Working Paper

Opportunities for computer abuse: Considering systems risk from the offender's perspective

By

Robert Willison & James Backhouse

No. 10 - 2005

Institut for Informatik

Handelshøjskolen
i København

Howitzvej 60
2000 Frederiksberg

Tlf.: 3815 2400
Fax: 3815 2401
http://www.inf.cbs.dk

Department of Informatics

Copenhagen
Business School

Howitzvej 60
DK-2000 Frederiksberg
Denmark

Tel.: +45 3815 2400
Fax: +45 3815 2401
http://www.inf.cbs.dk

Opportunities for computer abuse: Considering systems risk from the offender's perspective

Dr. Robert Willison
Department of Informatics
Copenhagen Business School
rw.inf@cbs.dk

Dr. James Backhouse
Department of Information Systems
London School of Economics and Political Science

Opportunities for computer abuse: Considering systems risk from the offender’s perspective

Systems risk refers to the likelihood that an IS is inadequately guarded against certain types of damage or loss. While risks are posed by acts of God, hackers and viruses, consideration should also be given to the ‘insider’ threat of dishonest employees, intent on undertaking some form of computer abuse. Against this backdrop, a number of researchers have addressed the extent to which security managers are cognizant of the very nature of systems risk. In particular, they note how security practitioners’ knowledge of local threats, which form part of such risk, is often fragmented. This contributes to situations where risk reducing efforts are often less than effective. Security efforts are further complicated given that the task of managing systems risk requires input from a number of departments including, for example, HR, compliance, IS/IT and physical security. In a bid to complement existing research, but also offer a fresh perspective, this paper addresses systems risk from the offender’s perspective. If systems risk entails the likelihood that an IS is inadequately protected, this text considers those conditions, within the organisational context, which offer a criminal opportunity for the offender. To achieve this goal a model known as the ‘Crime Specific Opportunity Structure’ is advanced. Focussing on the opportunities for computer abuse, the model addresses the nature of such opportunities with regards to the organisational context and the threats posed by rogue employees. Drawing on a number of criminological theories, it is believed the model may help inform managers about local threats and, by so doing, enhance safeguard implementation.

Introduction

Systems risk refers to the likelihood that an IS is inadequately guarded against certain types of damage or loss (Straub and Welke, 1998). While some risks are posed by acts of God (e.g. fire, flooding, earthquakes), and external threats such as hackers and viruses, consideration should also be given to those dishonest employees intent on undertaking some form of computer abuse (Dhillon and Moores, 2001; Kesar and Rogerson, 1998). Against this backdrop, a number of researchers have addressed the extent to which those managers responsible for security are cognizant of the very nature of systems risk (Straub and Welke, 1998; Loch et al, 1992; Goodhue and Straub, 1991). Indeed, Goodhue and Straub (1991) advance a model of managerial perceptions of systems risk. They note how informed perceptions are based on knowledge of three areas, including 'organizational environment' (knowledge of risks inherent to a specific industry), 'IS environment' (knowledge of the range of technical and managerial controls that can address systems risk) and 'individual characteristics' (knowledge of local systems risk and the threats which form part of such risk).

However, existing research notes that managerial knowledge of 'individual characteristics' is often 'fragmented' and 'incomplete' contributing to situations where efforts aimed at reducing risk are often less than effective (Straub and Welke, 1998; Loch et al, 1992; Straub, 1986a; Straub, 1986b). This is further complicated by the fact the organisational task of managing systems risk requires input from numerous departments including, for example, audit, HR, compliance, IS/IT and physical security (Schlarman, 2002; Fitzgerald, 2005; ISO/IEC 17799:2000, 2000).

In a bid to further this vein of research, but also offer a fresh perspective, this paper addresses systems risk from the offender's perspective. Given that systems risk entails the likelihood that an IS is insufficiently guarded, this text considers those conditions, within the organisational context, which offer a criminal opportunity for the offender. To achieve this goal a model known as the 'Crime Specific Opportunity Structure' is advanced (Willison, 2002). Focussing on the opportunities for computer abuse, the model addresses the nature of such opportunities with regards to the organisational context and the threat posed by rogue employees. Drawing on a number of criminological theories, the crime specific opportunity structure presents an in-progress view of IS security, which urges consideration of the relationships between the offender, the organisational context, the requisite safeguards (including the role of honest employees in enforcing security) and the departments responsible for them. Central to the model is the figure of the offender who, based on the perceived costs and benefits, decides whether a certain context offers an opportunity.

The model may complement existing IS security practices by informing managers as to the nature of opportunities in the organisational context. In this sense, knowledge of local systems risk, identified by Goodhue and Straub (1991) as 'individual characteristics', could possibly be enhanced. By assisting managers in identifying those elements which help form an opportunity, and appreciating how the offender defines a situation as such, the model may potentially be used to inform the application of countermeasures aimed at reducing systems risk.

The next section of the paper reviews the existing literature on opportunity. This is followed by a description of a number of theories that have helped to examine the concept in the field of criminology. An attempt by Clarke (1995) to synthesise these theories, in a model entitled the ‘Opportunity Structure for Crime, is then described. A number of changes made to the model are cited, culminating in a description of the ‘Crime Specific Opportunity Structure’ (Willison, 2002). An application of the model to a case of computer fraud forms the subsequent section followed by the discussion, conclusion and future research.

Criminal Opportunity

Of those texts that directly address opportunity, the literature divides into two distinct areas. The first group looks at how opportunities figure as a motivational factor with regard to individuals. The second attests to how opportunities are created through deficient security.

Opportunity as a Motivational Factor

A few researchers have discussed opportunities in terms of the motivational impact they may have on individuals (Hitchings, 1995; Forester and Morrison, 1994; BloomBecker, 1984). In an early paper, BloomBecker (1984), for example, cites eight types of motivational factors. One of these is ‘the land of opportunity’, where rogue employees exploit security loopholes located during the course of their daily work activities. However, other writings that discuss the relationship between opportunity and motivation merely mention this phenomenon in passing (Hitchings, 1995; Forester and Morrison, 1994) as evidenced by Forester and Morrison who argue:

> Experts on computer fraud attest to the fact that opportunity more than anything else seems to generate this kind of behaviour.
>
> (Forester and Morrison, 1994, p. 41)

Opportunity Formation Through Deficient Security

A number of texts focus on how opportunities are created through deficient security. With the aim of raising practitioners' awareness, the UK Audit Commission has been eager to spread the message regarding the relationship between poor security and opportunity. Its 1994 report, entitled *Opportunity Makes a Thief* (Audit Commission, 1994) indicates that one of the primary reasons for 'computer abuse' is a disregard for basic controls. More precisely, this disregard manifests itself in a failure to implement and maintain such controls. These findings are mirrored in the Commission's *Ghost in the Machine* (Audit Commission, 1998), which cites 'little improvement' with regard to the provision of internal controls. Furthermore, this continued neglect is reflected in the most recent report (Audit Commission, 2001) which states:

> Auditors and security specialists continue to stress the need for proper control and security measures. Nevertheless, the majority of breaches of IT security are still caused by a lack of the basic fundamental controls and safeguards.
>
> (Audit Commission, 2001, p. 17)

This view is supported by other writers who note how the absence, poor implementation and maintenance of safeguards may engender opportunities (Stevenson, 2000; Comer, 1988, Bologna, 1993). But what exactly are those factors which lead to such situations? The paper will now turn to this area.

