Working Paper

Considering the Offender: Addressing the Procedural Stages of Computer Crime in an Organisational Context

By

Robert Willison

No. 09 - 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

Considering the Offender: Addressing the Procedural Stages of Computer Crime in an Organisational Context

IS security represents a growing concern for organisations. Although hackers and viruses are often the basis of such concerns, the inside threat of employee computer crime should not be underestimated. From an academic perspective, there are a modest but growing number of texts which examine the 'insider' problem. While attention has been given to the influence on offender actions through deterrent safeguards, there has been a lack of insight into the interactive relationship between offender choices made during the actual perpetration of computer crimes, and the context in which such crimes take place. Knowledge of this relationship would be of obvious interest to practitioners who would aim to manipulate the environment and influence offender choices accordingly. To address this oversight, this paper, therefore, advances two criminological theories which it is argued can be used to examine the stages an offender must go through in order for a crime to be committed i.e. the 'procedural stages' of computer crime. Hence, this paper illustrates how the two theories, entitled the rational choice perspective and situational crime prevention, can be applied to the IS domain, thereby offering a theoretical basis on which to analyse offender choices/behaviour during perpetration. Through such an analysis greater insights may be offered into selecting appropriate safeguards to prevent computer crime.

Introduction

While hackers and viruses fuel the security concerns of organisations, the threat of employee computer crime should not be overlooked. This message is echoed by numerous security surveys which point to the magnitude of the 'insider' problem (CSI/FBI, 2004; DTI/PWC, 2004; E&Y, 2004). The 2004 CSI/FBI Computer Crime and Security Survey (CSI/FBI, 2004) revealed approximately 50% of security breaches occurred within the organisation. From another perspective, respondents to the UK DTI/PWC (2004) survey were asked about the source of their worst security incident. Of those representing small size (1-49 employees) organisations, 32% stated the source was internal. However, this figure rose to 46% and 48% respectively for medium (50-249 employees) and large (250 + employees) companies.

Against this backdrop, a growing number of researchers have turned their attention to the security problems posed by employee computer crime (Straub, 1990; Harrington; 1996; Kesar and Rogerson, 1998). However, to date there has been a lack of insight into the interactive relationship between offender choices made during the perpetration of computer crime, and the context in which such choices take place. An understanding of this relationship would be of obvious interest to practitioners who would attempt to manipulate the environment, and influence offender choices to prevent a criminal act.

To address this oversight, this paper focuses on the procedural stages of computer crime i.e. the stages an offender must go through in order for a crime to be committed. Two criminological theories, entitled the Rational Choice Perspective (Clarke and Cornish, 2000) and Situational Crime Prevention (Clarke, 1997), are advanced to support analysis of these stages. Rather than focussing on 'why' and 'how' people become criminals, these criminological theories attempt to provide explanations of how offenders interact within the

criminal context. Hence, this paper aims to illustrate how the two approaches may offer a theoretical basis on which to analyse the procedural stages of computer crime. It is argued that the theories may complement existing security strategies by helping to identify offender behaviour in all of the procedural stages, and the associated criminal choices which underpin such behaviour. By so doing, greater insights may be afforded into selecting appropriate safeguards to prevent continuation and successful perpetration of the criminal act.

The proceeding section of the paper reviews the existing IS security literature related to the area of employee computer crime. This is followed by an examination of those texts which have addressed computer crime from a criminological perspective. The latter acts as an introduction to a description of the two bodies of theory advanced in this paper, namely the Rational Choice Perspective and Situational Crime Prevention. The penultimate section discusses how these approaches can be applied to address the procedural stages of computer crime, followed by a summary of the main arguments and suggestions for future research, which form the conclusion.

Before examining the relevant literature, it is worth just clarifying the relationship between IS security and computer crime. According to Straub and Welke (1998) IS Security countermeasure strategies consist of four separate, but related, activities which include i) deterrence, ii) prevention, iii) detection and iv) recovery. These four areas are designed to reduce 'systems risk' i.e. a 'systems risk' exists when an IS is insufficiently protected. Hence, the four strategy areas aim to enhance security and protect against threats which include employee computer crime. As noted, the initial aim of an IS security countermeasure strategy would be to deter such activity. If deterrence proved ineffective, the second part of the strategy would aim at preventing the offender from perpetrating computer crime, and so

on. Therefore, consideration should be given to all four areas of the IS security countermeasures strategy to actively reduce 'systems risk'.

