INTERPRETING COMPUTER-RELATED CRIME AT THE MALARIA RESEARCH CENTER

A Case Study

GURPREET DHILLON[1] and LEISER SILVA[2]

[1]College of Business, University Of Nevada, Las Vegas, NV 89154. USA Email: dhillon@ccmail. nevada. edu

[2]Department of Accounting and MIS, University of Alberta, Edmonton, T6G 2R6, Canada Email: Leiser.Silva@ualberta.ca

Key words: Computer-related crime, computer fraud, computer ethics, business ethics, self-regulation, self-control.

Abstract: This paper assesses issues concerning management of computer-related crime. It argues that organizations that focus exclusively on formal regulatory measures in business management fall short of protecting their resources. The argument is conducted by analyzing the pre and post computer-related crime situation at the Malaria Research Center. Findings from the case study suggest that ethical managerial behavior can not be cultivated by strict rule structures but through self-regulation. The paper uses Gottfredson and Hirschi's (1990) theory to evaluate the case. In a final synthesis the paper illustrates how inappropriate control measures can adversely affect the integrity of an organization.

1. INTRODUCTION

Any occurrence of computer-related crime is a matter of grave concern for an Organization and often leads to disastrous consequences. Organizations however tend to deal with computer-related crime situations in a reactive mode, building on short term solutions rather than identifying long term options or the negative consequences of their actions. It is important therefore to analyze all possible causes and effects. The extent of the problem can be gauged from various surveys and reports that show marked increase in computer-related crime situations and the related protection measures. According to a report in The New York Times (Chen 1998), in 1996 companies spent $830 million on information security technology to guard against potential abuses. In the same year the Computer Security Institute survey found 42% of Fortune 500 companies reporting computer-related crimes (New York Times 1997). A subsequent study in 1999 by the Computer Security Institute reported losses amounting to nearly $124 million (theft of proprietary information $42.5 million; financial fraud $39.7 million; laptop theft $13 million). Similarly a 1997 British study by the Audit Commission found organizations reporting computer-related fraud to have increased from 34% in 1994 to 45% in 1997.

Computer-related crime is not just one type of crime; it is a ubiquitous variant of all crime. Parker (1983) contends that ultimately this variant will become a dominant form. Indeed, the myth of computer related crime has become so distorted and exaggerated that the real problems are not being addressed. According to Sieber (1986), such real problems relate to the "precise knowledge of the rapid changes regarding the phenomena and characteristics of computer crime". This paper is an attempt to understand the problems concerned with managing computer-related crime. It argues that organizations that focus exclusively on technical and formal control measures in their systems, fall short of protecting their resources. Hence it is argued that organizations should focus more on the pragmatic control measures (for other research sympathetic with this viewpoint see (Dhillon 1997; Hitchings 1996). The argument of this paper is conducted by analyzing the computer related crime situation at the Malaria Research Center. The case illustrates how inappropriate control measures can affect the integrity of an organization.

2. PRIOR RESEARCH

Literature suggests that white-collar crimes are spontaneous and opportunistic acts and that offenders are not really in control of their behavior (e.g. see Croall 1992; Hester and Eglin 1992; Taylor *et al* 1992). More often however, criminal behavior typically entails considerable detailed preparation. This contention would appear at odds with popular misconceptions where white-collar criminals are portrayed as habitual losers, scratching out a miserable existence by taking extreme risks or are too lazy and stupid to do anything else. Numerous studies have shown that those who commit occupational crimes tend to be exactly the kind of people companies would want on their pay roll (Parker 1983; Ball 1990). In fact Parker (1983) maintains that these individual are "almost always young, energetic, highly motivated and intelligent".

Research in white-collar crime can broadly be classified into three categories. First are those researchers who have focused exclusively on the personal factors of an individual. These researchers argue that most criminal activities arise because of the personal situation of the offenders. Croall (1992) for example considers greed to be the prime cause of criminal behavior. On the other hand Cressey (1986) links crime to personal, non-sharable financial problems. Indeed there is a positive correlation between the personal factors of an individual and incidents of crime. Clinard's (1983) research based on retired middle management executives supports this contention.