Organisational Complacency Towards IS Security: A primary reason for the absence of the appropriate safeguards is complacency by many organisations with regard to IS security (Hinde, 2001; Audit Commission, 1998). As noted, this manifests itself in the failure of some organisations to implement even the most basic controls, leaving their systems vulnerable and possibly forming those conditions that create opportunities. The last three UK Audit Commission reports clearly demonstrate this. A key control, for example, is establishing a security policy (Nosworthy, 2000; Osborne, 1998; Backhouse, 1997; Dorey, 1994). The reports of 1994 and 1998 indicate that one third of all surveyed organisations failed to implement this safeguard. While this position had improved by 2001, one quarter of all organisations still failed to take any heed.

One of the reasons for organisational complacency towards IS security may well be the failure of organisations to appreciate the value of their information assets, and the consequent need to protect them. A UK Department of Trade and Industry report (DTI, 2000) collated data from a representative sample of 1000 UK organisations. Surprisingly, of these 1000, 31% believed that they did not possess any information that they perceived as 'sensitive' or 'critical' in nature. Rather alarmingly, 7% of this figure related to organisations with over 500 or more employees.

Erroneous Perceptions of IS Security Risks: While companies may fail to appreciate the value of their information assets, they may also fail to recognise potential threats (Yapp, 2001; Riem, 2001; Wright, 2001; Hinde, 2001 Parker, 1997). A global security survey by Ernst & Young (2002) reveals:

> Yet again we see greater concern about vulnerability to external attack (57%), than internal (41%), and yet leading research groups continue to confirm that more than three quarters of attacks originate from within organisations … an alarming amount of evidence remains that organisations are lacking fundamental management information about security breaches (Ernst & Young, 2002, pp. 8-9).

This is confirmed by Parker (1997) who argues that the 'distorted image' of security held by top-level business people is often "informed" by trade publications such as the Wall Street Journal and Forbes. In a similar vein, the CSI/FBI (2002) report indicates how the actions of defrauded organisations help to reinforce the erroneous perceptions of threats held by management. Concerned with the consequences of bad publicity for their reputation, victims of financial fraud are often unwilling to invoke the aid of law enforcement agencies, preferring to deal with the matter internally. As fraud cases are rarely reported in business publications, such as those discussed by Parker, managers subsequently fail to appreciate the gravity of the problem. Indeed, Parker argues that information security practitioners must first attempt to understand what perceptions top managers hold and then proceed to correct any unfounded beliefs. One consequence of the inability of organisations to appreciate the actual risks to their IS is that measures may be implemented to address risks, which in reality are relatively minor, at the expense of those areas where the risks are high, but receive little attention.

Technical Perspective of IS Security: Additionally the 'distorted image' of security held by managers is often equated with a myopic understanding of the problem area and how it should be addressed. Several writers have affirmed how in many organisations IS security is often perceived as a purely technical concern (von Solms 2001; Osborne, 1998; Parker, 1997; Wood, 1995). The problem with this perspective is that it fails to view the whole of the problem domain, and hence fails fully to appreciate all the elements that constitute such an environment.

Funding of IS Security: The organisational security budget is influenced by management perceptions. Osborne (1998) argues that the technical perspective often leads to a poor return on investment owing to the inability of those responsible for security to understand and address the necessary and related managerial aspects of security (e.g. implementing a security policy), while concentrating too heavily on technical safeguards. Hence Osborne (1998) argues that those organisations that take a technical approach, while spending considerable funds on safeguards such as cryptographic systems and firewalls, may still experience security breaches owing to the failure to understand and act using an holistic approach. For an adequate level of organisational funding Wood (1997) argues that management need to have a clear understanding of the complexity of IS security. Once this is achieved, then there is a greater motivation for providing the necessary funds.

The Interrelated Nature of Security Controls: One problem often overlooked when safeguards are introduced is their interrelated nature. Security is very much like a house of cards: inadequate consideration for one area will impact on another, possibly creating those conditions that help to form an opportunity. One safeguard, for example, is an information security policy. Through the creation and maintenance of a security policy, management can provide support and direction for information security in an organisation. There is no denying the importance of a security policy as a cornerstone in the development of an organisation's control environment (Nosworthy, 2000; Osborne, 1998; Backhouse, 1997; Dorey, 1994). However, unless the policy is brought to life with education and awareness programmes, then all the work undertaken to create a policy will ultimately have been a waste of time (Nosworthy, 2000; Hansche, 2001; Hansche, 2001a; Spurling, 1995).

Implementation of Inappropriate Controls: Even prudent companies, who wish to establish effective security across the board, may unwittingly create the conditions which help to form opportunities through the implementation of inappropriate controls (Luzwick, 2001; Ølnes, 1994; Warman, 1993). If the safeguards introduced provide an inadequate level of security then the IS will be left vulnerable. However, the same is also true if the safeguards are perceived by staff as unworkable in the organisational context. One of the perennial problems for IS security is its uneasy relationship with business objectives. Although there is an obvious need to reduce the risks to IS, the related countermeasures are often seen by users as a constraint, because of the range of tasks required to fulfil the objectives. If the safeguards are perceived to be too heavy-handed or impractical (or both), staff may circumvent the controls just to make their lives easier. Again, non-compliant behaviour would leave the systems vulnerable, possibly providing opportunities for rogue employees. Hence, in this sense, although safeguards are obviously introduced to reduce risks, with a heavy-handed approach they may, paradoxically, create them.

Safeguard Implementation: Aside from the inappropriate nature of safeguards, a related issue concerns the implementation of controls. Poor implementation can negate any improvements in security for which a safeguard was designed. Schneier

(1998) discusses cryptographic systems as a case in point. He notes several problems pertaining to the poor implementation of this safeguard. With some systems, the plain text which the user wishes to encrypt is not destroyed after the whole process is completed. Other systems use temporary files on a computer in case of a systems crash. While this is prudent, if these systems are wrongly implemented, the plain text is left on the hard drive. Schneier further notes how, if poorly implemented, some systems can even leave the cryptographic keys on the hard drive.

Compliance Reviews: A key requisite of IS security is the need to confirm on a routine basis that the existing controls are working effectively. One of the lessons repeated in the UK Audit Commission (1994; 1998; 2001) reports is that many organisations fail to check whether their controls are operating as intended. As a consequence those safeguards which are failing to perform leave an IS vulnerable. Furthermore, given the failure of some companies to monitor their controls, these vulnerabilities may persist for considerable periods of time. The reason for this neglect may be the perception held by some managers that IS security is a one-off project and they have little need to consider the on-going nature of this function (Wood, 1997). The ISO/IEC17799:2000 Information Technology – Code of Practice for Information Security Management, however, advocates the need for compliance reviews at managerial and technical levels.

While advocating the need to review existing safeguards, ISO/IEC17799: 2000 also advises organisations to address new and emerging risks to their systems. As explained, the standard asserts that organisations can identify their security requirements by using risk assessment techniques. By doing so companies can identify their risks and implement the requisite controls. However, just as organisations change in terms of business practices and resources, so too must the security function, for with change come new risks (Anderson, 1994).

