levels, more investment in training and enhanced organizational clout for those responsible for information security."

Keeping in mind Neumann's three gaps and comment by the Director of CSI, this paper has contributed to enhance the awareness about the underlying causes of computer fraud and consequently promote a better understanding of the complex nature such act committed by employees in particular. Further it has provided an in-depth discussion on computer crime laws to reveal that such laws alone are still inadequate to deal with the emerging adverse consequences linked with IT (computer fraud within organisations in particular). In other words it has addressed what *can* be done rather than what *needs* to be done in the context of management of computer fraud committed by employees (Baskerville 1993).

REFERENCES

1. Angerfelt, B. (1992). Computer crimes-a study of different types of offences and offenders. Eighth IFIP International Symposium on Computer Security, IFIP Sec '92, Singapore, 27-29 May 1992, Elsevier Science Publishers B.V. (North Holland).

2. Audit Commission (1994). Opportunity makes a thief- an analysis of computer abuse. London, HMSO.

3. Audit Commission (1998). Ghost in the machine- an analysis of IT fraud & abuse. Milton Park, Abingdon, Oxon, HMSO.

4. Audit Commission (2001). Your business@ risk: an update of IT abuse 2001, London, Audit Commission Publications, HMSO.

5. Audit Commission Report, (2005). ICT Fraud and Abuse 2005. London, HMSO.

6. Bank of England Report, 1995, "Report of the Board of Banking Supervision: Inquiry into the Circumstances of the Collapse of Barings", HMSO. Extract from the conclusion of the Bank of England Report on the collapse of Barings. http://www.forex.com/members/regulation/boebar/boe.htm

7. BloomBecker, J. (1986). Computer crime law reporter. Los Angeles, National Center for Computer Crime Data.

8. Box, S. (1983). Power, crime and mysitication. London, Tavistock.

9. Braithwaite, J. (1984). Corporate crime in the pharmaceutical industry. London, Routledge & Kegan Paul.

10. Braithwaite, J. and Geis, G. (1982). "On theory and action for corporate crime control", Crime and Delinquency (April): 292- 314.

11. Clinard, M. B. and P. C. Yeager (1980). Corporate crime. New York, The Free Press.

12. CSI/FBI (2003). Computer Crime Security Survey. San Francisco, CSI: http://www.gocsi.com/

13. CSI/FBI (2004). Computer Security Issues and Trends. San Francisco, CSI.

14. CSI/FBI (2005). Computer Crime Security Survey. San Francisco, CSI.

15. D'Arcy and Hovav (2004). The role of individual characteristics on the effectiveness of IS security countermeasures. Tenth Americas Conference on Information Systems (AMCIS) 2004, New York: 1-8.

16. Clarke, R., Ed. (1997). Situational crime prevention: successful case studies. Albany, NY, Harrow and Heston.

17. Cressey, D. (1986). "Why managers commit fraud." Australian and New Zealand Journal of Criminology 3(19): 195-209.

18. Croall, H. (1992). White collar crime. Milton Keynes, Open University Press.

19. Croall, H. (2001). Understanding white-collar crime. Buckingham, Open University Press.

20. Dhillon, G. and J. Backhouse (1996). "Risks in the use of information technology within organisations." International Journal of Information Management 16(1): 65-74.

21. Dhillon, G. (1997). Managing information system security, Macmillan Press.

22. Dhillon, G. (1999). "Managing and controlling computer misuse." Information Management and Computer Security 7(5).

23. Dhillon, G. (2001). "Violation of safeguard by trusted personnel and understanding related information security concerns." Computers & Security 20 (2): 165-172.

24. Doig, A. (1984). Corruption and misconduct in contemporary British politics. Harmondsworth, Penguin Books.

25. Elbra, T. (1990). A practical guide to the Computer Misuse Act 1990. London, NCC Blackwell Limited.

26. Ernst & Young (2004). Global information security survey 2004. London, Ernst & Young: 28.

27. Forester, T., and Morrison, P. (1994). Computer ethics: cautionary tales and ethical dilemmas in computing. Cambridge, The MIT Press.