The second category of researchers is those who consider work situation as a determinant of criminal acts. In the literature it has been argued that low pay and oppressive working conditions often lead employees to get involved in criminal activity. Scraton and South (1984) for example argue that since operational level workers are often subjected to a high level of surveillance they often end up becoming disgruntled. As a consequence they have a greater probability of becoming involved in a crime. Furthermore, even minor offences by operational staff are less tolerated than by those who are high up in the management hierarchy. While explaining the opportunities afforded by the work situation, Carroll (1982) suggests that any criminal act is inherently rational. Therefore most offenders weigh the possible consequences of their actions and take advantage of the criminal opportunity only if it is in their interest to do so. A similar viewpoint is propounded by Clarke (1985). He defines an initial involvement model of crime. This model acknowledges the impact of psychological, sociological and environmental determinants in the conduct of a criminal activity.

In the third category are researchers who consider criminal activity to be arising from the socio-organizational environment. The socio-organizational environment is closely reflected by the organizational structure. It has been argued that the risk of criminal activity increases with the complexity and the geographical spread of a corporation (e.g. see Aubert 1977; Braithwaite 1985; Clarke 1990; Croall 1992). Typically subsidiaries of an organization can be used by the top management to circumvent control at the operational level. A common denominator in managing computer-related crime in an organization, irrespective of its size or geographical spread, is the quality of its management. This is because most crimes are committed through collusion or compliance of management and staff. It has been reported by Clinard (1980) that nearly 40% of the large corporations had no record of any offence. It therefore follows that the culture of an organization plays an important role in the performance of a criminal act. Such cultures and normative structures in an organization take form from the technological and social work organization and the senior management attitudes (e.g. see Croall 1992; Mintzberg 1983; Dhillon 1999).

Poor quality of management and inadequate management communication has often been considered as cornerstones of an unethical environment. Most organizational workplaces are characterized by such predicaments. The importance of establishing an ethical environment within an organization cannot be overstated. Forester and Morrison (1994) maintain that there is little doubt that the ethos of certain work environments is conducive to crime. Much of the responsibility for organizational ethics lies with senior managers for it is they who form the particular style that influences so many aspects of corporate behavior. Hearnden (1990) contends that "an unequivocal management attitude and a clear statement about what constitutes acceptable behavior vis-a-via (say) expense claims or private telephone calls, will help to set the parameters for employee behavior over a range of issues".

An organizational climate that adopts trust-based relationships encourages individuals to take responsibility for their actions. Trust, in this context, is considered to mean consistency and integrity, the feeling that a person or organization can be relied on to do what they say. Since every job embodies some element of trust, organizations could well harness this feeling and thus enhance employees' self esteem. When control and restrictions replace trust and confidence, the whole organization will experience disruption.

3. THEORETICAL BASE

In this paper we adopt the theoretical framework proposed by Gottfredson and Hirschi (1990) to describe and evaluate the case study. Gottfredson and Hirschi emphasize the importance of instituting individual restraint on the behavior of people. The notion of 'self-control' is central to Gottfredson and Hirschi's general theory of crime. The importance of self-control is qualified on basis of three tenants. First that people differ in extent to which they are compelled to undertake a criminal act. Second that criminal acts require no special capabilities, needs or motivations. Third that lack of self-control allows almost any deviant, criminal, exciting or dangerous act. These three principles form the basis for describing the nature of self-control and the related individual characteristics that result in a criminal act. Gottfredson and Hirschi contend that the nature of the individual characteristic can be derived by understanding the nature of the criminal acts. As will become evident in the following sections, the Malaria Research Center case study describes a particular criminal act and we use Gottfredson and Hirschi's principles to interpret the nature of the characteristics. Doing so helps us to identify the kind of controls that could have been put in place within the Research center.