Employees and computer crime

Within the broad body of work termed IS security, there are a number of texts related to the area of employee computer crime. This section of the paper, therefore, reviews this literature, which can be seen to fall into four areas and covers safeguards, the psychology of offenders, attributes for offending and the criminal environment.

Safeguards

Several writers have discussed the broad forms of controls which can be used as a safeguard against computer crime by employees (Hoffer and Straub, 1989; Backhouse and Dhillon, 1995; Kesar and Rogerson, 1998; Dhillon and Moores, 2001; Dhillon et al, 2004). Dhillon and Moores (2001), for example, while advocating traditional technical safeguards to enforce access to computer systems and their programmes, further note the need for formal and informal controls. Formal safeguards include written policies for clarifying the appropriate security responsibilities and roles of staff. These are complemented by informal controls, such as education and awareness campaigns which directly aim to influence the security behaviour of employees.

Several researchers consider the behaviour of employees with regard to the deterrent value of safeguards (Campbell, 1988; Hoffer and Straub, 1989; Straub, 1990; Straub and Nance, 1990; Cardinali, 1995; Sherizen, 1995; Harrington, 1996; Straub and Welke, 1998). Of this group, a number have applied General Deterrence Theory to the IS domain (Hoffer and Straub, 1989;

Straub, 1990; Straub and Nance, 1990; Cardinali, 1995; Harrington, 1996; Straub and Welke, 1998). This criminological theory posits that:

> Individuals with an instrumental intent to commit antisocial acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts.
> (Straub and Welke, 1998, p. 445)

Hence, deterrent safeguards advanced by writers in the field include detection activities, public reprimands for staff violating procedures, the bringing of civil and criminal suits against rogue employees, termination of contracts, security awareness programmes and codes of ethics (Campbell, 1988; Hoffer and Straub, 1989; Straub and Nance, 1990; Cardinali, 1995, Harrington, 1996, Straub and Welke, 1998).

The Psychology of Potential Offenders

While there are those writers who consider safeguards to deter offenders, others focus more specifically on the offender by examining the psychology of these individuals (Sherizen, 1995; Harrington, 1995, 1996; Shaw et al, 1998). Based on interviews with offenders, Shaw et al (1998) identified several psychological characteristics. When collectively present in an employee, they argue that these characteristics increase the likelihood of the individual perpetrating some form of computer crime. 'Computer dependency', for example, represents a situation where individuals exhibit addictive behaviour towards their computer and/or the Internet. Experiencing a history of ostracism and social failure, these individuals turn to computers as a substitute for interpersonal relationships.

The psychology associated with the criminal act itself, and the manner in which offenders rationalise their actions has also been a focus for security researchers (Sherizen, 1995;

Harrington, 1996). As part of her study into the influence of codes of ethics on employee computer abuse judgements, Harrington (1996) examines the ability of staff to deny responsibility (RD) for their actions. Those low in RD are able to accept responsibility for their behaviour and follow organisational and legal dictates while those high in RD are prone to ignoring such dictates by shifting responsibility to others. This ability to deny responsibility is also linked to criminal acts and is used by individuals to rationalise their actions in a manner which negates culpability.

Attributes for Offending

Other writers have considered the offender in terms of a series of attributes they require for perpetration (Tugular and Spafford, 1997; Parker, 1976, 1981, 1998; Wood, 2002). Parker (1976, 1981, 1998) argues practitioners need to consider all forms of potential 'cybercriminals' in terms of their skills, knowledge, resources, authority and motives (SKRAM), and as a consequence, the implications for an organisation's security. An alternative perspective is provided by Wood (2002) who solely focuses on the insider. While similarly urging consideration of skills, knowledge and motives, Wood departs from Parker by advocating examination of the offender's risks, processes and tactics.

The criminal environment

Closely related to the attributes for offending is the context in which criminal behaviour takes place (Becker, 1981; Sherizen, 1995). In an early paper on the subject, Becker (1982) argues for a focus on the environment, rather than an individual's personality, for predicting and preventing computer crime. Becker asserts dishonest employees perceive the organisational context in a number of ways and provides a classification of seven 'criminogenic environments'. So, for example, 'the land of opportunity' represents a context in which

dishonest employees exploit security loopholes spotted during the course of their daily work activities.