Deficiencies in Existing Notions of Opportunity

Although the literature concerned with opportunity has proven useful in highlighting the problem areas, certain deficiencies need to be addressed. First, very little is written about opportunity. This is probably due to the fact that the meaning of the term opportunity is regarded as self-evident and hence there is little reason to examine the subject.

Secondly, there has been a failure to define actually what an opportunity is. Indeed, a common-sense understanding of this phenomenon runs through the literature. From this viewpoint an opportunity might be perceived as a file left on a desk as an example of non-compliance with a clear desk policy, a PC left active at lunch time which should have been logged off, passwords posted to machines, and the like. The failure of this common-sense perspective lies in its inability to clearly explain why these so-called opportunities are acted on in some instances and not in others. Could it be that some of the instances simply do not afford an opportunity? This points to the interplay of other factors, which the common-sense perspective is at a loss to explain, but an understanding of which would be of great value to security practitioners. A more suitable theoretical explanation would be able to account for these ‘other factors’ and explain the variances. Unfortunately, one of the deficiencies with regard to IS security generally is the poverty of theory both used and advocated by academics in this field.

Thirdly, the prescriptive value of the existing literature is limited. A flawed understanding of opportunity offers little scope for developing effective solutions. If we can assume that opportunities arise in, and as a consequence of, the daily workings of an organisation then any approach used to understand opportunity must be able to address those elements involved in these routines, and explain how interactions between them may create opportunities.

However, this is far easier said than done. How does one know which factors are influential and which are not? How does one address the interactions between such factors? How can one assume a group of these factors will create an opportunity? In essence, how can one circumscribe the problem of opportunity in order to address it?

Criminological Theories and Opportunity

Clarke (1997) argues that one mistake of modern criminology is how the task of explaining crime has been assumed to be the same as explaining the criminal. 'Dispositional' criminological theories have been eager to provide accounts of why and how individuals through the assimilation of specific social or psychological influences, or the inheritance of traits, are as a consequence more inclined to acts of a delinquent or criminal nature. This is not the same as explaining the occurrence of crime, which aside from requiring a motivated offender, also warrants an opportunity. Simply to explain criminal dispositions, Clarke contends, is only half the equation.

What is further required are explanations of how offenders interact with the settings in which crime may or may not occur (Ekblom, 1994). It is for this reason that the following five criminological approaches are introduced in this paper for their insights into opportunity.

Situational Crime Prevention

Situational Crime Prevention (SCP) focuses on the criminal setting and aims to reduce the opportunities for crime through the implementation of measures in the environment. Furthermore, these measures a) target specific forms of crime, b) impact on the immediate environment via its design, management, or manipulation, and c) aim either to increase the effort and risks of crime, or to render these less rewarding or excusable. Examples of these measures, which are categorised into certain types, include the *controlling of facilitators* (e.g., gun controls: to increase the effort), *entry/exit screening* (baggage screening: to increase the risks), *target removal* (e.g., removable car radios: to reduce the rewards), and *rule-setting* (e.g., harassment codes: to remove excuses), (Clarke, 1997).

As noted, SCP's focus is crime-specific. This stems from a recognition that specific types of crime are unique in their mix of constituent environmental factors. In forgoing a discussion of crime prevention at the level of 'burglary' or 'robbery', greater emphasis is placed on those specific crimes that fall under these broader categories.

Furthermore, the introduction of safeguards into the immediate environment is designed to impact on the offender's perception about the potential costs and benefits of crime commission. Adjustments made in terms of the manipulation, design, or management of the environment are intended either to increase the perceived risks or reduce the rewards of the potential crime or both. The decision to commit a crime will be based on the perceptions and evaluations of the situation. It is no surprise, then, to learn that SCP has drawn heavily on rational choice theory, discussed further in the next section.

Finally, it is assumed as part of the decision-making process that some evaluation is made with respect to the possible moral costs of offending. While some offender may be prepared to shoplift, this does not mean they are prepared to mug the elderly. In an attempt however to overcome any feelings of guilt or shame, offenders may try to neutralise such feelings through the construction of excuses such as 'everybody else does it', 'I'm just borrowing it', etc. Support for this assertion comes from earlier criminological writings by Sykes and Matza (1957) who discuss 'techniques of neutralisation' and Bandura (1976) who, in a similar vein, addresses the concept of 'self-exoneration'.

Rational Choice Perspective

The watershed in the development of SCP was a simple 'choice' model of crime (Clarke, 1980), which later evolved into the formulation of a 'rational choice perspective', which has been extremely influential in determining the theoretical base of SCP (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Clarke and Cornish, 2000). The rational choice perspective assumes that crimes are deliberate and purposive: that is, those who commit crimes do so with the intention of deriving some type of benefit from such acts. Obvious examples are cash or material goods, but a broader reading of the term ‘benefits’ allows for the inclusion of other forms, such as prestige, fun, excitement, sexual gratification, and domination. Joyriding is an example of how the benefits may take the intangible forms of fun and excitement.

In addition, the rational choice approach assumes that decisions are characterised by what is termed ‘bounded’ or ‘limited’ rationality. In other words, criminal decision making is at times less than perfect, as a consequence of the conditions under which such decisions are made. With the associated risks and uncertainty in offending, criminals may make decisions without knowledge of all the potential costs and benefits (i.e. the risks, efforts and rewards).

Central to the rational choice perspective (and SCP) is the concept of crime specificity. The factors considered by criminals and the related variables that influence the decision making process vary considerably with the nature of the offence. Thus the analysis of decision-making needs to be made with reference to specific categories of crime.

Of further importance to the rational choice perspective is the division of criminal choices into two groups viz., ‘involvement’ and ‘event’ decisions. The former refers to choices an offender makes regarding their criminal careers. Hence, the offender must make decisions about embarking on criminal actions, whether or not to continue these activities over a period of time, and when, if at all, to cease them. Or to use the technical terminology, choices must be made about the initiation, habituation and desistance of a criminal career.

Event decisions refer to those choices made during the criminal act. These decisions are based on the offender's perceptions of the situation and the associated risks, efforts and rewards. Originally, work in this area focused solely on choices made in terms of the potential targets (Clarke and Cornish, 1985; Cornish and Clarke, 1986), but as a result of theoretical advancements, it was realised that as the criminal act unfolds, the perpetrator is required to make a series of decisions (Clarke and Cornish, 2000).

Environmental Criminology

One school of thought closely related to the rational choice perspective is environmental criminology. This approach has provided considerable insight into the 'search' patterns of offenders and illustrated how the majority of crimes are committed within areas visited by offenders during their routine work and leisure pursuits (Brantingham and Brantingham, 1991). Offenders develop an 'action space' in which these everyday pursuits take place and through such activities acquire a detailed knowledge of this environment, leading to what these authors describe as an 'awareness space'. Like the rational choice perspective, Brantingham and Brantingham (1991) argue that the motivated individual engages in a 'multi-staged decision process' prior to the commission - or not as the case may be - of a crime. Such a process is informed through knowledge gathered from the offender's awareness space. Furthermore, they argue that a specific environment emits cues relating to its spatial, cultural, legal and psychological characteristics. With experience, an offender is able to discern certain sequences and configurations of these cues associated with a 'good' target.