Based on Gottfredson and Hirschi's theory, table 1 summarizes various elements of interest in any crime situation. In subsequent sections these elements are used to tease out computer-related crime issues in the Malaria Research Center case study. It is our endeavor to understand different dimensions of the problem - on the one hand the characteristics of the individuals involved in a criminal act and on the other the management response in dealing with the situation. In the final synthesis it will be possible to draw interpretations from a real situation for good practice.

When interpreting the nature of gratification of desires, we are confronted with two dimensions - temporal and simplicity. The temporal dimension suggests that criminal acts provide an almost immediate gratification of desires and hence people with low self-control have a tendency to respond to substantial inducement. Since these people concern themselves with the immediate environment, they tend to have a very concrete orientation exclusively confined to the situation at hand. The second dimension deals with easy or simple gratification of desires, suggesting that the people with deviant behavior tend to be involved with acts that provide money without work and hence have very little persistence in a course of action.

The nature of consequences is another important element in Gottfredson and Hirschi's theory. It is contended that people with little self-control tend to be adventuresome, active and physical. Nature of consequences has also been posited as one of the primary components in Jones' (1991) moral intensity model. The general theory of crime considers cognitive requirements of a criminal act to be minimal and hence people lacking self-control do not necessarily possess or value cognitive or academic skills. Criminal acts also do not require any manual skills. It follows therefore that people with little self-control do not have any manual skills that require training.

The nature and scope of benefits from a criminal act (magnitude of benefits) form another dimension of the Gottfredson and Hirschi's theory of crime. They suggest that since crimes result in few or meager benefits, they are not necessarily equivalent to career or a job. Hence people with low self-control tend to have an unstable job profile and seem to be uninterested in long-term occupational pursuits. Criminal acts also result in pain or discomfort for the victim. As a consequence property is often lost, bodies are injured, privacy is lost and trust is broken. People with low self-control therefore tend to be self centered and insensitive to the feelings of others.

Table 1. Elements of interest in Gottfredson and Hirschi's general theory of crime

Gottfredson and Hirschi's self-control elements	**Predictions by Gottfredson and Hirschi's General Theory of Crime**	**Low self-control expressions**
Nature of gratification	Criminal behavior result in: Immediate gratification Easy or simple gratification of desires	People with low self-control: Respond to tangible stimuli in the immediate environment Have a 'here and now' orientation Look for money without work, lack diligence, tenacity or persistence
Nature of consequences	Criminal acts are exciting, risk thrilling	Criminal acts involve stealth, danger, speed, agility, deception, or power
Nature of planning and magnitude of benefits	Little skill or planning is needed for performing criminal acts Crimes result in: Few or meager benefits Pain or discomfort for the victim	People lacking self-control need not possess or value cognitive or academic skills People with low self-control tend to be little interested in and unprepared for long-term occupational pursuits People with low self-control tend to be indifferent or insensitive to the suffering and needs of others

4. THE CONTEXT OF THE MALARIA RESEARCH CENTER CASE

This section presents a case study of illicit activities at the Malaria Research Center, a research organization associated with the United Nations. The field research was carried out at the headquarters of the organization during 1995/97. A total of 30 formal in-depth interviews were conducted with various groups within the organization (senior managers, middle managers and employees in supportive roles). Interviews were also carried out with an ex-employee of the Research Center. This helped in validating the findings. The logical form of the interviews was based on a topic guide, the content of which was drawn from previous related research and Gottfredson and Hirschi's general theory of crime. Topic guides were customized for each interview. During data collection, the theoretical aspects of computer related crime were kept separate from the actual case (i.e. interpretations were made only after data collection). This prevented personal bias from influencing data collection (as suggested by Walsham 1995; Symons 1991). Based on the traditions of qualitative research, the methodological approach was interpretive in nature. Discussion of an interpretive research paradigm is beyond the scope of this paper. However the theoretical aspects of interpretive research can be found in Walsham

(1993) and Orlikowski & Baroudi (1991). Application and examples of interpretive research designs can be found in the works of Dhillon (1997), Serafeimidis (1997) and Madon (1991).