28. Fox, R. (1998). "News track: Latest computer security numbers." Communications of the ACM 41(11): 9-16.

29. Gapper, J. and N. Denton (1996). All the glitters. USA, Hamish Hamilton.

30. Goodwin, B. (2000). "Just 37 get security cert." Computer Weekly. London: 2.

31. Gotterbarn, D. (1991). "Computer ethics: responsibility regained." National forum: The Phi Beta Kappa Journal (LXXI) 3:26- 31.

32. Gottfredson, M. R., and Hirschi, T. (1990). A general theory of crime. Stanford, CA, Stanford University Press.

33. Harrington, S. J. (1996). "The effects of codes of ethics and personal denial of responsibility on computer abuse and judgments and intentions." MIS Quarterly (20) 3: 257-278.

34. Hollinger, R. C., Ed. (1997). Crime, deviance, and the computer. Dartmouth, Dartmouth Publishing Company.

35. Hollinger, R. C. and L. Lanza-Kaduce (1997). The process of criminalization: the case of computer crime laws. Crime, deviance and the computer. R. C. Hollinger (ed). Dartmouth, Dartmouth Publishing Company Limited: 59- 84.

36. Icove, D., Seger, K., and VonStorch, W. (1995). Computer crime: a crime fighter's handbook. Sebastopol, O'Riley & Associates.

37. James, H. and J. Palmer (1994). Computer crime in Western Australia and why organisations do not report it. Curtin Business School, Curtin University of Technology, WA.

38. Johnson, D. G. (1994). Computer ethics. Englewood Cliffs, Prentice-Hall.

39.Johnson, D. G., and Mulvey, J.M. (1995). "Accountability and computer decision systems." Communications of the ACM 38 (12): 58-64.

40. Johnson, D. G., and Snapper, J.W. (1985). Ethical issues in the use of computers. Belmont, California, Wadsworth.

41. Jones, M. R. (1992). Dealing with computer misuse - the need for an international approach. Eighth IFIP International Symposium on Computer Security, IFIP Sec '92, Singapore, 27-29 May 1992, Elsevier Science Publishers B.V. (North Holland).

42. Kankanhalli, A., Teo, H.H., Tang, B.C., and Wei, K.K. (2003). "An integrated study of information systems security effectiveness." International Journal of Information Management 23 (2): 139- 154.

43. Kennedy, G. (2001). Hong Kong steps up efforts to tackle computer crime. Hong Kong, Government of Hong Kong. 17: 110-113.

44. Kesar, S., and Rogerson, S. (1998). "Managing Computer Misuse" Social Science Computer Review (SCCORE), Special Issue: ISTAS '97: Computers and Society at a Time of Sweeping Change, a Sage Referred Journal 16 (3): 240-251.

45. Kluth, D. J. (1990). "The computer virus threat: a survey of current criminal statues." Hameline Law Review 13(Spring): 297-312.

46. Laudon, K. C. (1995). "Ethical concepts and information technology." Communications of the ACM 38 (12): 33-39.

47. Lee (1995). "Legal aspects of computer crimes and information systems in Hong Kong", Matthew Lee, City University of Hong Kong, Source: Source: http://www.is.cityun.edu.hk/Research/Publication/paper/9404.pdf

48. Levi, M. (1999). White-collar crime in the news. British Criminology Conference, Liverpool, July.

49. Lloyd (1990). Computer crime. Computer law. C. Reed (ed), London, Blackstone.

50. Magklaras, G. B., and Furnell, S.M. (2003). "Insider threat prediction tool: evaluating the probability of IT misuse." Computers & Security 21 (1): 62-73.

51. Magklaras, G. B., and Furnell, S.M. (2005). "A preliminary model of end user sophistication for insider threat prediction in IT systems." Computers & Security. 16th December 2004, http://www.sciencedirect.com/science.

52. Maner, W. (1996). "Unique ethical problems in information technology." Science and Engineering Ethics 2 (2): 137-154.

53. Mars, G. (1982). Cheats at work, an anthropology of workplace crime. London, George Allen & Unwin.

54. Mintzberg, H. (1983). Power in and around organisations. Englewood Cliffs, Prentice-Hall.

55. Nelken, D. (1997). White-collar crime. The Oxford Handbook of criminology. M. Maguire, R. Morgan and R. Reiner. Oxford, Clarendon Press.