Routine Activity

SCP has further been developed by Routine Activity Theory, another relative newcomer to the field of criminology. Cohen and Felson (1979) discuss how changes in what they describe as 'routine activities' of society's members have impacted on the levels of direct-contact predatory crimes, i.e. crimes where one or more persons directly take or damage the person or property of another. These activities include the provision of food, shelter, leisure, work, child-rearing, and sexual outlets. It is argued that these forms of behaviour influence direct-contact predatory crime rates by impacting on the convergence in time and space, of the three elements required for a crime to occur. These elements consist of a likely offender, a suitable target, and the absence of a capable guardian, who, if present, would be in a position to stop a criminal act. Cohen and Felson assert that it takes merely the absence of one of these three elements for a crime not to occur. So for example, drawing on U.S.A. census data and victimisation surveys, they reveal how between 1960-1970, daytime residential burglary increased by 15%. They partly explain this rise by noting how the decade also witnessed an increase in the number of females in the workforce and a rise in the number of individuals living alone. As a consequence, there was a related rise in the number of properties left vacant and lacking a capable guardian during the working day.

Routine activity theory is still in a period of transition, as witnessed by the attempts of Felson (1992) to extend the scope of routine activity (by suggesting minimal elements for other categories of crime), and include a fourth element - that of the 'intimate handler' - in relation to direct-contact predatory offences. Drawing on social control theory (Hirschi, 1969), 'intimate handlers' refers to those individuals who, by knowing an offender, may act as a brake on illegal activities carried out by the latter. As a means of enhancing its contribution to crime prevention, Clarke (1992) advocates that routine activity theory could incorporate the category of 'crime facilitators'. These relate to items such as cars, guns, and credit cards, which act as tools for specific crimes - as well as dis-inhibitors such as alcohol, which facilitate the precipitation of crimes.

Lifestyle Theory

Lifestyle theory represents a school of thought closely related to the routine activity approach. A central theme of lifestyle theory asserts how the differential risks of victimisation are related to the differential exposure to offenders. While socio-demographic factors exert some influence on this relationship, an individual's lifestyle activities must also be acknowledged when considering the risk of victimisation, given that such activities may increase contact with potential offenders. This is confirmed by Hindelang *et al* (1978) who advance a theoretical model of victimisation based on data from eight American cities. In addition, they list a series of propositions with respect to how particular lifestyles carry greater probabilities of victimisation. These include, for example:

> The probability of suffering a personal victimisation is directly related to the amount of time that a person spends in public places (e.g. on the street, in parks, etc.), and particularly in public places at night (p. 251).
>
> The probability of being in public places, particularly at night, varies as a function of lifestyle (p. 253).
>
> (Hindelang *et al*, 1978)

The findings produced by victimological studies indicate how the risks of victimisation can be reduced through the modification of patterns of behaviour.

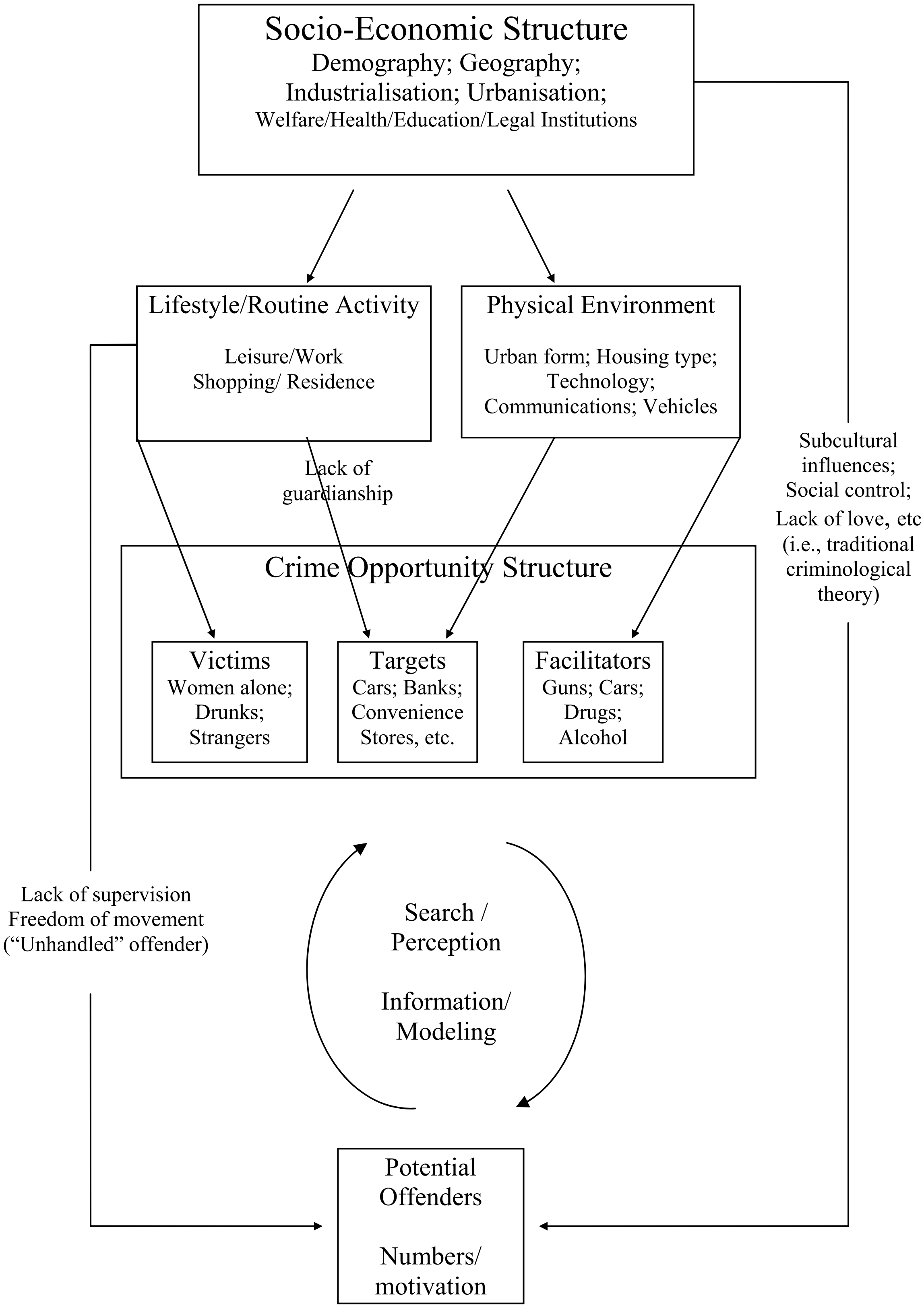
The Opportunity Structure for Crime

In an article by Cusson (1986), he argues that a synthesis of these theories is inevitable. Clarke (1995) attempts such a synthesis as shown in Fig. 1 entitled the 'Opportunity Structure for Crime'. While the model is able to incorporate dispositional variables of traditional criminology, it should again be stressed that through the synthesis of the five criminological approaches, the focus of the model is very much on the interaction between the offender and their environment.

As per Fig.1, the *physical environment* encompasses the layout of cities, forms of housing, retail and transport systems, technology and communications and the various types of vehicles used by individuals. Hence the physical environment affords both *targets* and *facilitators*. Convenience stores and banks are example of the former, while get-away cars and guns illustrate the latter. Furthermore, as noted earlier, *lifestyle* and *routine activities* also influence the number of targets. The behaviours inscribed in lifestyle and routine activities i.e. work, leisure, residence and shopping, can either enhance or hinder guardianship. For example, a house left vacant owing to the single occupant working during the day manifests a lack of guardianship, and represents a more viable target for a burglar. The behavioural patterns represented in lifestyle and routine activities also play a significant role in supplying *victims* of personal and sexual attacks e.g. an individual walking home alone at night after visiting a night-club with friends, or working a shift in a restaurant.