The Research Center was set up at the behest of the Malaria World Wide Research Organization (MWRO). Ever since its conception, the Research Centers' mission has been to investigate problems associated with malaria and other tropical diseases across the globe. The head of Research Center is the Director, appointed directly by MWRO. Given that the Research Center is governed by two separate organizations (MWRO and the Directive Council, constituted of health ministers of member countries) the process of decision-making is very complex. The organizational structure at the Center is matrix thus resulting in multiple reporting lines. For example, a person working on a specific research project, might report to three different roles: the project manager, the head of the technical division and the co-ordination offices. Supervision, as in many academic and research organizations, is based on responsibility rather than by putting pressure on employees.

The two main areas in which the Research Center faces competition are technical co-operation and research. While competition on research comes from both universities and the Non Governmental Organizations (NGO), competition on technical co-operation is mainly from the NGOs. In fact, these competitive forces question the very existence of the Research Center. The decision-making process for negotiating a research project is inflexible. Small NGOs, however, can reduce overhead costs and without a complex organization, as in the case of the Research Center, negotiations with donors are more straightforward. However the most serious problem at the Research Center was the discontinuous nature of the budget. It was project based and hence there was no guarantee that jobs could be maintained after work on a particular project was completed. Such a situation resulted in instability and uncertainty among staff members.

During 1994-95 the budget was reduced by approximately 40%. As a consequence a large number of staff at the Research Center were made redundant. This drastic reduction in personnel resulted in low morale among staff members. Although the Director adopted certain measures to rectify the situation, discussions with various staff members revealed that the Director had been slow in recognizing the problem. The researchers had regularly complained that the internal administration of the Center was not only too expensive (averaging approximately at US$ 600,000 a year) but also inefficient. Given the inherent complexity within the Malaria Research Center, the following sections explore as to how various organizational measures fell short of maintaining the overall integrity. Elements drawn from Gottfredson and Hirschi's general theory of crime are used to review various aspects of the case.

5. INTERPRETING THE NATURE OF GRATIFICATION

Gottfredson and Hirschi posit nature of gratification as one of the determinants of self-control in a given situation. When interpreting the nature of gratification, the general theory of crime stresses on 'immediacy' and 'ease' dimensions (i.e. how immediately or easily can criminal acts provide gratification of desires). The paragraphs below describe a situation at the Research Center and interpret it on basis of the two dimensions of gratification.

Background

Because of the composite nature of the administration at the Research Center, i.e. being administrated by MWRO and receiving funds from donors, and competing in the marketplace, clearance of accounts was a very complex process. However the administrative procedures in place were complex and not very cost effective. This resulted in a significant budgetary deficit. As a consequence the donor agencies got concerned about the manner in which the Research Center was administered. In 1989 MWRO appointed a new administrator whose main mission was to reduce the deficit by implementing tighter administrative controls.

Easy gratification of desires at the Malaria Research Center

The new administrator saw the development and implementation of a computer-based information system as a means to achieve administrative efficiency, The information system was also seen as an effective way to institute new control structures. It was decided that the new information system would eventually substitute an obsolete system that was believed to be one of the most notorious culprits of the deficit. The old system was running on a mini computer bought in the 70s and it was programmed in a traditional procedural language. The new information system was to be implemented on a microcomputer network and programmed in a fourth generation language. The Director of the Research Center thought that the administrative information system was exclusively a matter for the administration and therefore did not intervene in its design or development. With total control over the new information system, the administrator decided to launch the system in 1990. The new information system centralized and controlled majority of the operations – ranging from the purchase function (from computers to laboratory reactives) and the hiring of new staff. Once the system was in place many researchers complained about it, indicating that the new controls were in fact an obstacle in performing their day to day activities. The researchers pointed out that the administration had ignored their information needs while developing the system. Since at the time of system analysis and design the task of reducing the deficit was the main priority for the Center, the complaints were dismissed with indifference.