An alternative perspective is offered by Sherizen (1995) who discusses the 'criminogenic environment' with reference to how an organisation's existing structure, values and culture may help to reinforce a criminal context. As Sherizen states:

> Do employees perceive that access control measures are put in place? Do they feel that security measures are operating? Do they assume that their bosses have little interest in security? Are crime often found in the organization, indicating organizational vulnerability? If these factors are found, the organization may have a climate that supports or in other ways fosters computer crime. If this is true, then security personnel need to actively change organisational structures and employee perceptions.
> (Sherizen, 1995, pp. 180-181)

As noted, writers in the IS security field have considered employee computer crime by focusing on safeguards to prevent such behaviour, the psychology of offenders, attributes for offending and the environment in which it takes place. However, there has been little focus on the actual behaviour of offenders, and the decisions which underpin such behaviour, during the perpetration of computer crimes. To add some context to this argument, it is worth recalling the work of Straub and Welke (1998) who argue IS security countermeasure strategies consist of four activities which include i) deterrence, ii) prevention, iii) detection and iv) recovery. As noted, several researchers focus on deterrence and apply general deterrence theory to examine which safeguards achieve this desired form of behaviour. Hence, such research addresses how controls deter criminal behaviour through influencing the criminal choices of potential offenders.

However, what of the second stage of safeguard strategies i.e. prevention? There is currently a lack of insight into the interactive relationship between offender choices made during the perpetration of computer crime, and the context in which such choices are made. Gaining greater knowledge of this relationship would be of obvious interest to practitioners who could potentially use this knowledge to manipulate the environment and influence offender choices, in order to prevent a criminal act. Advances in this area would complement deterrence efforts and bolster security strategies as a whole. To address this deficiency, two criminological theories are advocated in this paper. Hence, the following section of the text briefly discusses those criminological texts which have addressed computer crime. This acts as an introduction to a description of the theories entitled the Rational Choice Perspective and Situational Crime Prevention. It is argued these two schools of thought enable insight into the offender/context relationship through an examination of the different procedural stages an offender must go through in the perpetration of a crime. By so doing, these theories may possibly enhance prevention strategies through more informed safeguard selection.

Criminology and Computer Crime

Computer crime is a relatively new area of exploration for criminology, accounting for a small but growing number of texts. Common to the vast majority is a preoccupation with crimes which take place via the Internet. The forms of crime examined are diverse in nature, and include telecommunication fraud (Graboksy and Smith, 1998), pornography (Chatterjee, 2001), cyber-stalking (Ellison, 2001), hacking (Duff and Gardiner, 1996) and online securities fraud (Grabosky, Smith and Dempsey, 2001), to name but a few.

Other criminological research has attempted to profile the personal characteristics of computer criminals (Hollinger, 1993; Skinner and Fream, 1997). Using a self-report survey and a sample of graduate students enrolled at a US university, Hollinger (1993), for example, examined the characteristics of those who committed software piracy or accessed the accounts of other end-users on an unauthorised basis.

Related to the aforementioned criminological writings are those texts which fall under the heading of 'white-collar' crime (for reviews of the white-collar literature see Braithwaite, 1985; Coleman, 1987; Nelken, 2002). Topics studied under this umbrella term are diverse and numerous including for example, bribery, price fixing, insider trading, toxic dumping, long-firm fraud, the manufacturing of unsafe pharmaceuticals, and the like (Paternoster and Simpson, 1993; Nelken, 2002). While very few of the white-collar texts have a sole focus on employee computer abuse (Hildreth, 1997), there is a degree of overlap with the IS security field in that issues of prevention and deterrence are examined (Braithwaite and Makkai, (1991); Schnatterly, 2003; Patternoster and Simpson, 1993; Felson; 2002). These studies can be seen as a response to critics who argue researchers in the white-collar field have focussed on 'who' commits such crimes and 'why', to the neglect of addressing the equally if not more important issue of 'how' (Levi, 1984; Braithwaite, 1985; Nelken; 2002). Indeed, of those writers who discuss the issue of prevention and deterrence, a number have turned their attention to the specific behaviour of employees during the commission process (Paternoster and Simpson, 1993, 1996; Felson, 2002). Paternoster and Simpson (1993), for example, advance a rational choice model of corporate crime.

The consideration by white-collar researchers as to 'how' crime is committed reflects changes in criminology as a whole. Clarke (1997) argues one 'mistake' made by modern criminology

is that the task of explaining crime has been assumed to be the same as explaining the criminal (Gottfredsen and Hirschi, 1990). '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. However, 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 setting in which crime may or may not take place (Ekblom, 1994). Through developing such explanations, insights are afforded into the offender/context relationship, which can be used to inform prevention programmes. Hence, what has emerged over the last four decades are a number of approaches entitled Routine Activity Theory (Felson, 2002), Environmental Criminology (Brantingham and Brantingham, 1991), Situational Crime Prevention (Clarke, 1997), and the Rational Choice Perspective (Clarke and Cornish, 2000), which focus on the relationship between an offender and the environment in which crimes occurs. Of these approaches the Rational Choice Perspective and Situational Crime Prevention will now be described, followed by a discussion of how they may be applied to address the procedural stages of computer crime.