Fig. 1

Opportunity Structure For Crime



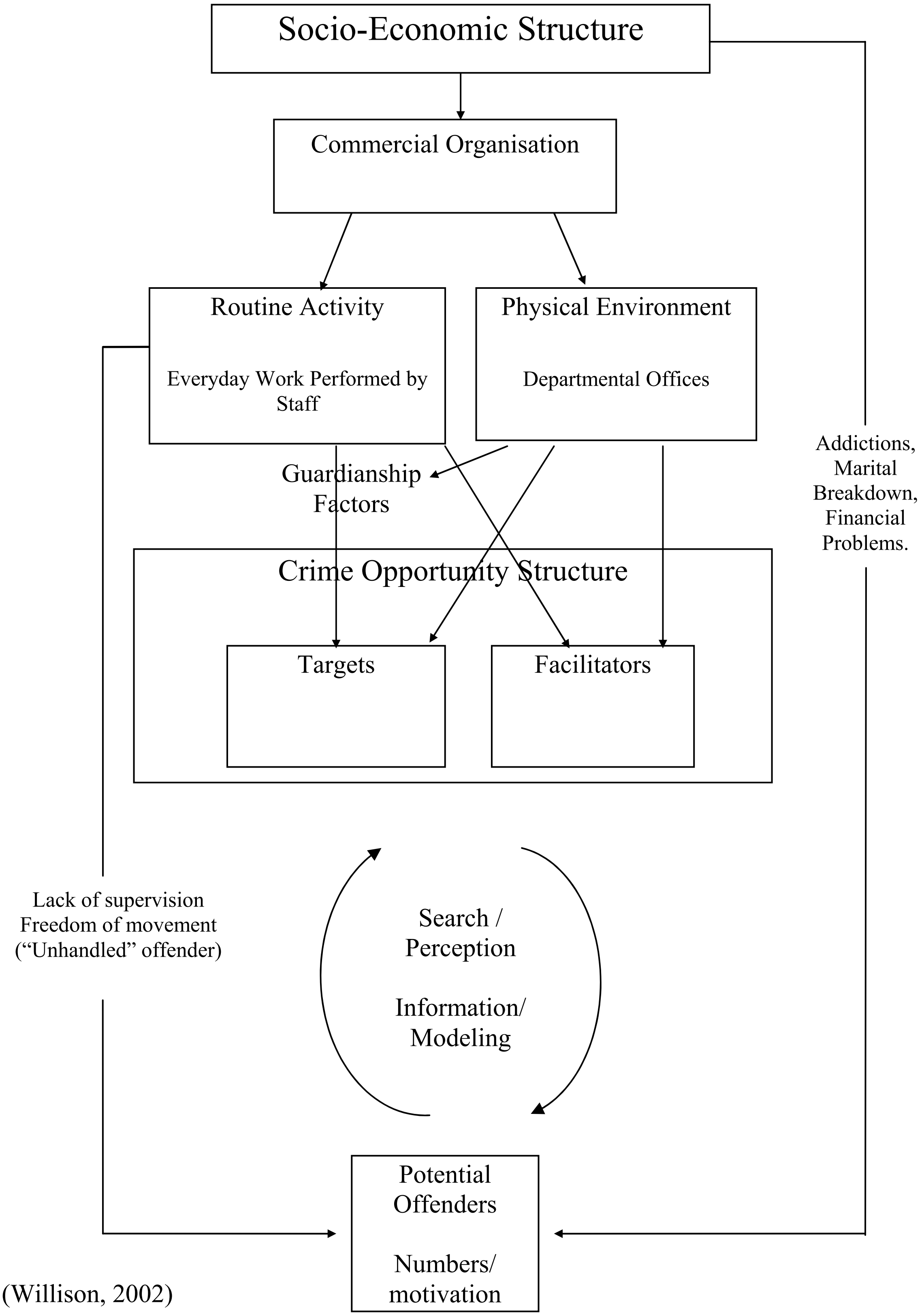
At a macro level, the *socio-economic structure* determines the lifestyle/routine activities and the physical environment. The former includes demography, geography, industrialisation, urbanisation, welfare/health, education, and legal institutions. The socio-economic structure also partly determines the number of *potential offenders* through sub-cultural influences, such as neglect and lack of love, alienation etc. (identified by traditional criminology), and partly through lifestyle and routine activities. These can influence the degree of social control afforded by intimate handlers, leading to a possible *lack of supervision* and *freedom of movement*. What needs to be stressed here is that the opportunity structure is not simply a physical entity, consisting of the routine activities of the population and the nature of the physical environment. Rather, it comprises interaction between supplies of victims, targets, potential offenders, and facilitators, which determine the nature and the scale of opportunities. These interactions largely take place in the 'action' and subsequently in the 'awareness' spaces of offenders as indicated by the *search/perception – information modelling* sections of the model and highlighted by environmental criminology. The offender's *perceptions*, - highlighted by the rational choice perspective, but also environmental criminology - of the risks, efforts, and rewards associated with such spaces play a crucial role in defining the opportunity structure.

Crime Specific Opportunity Structures?

As discussed earlier, the measures employed by SCP are crime specific. Hence, measures are not aimed at broad categories of crime such as burglary or robbery, but tailored specifically to those offences which fall under these umbrella terms. Poyner

Fig. 2

Crime Specific Opportunity Structure



(Willison, 2002)

and Webb (1991), for example, from their research into burglary in a British city, argue that different controls are required to combat domestic burglary, which targets cash and jewellery, from that which targets electronic goods. While Fig. 1 represents at a generic level those items thought to constitute an opportunity, is it feasible to advance the idea of crime specific opportunity structures? In other words, is it feasible to address opportunities in this manner? Fig. 2 represents a hypothetical

crime specific opportunity structure with regard to computer input fraud (Willison, 2002). Clarke's (1995) model has been modified given the nature of the crime and the context in which the crime is traditionally enacted i.e. the organisational environment.

As can be seen from Fig. 2, the 'Lifestyle' patterns of behaviour, and the 'victims' box has been omitted. The intention here is not to suggest that organisations are not victims of computer input fraud. Instead, the theory underpinning this part of the model – lifestyle theory – explains how an individual's behaviour can increase their risk of victimisation. As a consequence, it was felt that this element of Clarke's (1995) model had little relevance to the organisational context.

In keeping with Fig.1, targets and their nature are the result of the physical environment, which in this instance consists of departmental offices. The commission of input fraud involves entering false information into computer systems. Given this, the target could therefore be computerised accounting records, bank account details etc. Targets are also partly determined by routine activities, which in the organisational domain encompass work practices. Such practices can be seen to either enhance or hinder control over a target, and are depicted in Fig. 2 as guardianship factors. The intention here is to illustrate the plethora of safeguards required in the organisational domain to provide effective guardianship. Staff non-compliance with security procedures, for example, would provide a lack of guardianship and leave the associated IS vulnerable.