Immediate gratification of desires at the Malaria Research Center

By the end of 1990, the deficit had not yet been reduced and MWRO became impatient and continuously kept sending auditors to the Research Center. One such mission in January 1991 discovered something wrong in the accounting books particularly those related with computer purchases and the payment of staff health insurance. Nobody within the Research Center had questioned the transactions since the whole process had been computerized. The main problem was that a number of computers registered on the books were greater than those actually existing on site. Given that the computers bought were cheap clones, the prices listed in the accounting books were excessively high in comparison with market prices. Furthermore, even though a computer system aimed at increasing efficiency had been implemented; the payment of health insurance was being made one month late. The auditors established that in fact the money was being deposited in a bank account to earn interest in favor of the administrator and that the insurance company had agreed to receive their payment thirty days later. The auditors also discovered that the computer hardware provider was a closed friend of the administrator and that the insurance company had agreed to give a month's credit as an incentive for 'winning' in the tendering process, which of course was controlled by the administrator. Clearly the administrator would have not been capable of doing this without full control on the analysis, design and management of the information system.

6. NATURE OF CONSEQUENCES AT THE MALARIA RESEARCH CENTER

Gottfredson and Hirschi suggest that people involved in criminal acts are shortsighted in their orientation. They do not necessarily consider all the pros and cons prior to getting involved in a criminal act. This contention is evidenced in the Research Center case. Clearly the administrator lacked self-control and exhibited typical traits of being adventuresome and not being cautious. Obviously the administrator was not interested in maintaining the long-term viability of the institute. This becomes clear from the sequence of events described below.

In February 1991 the administrator was asked to leave the Research Center. He had been formally discharged on grounds of fraud. The administrative charge of the Research Center was taken up by MWRO. A new administrator was appointed at the end of the intervention whose mission was not only to reduce the deficits but also to eradicate corruption. She introduced even tighter controls. Instead of making the administrative information system flexible, it was transformed into a 'bureaucratic toy'. As a consequence of the intervention, by explicit orders of MWRO, the authority of the Director was curtailed. The Director was no longer entitled to purchase goods whose prices were above five thousand US dollars. Director's responsibility for authorizing permanent contracts was also dissolved. Furthermore the director was not even entitled to authorize trips beyond the limits of the immediate geographical region.

The difficulties in conducting business at the Research Center are exacerbated by the fact that MWRO headquarters were very slow in responding to most of the requests. As a result of the intervention, contracts of research projects and the acceptance of donations although negotiated by the Director of the Center could only be authorized by MWRO. However, the most serious damage was the reputation and credibility of the Research Center. Soon after the intervention the respective governments, competitor NGOs and donors undoubtedly questioned the trustworthiness of the Research Center and were concerned of their association. The intervention also had serious consequences in the social integration of the Center. Although the new administrator was eventually able to reduce the deficit and there were no incidents of fraudulent behavior, the price paid was high. The Center resulted in having centralized and extremely despotic administrative processes. The administrative information system, instead of facilitating organizational processes, was an obstacle in achieving the objectives of the research projects. This resulted in the alienation of the research staff. Over the past five years, the administrators and the research staff have constantly been pointing fingers at each other. As a consequence most research projects fail to finish on time and end up being over budget. The context of the Center is such that it will not be long when the losses will amass and the organization will face a financial crisis.

We are not claiming that the fraud committed in the Research Center was the cause of all organizational and economic problems of the Center. However, we cannot deny that the social and material price paid as a consequence of the crime is very high. Had the frauds not been committed, the Center could have saved a lot of time effort and resources. Most importantly the Research Center would have retained its autonomous position. Indeed computer-related crime has effects that go beyond the disappearance of goods and resources. In fact organizations and jobs might disappear as a consequence of it.