56. Nissenbaum, H. (1994). "Computing and accountability." Communications of the ACM: 37 (1): 74-80.

57. Oz, E. (1992). "Ethical standards for information systems: a case for unified code." MIS Quarterly 16(4): 423-433.

58. Parker, D. B. (1976). Crime by computer. New York, Charles Scribner's Sons.

59. Parker, D. B. (1981). Computer security management. Reston, Prentice-Hall.

60. Parker, D. B. (1998). Fighting computer crime: a new framework for protecting information. New York, John & Wiley Sons.

61. Parker, D. B., and Nycum, S. (1984). "Computer crime." Communications of the ACM 27 (4): 313-315.

62. Pearson, J. M., L. Crosby, J.P. Shim (1996). "Modeling the relative importance of ethical behaviour criteria: a simulation of information systems professional ethical decisions." Journal of Strategic Information Systems (5) 4: 275-291.

63. Peterson, M. B. (1994). Applications in criminal analysis. London, Greenwood Press.

64. Perrolle, J. A. (1987). Computer and social change: information property, and power, Waddsworth.

65. Power, R. (2001). "Computer crime and security survey". Computer Security Institute (VII) 1, San Francisco, USA.

66. Punch, M. (1996). Dirty business: exploring corporate misconduct. London, Sage Publications.

67. Perrolle, J. A. (1987). Computer and social change: information property, and power, Waddsworth.

68. Reed, C. and J. Angel. Eds. Computer law. London, Blackstine Press Limited.

69.Schultz, E. E. (2002). "A framework for understanding and predicting insider attacks." Computers & Security 21 (6): 526-531.

70.Schrager, L. S., and Short, J. F. (1977). "Towards sociology of organisational crime." Social problems 25 (4): 407-419.

71. Shackelford, S. (1992). "Computer-related crime: an international problem in need of an international solution." Texas International Law Journal 27: 479- 505.

72. Slapper, G. and Tombs, S. (1999). Corporate Crime. London, Addison Wesley Longman.

73. Smith, N. C. (1988). The case study: a vital yet misunderstood research method for management. British Academy of Management Conference, Cardiff.

74. Straub, D. W., and Welke, R. J. (1998). "Coping with systems risks: security planning models for management decision making." MIS Quarterly 22 (4): 441- 464.Straub, D. W. (1990). "Effective IS security: an empirical study." Information System Research 1 (2): 255-277.

75.Rawnsley, J. (1995). Going for broke: Nick Leeson and the collapse of Barings Bank, Hammersmith, London, Harper Collins.

76. Raymond, J. and Erdwin (1997). Technology, property and law. Crime, deviance, and the computer. R. Hollinger (ed). Dartmouth, Dartmouth Publishing Company Limited: 85- 105.

77. Rigby, A. (1994). "Computer crime: computer hacking and misuse is now a criminal offence." Solicitors Journal 138: 624-5.

78. Tittle, C. R. (1980). Sanctions and social deviance: the question of deterrence. New York, Praeger.

79.Turner, B. A. (1994). "Causes of disaster: sloppy management." British Journal of Management 5(5): 215-219.

80.Vitell, S. J. and D. L. Davies (1990). "Ethical beliefs of MIS professional: the frequency and opportunity for unethical behaviour." Journal of Business Ethics 9(1):63-70.

81.Walden, I. (2000). Computer crime. Computer law. C. Reed and J. Angel (eds). London, Blackstone Press Limited: 277-298.

82. Walsh, A. (2000). "Partner in crime." The Computer Bulletin **2**(5):6-7.

83.Wilkins, L. (1990). Retrospect and prospect: fashions in criminal justice theory and practice. Policy and theory in criminal justice. D. Gottfredson and R. Clarke. Eds. Aldershot, Avebury: 14-26.

84.Willison, R. (2002). Opportunities for computer abuse: assessing a crime specific approach in the case of Barings Bank. PhD Thesis (Information Systems). London, London School of Economics.

Websites

1. Council of Europe's draft on cyber crime convention: http://www.cyber-rights.org/cybercrime/

2. Computer Misuse Act 1990, HMSO July 1990: http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.

3. Data Protection Act 1984, HMSO, July 1984 and Data Protection Act 1998, HMSO, July 1998.

http://www.is.cityun.edu.hk/Research/Publication/paper/9404.pdf