As a departure from Fig. 1, facilitators are provided not only by the physical environment, but also by the routine activities of staff. In terms of the environment, the organisational context provides facilitators in the form of computers, which the offender uses to help carry out the input fraud. With regard to routine activities of staff, the organisational environment provides a forum in which cognitive facilitators can be developed and used by potential offenders (Willison, 2002, 2004). This type of facilitator includes those skills and knowledge that a person acquires to discharge their job responsibilities. Although such skills are used by staff, on the whole, for purely legitimate activities, they can also be used to help perpetrate behaviour of an illegal nature.

Again, at a macro level, the *socio-economic structure* determines the routine activities and physical environment in the form of *commercial organisation*. The socio-economic structure, as per Fig. 1, partly determines the number of *potential offenders*, through sub-cultural influences including alienation, lack of love, etc., or in other words the traditional domain of dispositional theories. While Fig. 2 maintains this element of the model, the focus on specific socio-economic factors shifts. Classic fraud profiles point to a different set of socio-economic factors, which may motivate an offender (Bologna, 1993; Comer, 1998). These include addictions in their various guises, marital breakdown, financial problems and the like.

The number of potential offenders as with Fig. 1 is also partly determined by routine activities in terms of the degree of supervision afforded by managers, leading to either handled or *unhandled* staff, and hence potential offenders. In keeping with the original model, Fig. 2 acknowledges the *search-perception* and *information modelling* activities of potential offenders in their action and awareness spaces. In this instance, departmental offices represent the awareness space for rogue staff. Through the discharging of their work responsibilities, potential offenders are able to assess the integrity of their respective control environments, 'searching' for potential vulnerabilities, and using this information possibly as a basis for criminal activity. Through the incorporation of the criminological theories, the crime specific opportunity structure affords consideration of the forms of behaviour an offender exhibits when planning and perpetrating a crime. A better understanding of this behaviour can be used to inform employees responsible for managing systems risk through the implementation of countermeasures.

An application of the model can perhaps illustrate its potential. The 2001 UK Audit Report (Audit Commission, 2001), entitled *Yourbusiness@risk*, cites the example of a local government employee who committed computer input fraud. Prior to the actual perpetration of the fraud, the dishonest staff member developed trusting relationships with his fellow employees. This trust was reflected in the fact that his workmates neglected to lock-down their computers when leaving the office. This vulnerability provided the necessary opening for the offender, as different computers provided different access to parts of an invoicing system. As a consequence, when his colleagues left the office, the dishonest staff member would access their computers to process the fraud. In total, £15,000 was embezzled through the setting-up, inputting and authorisation of fictitious invoices.

When applying the model to the above example, consideration can first be given to the routine activities of the offender. The case highlights a lack of managerial supervision leaving the offender *unhandled*. Indeed, the Audit Report (Audit Commission, 2001) notes how the local authority subsequently increased oversight of employees working with the invoicing system. Although not mentioned in the case, it could be that the embezzlement was motivated by an addiction, marital breakdown, financial problems and so forth. Did the local authority have any monitoring or counselling in place to help identify and address these potential problems?

As noted in the model, unhandled offenders and factors such as addictions and marital break-downs provide the *numbers* for and *motivations* of *potential offenders*. At the *search/perception* and *information/ modelling* stage of the crime specific opportunity structure, offenders assess their environment (awareness space), gleaning information about any security vulnerabilities that may possibly be exploited. It is clear that this offender had a sound knowledge of existing security vulnerabilities. With regard to the concept of bounded rationality, given that he worked in the organisation where the crime took place, the offender had access to a relatively high quality of information. During the course of his routine activities the offender was, therefore, able to garner the requisite information. More specifically, the dishonest employee was able to gather precise knowledge about the *guardianship factors* designed to safeguard the *target*, in this instance the invoicing system. Hence, the offender was able to identify the vulnerability created when colleagues, on leaving the office, failed to lock-down their computers (creating a lack of guardianship). Indeed, the offender was instrumental in creating the vulnerability by fostering trusting relationships with workmates. This ability to manipulate the environment in which the crime takes place is an option open to relatively few offenders, and generally only to those who are employed in such contexts.

To set up, input and authorise the fictitious invoices, the rogue employee required access to a number of computers. Thus, at a technical level, there was a segregation of access rights. While this safeguard was overcome by the offender, in order to perpetrate the fraud he also required working knowledge of the whole invoicing system. There is no mention in the Audit Report, of how this *cognitive facilitator* was acquired by the offender. It is possible that he was previously employed by the local authority to work on other parts of the invoicing system, thus enhancing his knowledge of the processes. Alternatively, the offender might have abused the trust developed with colleagues, by 'innocently' enquiring about the workings of the system. In either case, the offender was able to develop the cognitive facilitator to a level which afforded perpetration of the fraud.

The above example can be seen to support the concepts inscribed in the crime specific opportunity structure. In addition, the criminological theories can further be drawn on to provide tools, techniques and analytical methods for practitioners intent on reducing systems risk. For example, organisations could adopt the opportunity-reducing techniques advocated by SCP. Their implementation would be aided by the fact that the techniques are underpinned by a theoretical conceptualisation of the offender, advanced by the rational choice perspective. As a consequence, the range of techniques offers a thorough and systematic classification for practitioners.

Another example, which can be seen to support the application of the model and efforts to reduce systems risk, concerns the development of crime scripts (Cornish, 1994; Willison, 2005). This preventive method can assist in the implementation of suitable safeguards, through the analysis of the criminal behaviour, which leads to the commission of a crime. Although originally developed to assist in the implementation of SCP controls, there is no reason why the method could not be utilised by IS security practitioners (Willison, 2005). Indeed, it should be noted that, in keeping with the crime specific opportunity structure, scripts also have a crime-specific focus.

The origins of this method can be found in the field of cognitive science, which has addressed the production and understanding of sequences of events and actions. As its name suggests, the concept derives from recognition of how knowledge about processes and routines take a specific form, similar to a theatrical script (Schank and Abelson, 1977). When applied to criminal behaviour, the aim of developing scripts is to help practitioners correctly to identify the stages (or 'scenes') in the commission of a crime. Through a clearer understanding of these stages, greater insight is afforded into the placement of suitable controls.

Table 1 provides an example of a crime script developed with regard to the local authority fraud (Willison, 2005). The first column represents the stage in the script.

With each stage comes a corresponding behaviour. Once this behaviour is correctly identified, suitable controls can be applied. Used in conjunction with the crime specific opportunity structure, a related script can enhance understanding of the interaction between the potential offenders, targets and facilitators.

Table 1 Computer Input-Fraud Script

SCENCE FUNCTION	SCRIPT ACTION	SITUATIONAL CONTROL
Preparation	Deliberately gaining access to the organisation	Prospective employee screening
Entry	Already authorised as employee	------
Pre-condition	Wait for employees absence from offices.	Physical segregation of duties. Staggered breaks Signing In/Out of offices
Instrumental Pre-Condition	Access colleagues' computers	System time outs Biometric fingerprint authentication
Instrumental Initiation	Access programmes	Password use for access to specific programmes
Instrumental Actualization	False customer account construction	Two person sign-off on creation of new accounts
Doing	Authorisation of fictitious invoices	Audit of computer logs Budget monitoring
Post Condition	Exit programmes	------
Exit	Exit system	User event viewer
Doing Later	Spend the transferred money	------

(Willison, 2005)

Discussion

The model elaborated in this paper may act as a useful conceptual schema, with its consideration of offender behaviour in the organisational context. Insights gleaned through the application of the model can then be used to inform practitioners' knowledge of local systems risk. This is turn can likewise be used to inform the implementation of countermeasures. Undoubtedly all of the safeguards indicated in the example of the local government fraud are already being implemented by good security management in many organisations. What the crime specific opportunity structure offers is a holistic conceptualisation of the problem under scrutiny, and the means through which to analyse the said problem. In this way, management may draw on the model for guidance when considering systems risk.