7. NATURE OF PLANNING AND MAGNITUDE OF BENEFITS AT THE MALARIA RESEARCH CENTER

When understanding the nature of planning and magnitude of benefits at the Research Center, the interpretations seem to be at odds with the argument proposed by Gottfiedson and Hirschi (1990) in their general theory of crime. Gottfredson and Hirschi recognize the shortcoming when they note, "the concept of white-collar crime is usually seen as incompatible with most theories of crime" (pg 196). The general theory of crime suggests that usually little skill or planning is needed for criminal acts. Furthermore crimes provide few or meager long-term benefits. The situation at the Research Center was to the contrary. The situation at the Center suggests that computer related crime is a rational act, since the crime was committed by an internal employee who typically evaluated two key factors. First, the likelihood of being caught. Second the severity of the punishment if the crime is detected.

The traditional means to contain computer-related crimes has focused on increasing the probability of detection. Invariably this demands extra controls to be instituted in any organization. In the case of the Center, such controls have made the information system virtually unusable. This means that perhaps more appropriate means of curtailing computer-related criminal activities need to be put in place. Indeed Bologna (1984) suggests that a good means to secure organizational assets is to shift the concentration of cost and effort from physical controls to decreasing the probability of commission. This calls for a shift in the mindset in terms of dealing with criminal activities within organizations. If we analyze the control systems in place within the Research Center, after the fraud facilitated by the computer system had taken place, we see that an excessive thrust had been placed on the technical and formal measures.

When the new administrator was appointed, one of the fears of the organization was to curtail any occurrence of crime. This resulted in a number of overt control measures being instituted. In general, control measures correspond to the level of criminal activity. Dhillon (1998) suggests criminal activity to occur at the input, throughput or output stages. Input crimes are typically committed by entering false or manipulated information into the computer systems. The throughput frauds generally take the form of 'salami slicing'. Output crimes are generally committed by either concealing bogus inputs or by postponing detection. Since within the Research Center the computer-related fraud had taken place at input and output levels only, most of the controls were formal bureaucratic ones. Informal discussions with different individuals within the Research Center however revealed that it was really the management practices and personnel policies that should have been addressed. This raises an interesting question of establishing a balance between the more pragmatic measures against the formal and technical controls. This is a strategic issue that needs to be addressed at a corporate level. Provided that an organization begins to consider the more human/behaviorist countermeasures, the management focus then would be on decreasing the probability of commissioning of a fraud. This will be in contrast to the earlier focus on decreasing the probability of occurrence. At the Research Center, with the appointment of a new administrator, organizational thrust was definitely on minimizing occurrences of fraud. This may not necessarily be the desired option. On the other hand, if the organizational thrust is on decreasing the probability of commissioning of a fraud, management attention shifts towards other softer issues. Such softer issues may include aspects of self restraint and inducement restraint, something that was absent at the Research Center. If attention is paid to these softer concerns, promotion of self-esteem of individuals and the development of an ethical culture are facilitated.

The management at the Research Center has been reactive in dealing with the post computer-related crime situation. The implementation of overt controls by the new administrator perhaps resulted in feelings of oppression, which in turn leads to disaffection among employees. Since previous research has shown that internal employees of the organization pose the greatest threat (e.g. see Dhillon 1999; Brown 1991; Audit Commission 1994), the Research Center is potentially vulnerable to further criminal activity. In order to manage the Research Center better and to decrease the probability of commissioning of a crime, the focus should be on building a high level of trust that incorporates the deterrence doctrine. The inherent argument of such an approach is that an environment, which embodies high levels of trust between management and employees, acts to reduce the need for excessive management controls. Self-control becomes the dominant ethos, rather than imposed control. The overall strategy encompasses two principal techniques, individual/group self-control and good organizational practices.

Lessons learnt

Based on the study presented in this paper, two broad categories of lessons can be learnt. The first lesson pertains to the practical importance of inculcating a culture of self-control within organizations. Gottfredson and Hirschi’s (1990) theory of general crime supports this contention. The second lesson is methodological in nature and is concerned with the advantages and disadvantages of using the general theory of crime in this study. Both these lessons are discussed below.