Furthermore, as the crime specific opportunity structure affords additional guidance on safeguard implementation, uncertainty is reduced with regard to the input from those departments collectively responsible for IS security. This guidance is enhanced by the model through its identification of the different aspects of the offender (e.g. motivation, search patterns). Indeed, the role of the respective departments can be elicited more accurately if the model is used in conjunction with the scripts concept. This would help to ensure the appropriate implementation of safeguards and the departments responsible for them.

As security breaks out of its technical citadel to become a ubiquitous reality for all users of information, there is a pressing need for a theoretical framework against which practitioners may diagnose problems, plan action and implement solutions. The question then becomes one of which theory? If we are attempting to address computer criminals and their criminal behaviour, criminology would appear a suitable body of theory from which to draw on (Harrington, 1996; Straub and Welke, 1998; Willison, 2004, 2005). Each theory inscribed in the model may potentially offer the practitioner new insights into the behaviour of dishonest staff. The rational choice perspective, for example, affords practitioners a theoretical insight into the decision-making processes undertaken by potential offenders. As noted with the literature on opportunity, common sense perceptions, which more often than not guide security practices, often fail on closer scrutiny, and hence the importation of criminological theory may prove timely.

Conclusions and Further Research

The likelihood that an IS is inadequately protected against certain types of damage or loss constitutes systems risk (Straub and Welke, 1998). When addressing the latter, consideration should be given to the threat posed by dishonest employees, intent on committing some form of computer abuse (Dhillon and Moores, 2001; Kesar and Rogerson, 1998). A number of researchers have examined the extent to which those responsible for managing security are cognizant of the very nature of systems risk. Goodhue and Straub (1991) advance a model of managerial perceptions of this form of risk. They note how informed perceptions are based on knowledge of 'organisational environment', 'IS environment' and 'individual characteristics'. In terms of individual characteristics, this refers to knowledge of local systems risk and the associated threats.

Unfortunately, existing research notes how practitioners' knowledge of individual characteristics is often 'fragmented' and 'incomplete', contributing to situations where efforts to reduce systems risk are often less than effective (Straub and Welke, 1998; Loch et al, 1992; Straub, 1986a; Straub, 1986b). To complicate matters, any effective attempt to enforce IS security requires input from a number of departments, including, for example, HR, IS/IT, and physical security (Schlarman, 2002; Fitzgerald, 2005; ISO/IEC 17799:2000, 2000).

In an attempt to compliment existing research, but also representing a departure, this paper addresses systems risk from the offender's perspective. More specifically a model known as the 'Crime Specific Opportunity Structure' is advanced (Willison, 2002). Drawing on a number of criminological theories, the model potentially aids conceptualisation of the relationship between the offender, the organisational context, the requisite safeguards and the departments responsible for them.

SCP systematically classifies a range of safeguards which could feasibly be adopted for the IS security domain. The rational choice perspective provides insights into the decision making processes of the offender. Complemented by the 'scripts' concept, there is the potential for a clearer understanding of the stages (scenes) of a specific crime. In a similar vein, environmental criminology acknowledges the multiple stages, and the related decisions, of a criminal act. In addition, this body of theory addresses the search patterns of offenders with regard to potential targets. Each specific environment emits cues relating to spatial, cultural, legal and psychological characteristics. As a consequence, an experienced offender is able to discern 'good' targets, which are characterised by certain sequences and configurations of these cues.

Appreciating and understanding these sequences and configurations may have implications for IS security control environments. Finally, routine activity theory looks at the elements required for a crime to occur. Central to this approach is an appreciation of how individuals act as guardians over potential targets. As seen, it was the failure by the local authority to provide guardianship over their computers, which enabled the perpetration of the fraud by their dishonest employee. Understanding the chemistry of crimes and the role of facilitators (both in terms of how they are developed and prevented), may provide additional food for thought for practitioners.

When these approaches are combined in the form of the crime specific opportunity structure, there is the potential for a deeper understanding of the relationship between an offender and the environment in which they commit crime. More informed insights into this relationship can feasibly inform managers as to the nature of opportunities in the organisational context, when addressing systems risk. Based on such insights, managers can use this knowledge to underpin the application of countermeasures. In addition, the criminological theories can further be drawn on to provide tools, techniques and analytical methods for enhancing the application of countermeasures.

Theoretical coherence of the crime specific opportunity structure

In an attempt to assess the theoretical soundness of the model, further research could involve the application of the model to numerous forms of computer abuse. By doing so, theoretical shortcomings of the crime specific opportunity structure would be evident. From another perspective, the application of the model can be seen as a chance to develop the criminological concepts inscribed in the theories (Willison, 2002, 2004). The use of such theory in new contexts enables the possibility of expanding and enhancing existing themes and concepts. Facilitators are a case in point. Traditional examples of this concept (e.g. get-away cars, guns for robberies) have a physical nature. Examining computer abuse in the organisational setting affords consideration of those facilitators used by rogue employees. While 'cognitive' facilitators are a marked departure from their physical cousins, their role is the same. As with traditional facilitators, preventive strategies can consider control techniques e.g. segregation of duties.

The value of the model for practitioners:

Further research is required to investigate whether the crime specific opportunity structure is able to provide practitioners with a better view of the problem domain, including the interaction between the potential offenders and their environments. Does the model identify organically problems that would otherwise be randomly addressed or indeed ignored altogether? How far can the model be used as a basis for educating managers about local systems risk? Can the model be used to support safeguard allocation?

The perspective offered by the crime specific opportunity structure provides a potential alternative to some of the technocratic approaches to IS security. While further research is required to assess the feasibility of the model, introducing criminology into the field offers news perspectives and opens up the way for much-needed theoretical imports.

References

Anderson, R. (1994) Why Cryptosystems Fail. *Communications of the ACM* 37 (11): 32-40.

Audit Commission. (1994) *Opportunity Makes a Thief: An Analysis of Computer Abuse*. London. Audit Commission Publications.

Audit Commission. (1998) *Ghost in the Machine: An Analysis of IT Fraud and Abuse*. London. Audit Commission Publications.

Audit Commission. (2001) *Your Business@Risk: An Update on IT Abuse 2001.* London. Audit Commission Publications.

Backhouse, J. (1997) Information at Risk. *Information Strategy*. January: 33-35.

Bandura, A. (1976) Social Learning Analysis of Aggression. In E. Ribes-Inesta and A. Bandura (eds.), *Analysis of Delinquency and Aggression*. Hillsdale, NJ. Lawrence Erlbaum Associates, Publishers.

BloomBecker, J. (1984) Introduction to Computer Crime. In J. Finch and E. Dougall (eds.), *Computer Security: A Global Challenge*. North-Holland. Elsevier Science Publishers.

Bologna, J. (1993) *Handbook on Corporate Fraud.* Boston. Butterworth-Heinemann.

Brantingham, P. and Brantingham, P. (1991) Environmental Criminology. (2nd ed.). Prospect Heights, IL. Waveland Press.

Clarke, R. (1980) Situational Crime Prevention : Theory and Practice. *British Journal of Criminology* 20: 136-137.

Clarke, R. (ed.) (1992) *Situational Crime Prevention : Successful Case Studies*. Albany, NY. Harrow and Heston.

Clarke, R. (1995) Situational Crime Prevention. In M. Tonry and D. Farrington (eds.), *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research*. Vol. 19. Chicago. University of Chicago Press.

Clarke, R. (ed.) (1997) *Situational Crime Prevention : Successful Case Studies*. 2nd ed. Albany, NY. Harrow and Heston.

Clarke, R. and Cornish, D. (1985) Modelling Offender's Decisions : A Framework for Policy and Research. In M. Tonry and N. Morris (eds.), *Crime and Justice : An Annual Review of Research*. Vol. 6. Chicago. University of Chicago Press.

Clarke, R. and Cornish, D. (2000) Rational Choice. In R. Paternoster and R. Bachman (eds.), *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory*. Los Angeles, CA. Roxbury Publishing Company.

Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends : A Routine Activity Approach. *American Sociological Review* 44: 588-608.

Comer, M. (1998) *Corporate Fraud* (3rd ed.). Vermont. Gower.

Cornish, D. and Clarke, R. (1986) Situational Prevention, Displacement of Crime and Rational Choice Theory. In K. Heal, and G. Laycock (eds.), *Situational Crime Prevention: From Theory into Practice*. London. H.M.S.O.

Cornish, D. (1994) The Procedural Analysis of Offending and its Relevance for Situational Prevention. In R. Clarke (ed.) *Crime Prevention Studies*, Vol. 3. Monsey, NY. Criminal Justice Press.

Cusson, M. (1986) L'analyse Strategique et Quelques Developpements Recente en Criminologie. *Criminologie* 19: 51-72.

CSI/FBI (2002) *Computer Security Issues and Trends*. San Francisco. CSI.

Dhillon, G. and Moores, S. (2001) Computer Crimes: Theorizing About the Enemy Within. *Computers and Security* 20 (8): 715-723.

Dorey, P. (1994) Security Management and Policy. In W. Caelli, D. Longley and M. Shain, (eds.), *Information Security Handbook*. Macmillan Press Ltd. London.

DTI (2000) *Information Security Breaches Survey*. London. DTI.

Ekblom, P. (1994) Proximal Circumstances: A Mechanism-Based Classification of Crime Prevention. In R. Clarke (ed.), *Crime Prevention Studies*. Vol. 2. Monsey, NY. Criminal Justice Press.

Ernst and Young. (2002) *Global Information Security Survey*. Presentation Services. London.

Felson, M. (1992) Routine Activities and Crime Prevention: Armchair Concepts and Practical Action. *Studies on Crime and Crime Prevention*. 1: 31-34.

Fitzgerald, T. (2005) Building Management Commitment Through Security Councils. *Information Systems Security* 14 (2): 27-36.

Forester, T. and Morrison, P. (1994) *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press. Cambridge, MA.

Goodhue, D. and Straub, D. (1991) Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security. *Information & Management* 20 (1): 13-27.

Hansche, S. (2001) Designing a Security Awareness Program: Part 1. Information Systems Security 9 (6): 14-22.

Hansche, S. (2001a) Information System Security Training: Making it Happen: Part 2. Information Systems Security 10 (1): 51-70.

Hinde, S. (2001) The Weakest Link. *Computers & Security* 20 (4): 295-301.

Hindelang, M., Gottfredson, M. and Garofalo, J. (1978) *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimisation*. Cambridge, MA. Ballinger.

Hirschi, T. (1969) *Causes of Delinquency*. Berkeley and Los Angeles. University of California Press.

Hitchings, J. (1995) Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. *Computers & Security* 14 (5): 377-383.

ISO/IEC 17799:2000 (2000) *Information Technology – Code of Practice for Information Security Management*. ISO.

Kesar, S. and Rogerson, S. (1998) Developing Ethical Practices to Minimize Computer Misuse. *Social Science Computer Review* 16 (3) 240-251.

Loch, K., Houston, C. and Warkentin, M. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly* 16 (2) 173-186.

Luzwick, P. (2001) Security? Who's Got Time For Security? I'm Trying to Get my Job Done. *Computer Fraud & Security*. January 2001.

Nosworthy, J. (2000) Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? *Computers & Security* 19 (4): 337-347.

Osborne, K. (1998) Auditing the IT Security Function. *Computers & Security* 17 (1): 34-41.

Parker, D. (1997) The Strategic Values of Information Security in Business. *Computers & Security* 16 (7): 572-582.

Poyner, B. and Webb, B. (1991) *Crime Free Housing*. Oxford. Butterworth Architect.

Riem, A. (2001) Cybercrimes of the 21st Century. *Computer Fraud & Security.* April 2001.

Schank, R. and Abelson, R. (1977) *Scripts, Plans, Goals and Understanding: An Inquiry into Human Knowledge*. Hillsdale, NJ. Erlbaum.

Schlarman, S. (2002) The Case for a Security Information System. *Information Systems Security* 11 (1): 44-50.

Schneier, B. (1998) Security Pitfalls in Cryptographic Design. *Information Management & Computer Security* 6 (3): 133-137.

Spurling, P. (1995) Promoting Security Awareness and Commitment. *Information Management & Computer Security* 3 (2): 20-26.

Stevenson, G. (2000) Computer Fraud: Detection and Prevention. *Computer Fraud & Security*. November 2000.

Straub, D. (1986a) Computer Abuse and Computer Security: Update on an Empirical Study. *Audit and Control Review* 4 (2): 21-31.

Straub, D. (1986b) *Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment*. Unpublished PhD thesis. Indiana University Graduate School of Business.

Straub, D. and Welke, R. (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly* 22 (4): 441-469.

Sykes, G. and Matza, D. (1957) Techniques of Neutralisation: A Theory of Delinquency. *American Sociological Review* 22: 664-670.

von Solms, B. (2001) Corporate Governance and Information Security. *Computers & Security* 20 (3): 215-218.

Warman, A. (1993) *Computer Security Within Organisations*. London. Macmillan.

Willison, R. (2002) *Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank.* Unpublished PhD thesis. University of London.

Willison, R. (2004) *Understanding the Offender/Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context.* Proceedings of the Hawaii International Conference on Systems Sciences (HICSS-37), Big Island, USA, January 5-8.

Willison. R. (2005) Considering the Offender: Addressing the Procedural Stages of Computer Crime in an Organisational Context. Copenhagen Business School. Department of Informatics Working Paper no. 9.

Wood, C. (1995) Writing InfoSec Policies. *Computers & Security* 14 (8): 667-674.

Wood, C. (1997) Policies Alone Do Not Constitute a Sufficient Awareness Effort. *Computer Fraud and Security*. December 1997.

Wright, M. (2001) Keeping Top Management Focussed. *Computer Fraud & Security*. May 2001.

Yapp, P. (2001) Passwords: Use and Abuse. *Computer Fraud & Security*. September 2001.

Ølnes, J. (1994) Development of Security Policies. *Computers & Security* 14 (8): 628-636.