The notion of individual and group self-control adopts proactive mechanisms, which encourage self-restraint. Research done by Hollinger and Clark (1983) has identified a positive correlation between certainty of detection and severity of punishment in the reduction of levels of theft. Empirical evidence from the retail sector supports Hollinger and Clark's contention (e.g. see McNees 1976; McClaughlin 1976). In the context of managing computer related crime, a focus on self and inducement restraint will result in discrete, though explicit warnings to employees that all breaches of security will not only result in instant dismissal but also criminal prosecution. Moreover employees should be encouraged to report instances of security breaches that they encounter. This can be reinforced by linking salary increases or productivity bonuses to levels of security breaches. The aim should be to promote the notion that honesty rather than dishonesty brings rewards. Since employees are deemed to act rationally, the assumption is that they will seek to obtain the maximum benefit. In the case of the Center, although the old administrator was dismissed instantly, no criminal proceedings were initiated. Furthermore, no effort was made to encourage employees to be part of the drive to curtail computer related criminal activities. At the Center, although it was a high ranking official who had been involved in the crime, the resultant controls in the management procedures and the information system had a more direct effect on the lower level employees. Discussions with various people in the organization revealed that most employees of the Center were not entirely happy with the way the business was conducted. They felt that they were being left out from all major decision making exercises and were not informed of the latest developments. It should be remembered that since majority of the Center employees are highly qualified individuals, the existing work practices within the organization would result in these individuals becoming dissatisfied, disillusioned and disgruntled. This may become a potential source of further computer related criminal activity, especially because it is these people who come in contact with the information system on a regular basis.

Although Gottfredson and Hirschi (1990) claim that their theory has general applicability, evidence coming from the Research Center case suggests that the general theory of crime falls short in explaining certain kinds of white collar crime. Although the theory was useful in interpreting the nature of gratification and consequences, it fell short of making accurate predictions about the nature of planning and the magnitude of benefits. Nevertheless the arguments proposed by the theory were helpful in analyzing the Research Center situation. Clearly further case study research is needed to validate the usefulness of the conceptual framework presented in table 1.

Prior research in testing the general theory of crime has largely taken a quantitative mode of inquiry (e.g. see Evans et al. 1997). This research uses qualitative case based interpretive research as a means of understanding a computer related crime situation. Qualitative case based studies are beneficial in developing an in-depth insight into particular situations. However they have often been subjected to criticism for their lack of generalizability. However the intention of this paper is not to draw generalizations. Rather it aspires to present a descriptive understanding of a given situation. This is done by borrowing a 'lens' (i.e the theory proposed by Gottfredson and Hirschi 1990). There are limitations in doing so as Walsham (1993) comments "theory is both a way of seeing and a way of not seeing" (p6). Provided a researcher is aware of the limitations, such problems can be overcome. Future research directions certainly demand a further review of the general theory of crime in interpreting other computer-related crime situations.

8. CONCLUSION

At a practical level this paper has shown the limitations of a misguided confidence placed in technical and formal control measures while protecting organizational resources. In doing so the paper has highlighted the importance of more pragmatic measures. Such measures have been related to good management practices and management communication. In addressing the issue of computer related crime, this paper has suggested that the management will have to institute changes in its attitudes, values and corporate working environment. Therefore by focusing on the more pragmatic measures it is possible to build in high levels of trust. In using Gottfredson and Hirschi's (1990) concepts qualitatively, this paper makes a methodological contribution to computer-related crime literature. The paper also identifies certain weaknesses in the general theory of crime to explain certain white-collar crime situation. Further investigation in this area is warranted for.

9. REFERENCES

Aubert, V. (1977). *White collar crime and social structure.* The Free Press, New York.

Audit Commission, (1994) Opportunity makes a thief. Analysis of computer abuse, The Audit Commission for Local Authorities and the National Health Service in England and Wales.

Ball, L. (1990). Computer crime. In: *The information technology revolution.* T. Forester, Ed. Basil Blackwell, Oxford.

Bologna, J. (1984). *Computer fraud: the basics of prevention and detection.* Butterworth, London.

Braithwaite, J. (1985). White collar crime. *Annual Review of Sociology* (11): 1-25.

Brown, R. K., (1991) Security overview and threat, National Computer Security Educators, Information Resource Management College, National Defense University, Washington DC, Tutorial Track, NCSC.

Carroll, J. (1982). Committing a crime: the offenders decision. In: *The criminal justice system: a social psychological analysis.* V. Konecni and E. Ebbesen, Eds. Freeman and Company, San Francisco.

Chen, D. (1998) Man Charged With Sabotage of Computers. New York Times, February 18,1998.

Clarke, M. (1 990). *Business crime: its nature and control.* Polity Press, Cambridge.

Clarke, R. and D. Cornish (1985). Modeling offenders decisions: a framework for research policy. *Crime and Justice - An annual review of research* 6: 147-185.

Clinard, M. B. (1983). *Corporate ethics and crime.* Sage Publications, Beverly Hills.

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

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

Croall, H. (1992). *white collar crime.* Open University Press, Milton Keynes, UK.

Dhillon, G. (1997). *Managing information system security.* Macmillan, London.

Dhillon, G. (1998). Choosing appropriate organizational controls: managing the informtion assets. In: *Effective utilization and management of emerging information technologies.* M. Khosrowpour, Ed. 473-477. Idea Group Publication, Hershey PA.

Dhillon, G. (1999). Computer crime: interpreting violation of safeguards by trusted personnel. In: *Managing information technology resources in organizations in the next millennium.* M. Khosrowpour, Ed. 602-606. Idea Group Publishing, Hershey.

Evans, T. D., F. T. Cullen, et al. (1997). The social consequences of self-control: testing the general theory of crime. *Criminology* 35(3): 475-504.

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

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

Hearnden, K. (1990). Computer crime and people. In: *A handbook of computer crime.* K. Hearnden, Ed. Kogan Page, London.

Hester, S. and P. Eglin (1992). *A sociology of crime.* Routledge, London.

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. In: *Information systems security: facing the information society of the 21st century.* S. K. Katsikas and D. Gritzalis, Eds. 3-12. Chapman & Hall, London.

Hollinger, R. and J. Clark (1983). Deterrence in the workplace: perceived certainty, perceived severity and employee theft. *Social Forces* 62(2): 398-418.

Jones, T. M. (1991). Ethical decision making by individuals in organizations: an issue-contingent model. *Academy of Management Review* 16(2): 366-395.

Madon, S. (1991). The impact of computer-based information systems on rural development: a case study in India. Pb.D. Thesis. University of London, .

McClaughlin, T. (1976). A proposal for a behavioral approach to decrease shoplifting. *Corrective and Social Psychiatry* 22: 12-14.

McNees, M. e. a. (1976). Shoplifting prevention: providing information through signs. *Journal of Applied Behavioral Analysis* 9: 339-405.

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

New York Times. (1997) Big eight Ministers meet on international computer crime. , 12 November.

Orlikowski, W. J. and J. J. Baroudi (1991). Studying information technology in organizations: research approaches and assumptions. *Information Systems Research* 2(1): 1-28.

Parker, D. (1983). *Fighting computer crime.* Charles Scribner's Sons, New York.

Scraton, P. and N. South (1984). The ideological construction of the hidden economy. *Contemporary Crises* (8).

Serafeimidis, V. (1997). Interpreting the evaluation of information systems investments: conceptual and operational explorations. Ph.D. thesis In: *Information Systems Department.:* London School of Economics and Political Science, University of London, London.

Sieber, U. (1986). *The international handbook on computer crime.* John Wiley & Sons, Chichester.

Symons, V. J. (1991). A review of information systems evaluation: content, context and process. *European Journal of Information Systems* 1(3): 205-212.

Taylor, I., P. Walton, et al. (1992). *The new criminology: for a social theory of deviance.* Routledge, London.

Walsham, G. (1993). *Interpreting information systems in organizations.* John Wiley & Sons, Chichester.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems* 4(2): 74-81.