Rational Choice Perspective

Although rational choice theory has a considerable academic pedigree in its mother field of economics, it is a relative newcomer to criminology. Admittedly, several rational choice theories do exist in criminology (Clarke and Cornish, 1985, Cornish and Clarke, 1986) but it is the 'perspective' advocated by Clarke and Cornish (2000), which is discussed in this paper.

Central to their perspective are a number of propositions (Clarke and Cornish, 2000). These include the assumption 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.

Another of the propositions relate to 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 an analysis of decision-making needs to be made with reference to specific categories of crime. Legal categories of robbery and auto-theft are too generic, because these umbrella terms cover diversely motivated offences undertaken by a broad spectrum of offenders utilising a plethora of skills and methods. For example, the theft of a car for temporary transport is different from the theft of a car for joyriding, which is again different to the theft of a car to be sold locally or overseas.

Of further importance to the rational choice perspective is the proposition that criminal choices can be categorised into two groups, viz., 'involvement' and 'event' decisions. The former relate to the three stages of the criminal or delinquent career. The offender must make decisions about embarking on criminal activities, whether or not to continue these activities over a period of time, and when, if at all, to cease offending. The latter refers to those decisions made during the commission of a crime, and in the case of suburban burglary, for example, could involve choices as to the target, the point of entry, and decisions about which items to steal. These choices are framed within the crime-specific focus.

The final proposition to be discussed centres on the sequence of event decisions, which an offender faces during the commission of a crime. Original work in this area focused solely on choices made in terms of potential target selection (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 about other stages in the crime commission process (Clarke and Cornish, 2000). These stages include, for example, the preparation, target selection and the actual commission of the criminal act.

Situational Crime Prevention

SCP is a relatively new school of thought. Differing in its focus from most criminology, its starting point is an examination of those circumstances which afford specific kinds of crime. Through an understanding of these situations, measures are introduced to induce change in the relevant environments with the aim of reducing the opportunities for specific crimes. Its emphasis is therefore on the criminal setting. Rather than sanctioning or detecting offenders, the intention is to deter the occurrence of crime, and rather than seeking to reduce criminal tendencies through the enhancement of certain aspects of society, such as better housing or education, the relatively simple aim is to make criminal action less appealing to offenders (Clarke, 1997).

Efforts to achieve this goal involve implementing opportunity reducing techniques, which target specific forms of crime and impact on the immediate criminal environment, in terms of its design, management or manipulation. As can be seen in Table 1, associated with the techniques, are five major aims, which include increasing the effort or risks of crime, or

reducing the potential rewards. These are further complemented by removing the excuses of crime and negating provocative phenomena. Examples of the techniques include *target hardening* (e.g. anti-robbery screens: to increase the effort), *utilising place managers* (multiple clerks in convenience stores: to increase the risks), *target removal* (e.g. removable car radios: to reduce the rewards), *reducing frustrations and stress* (e.g. efficient queues and polite service: to reduce provocations) and the *setting of rules* (e.g. harassment codes: to remove excuses), (Cornish and Clarke, 2003).

In an attempt to block the commission of specific crimes, measures introduced into the immediate environment are designed to impact on the offender's perceptions about the potential costs and benefits of crime commission. In addition, 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 offenders 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 feeling through the construction of excuses such as 'everybody else does it', 'I'm just borrowing it', etc (Clarke, 1997). SCP theorists have further acknowledged how the immediate environment may not only afford potential opportunities, but also provoke criminal behaviour. Hence a number of techniques have been developed to assuage such phenomena (Cornish and Clarke, 2003).

A final point to mention, and in keeping with the Rational Choice Perspective, is SCP's crime specific focus. Forgoing, for example, 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. The argument advanced is that only a detailed understanding at the level of 'specific crimes' will afford insights for prevention programmes.

Table 1: Twenty –five Techniques of Situational Prevention

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
1. Target harden: • Steering column locks and immobilisers • Anti-robbery screens • Tamper-proof packaging	*6. Extend guardianship:* • Take routine precautions: go out in group at night, leave signs of occupancy, carry phone • "Cocoon" neighbourhood watch	*11. Conceal targets:* • Gender-neutral phone directories • Unmarked bullion trucks	*16.Reduce frustrations and stress:* • Efficient queues and polite service • Expanded seating	*21.Set rules:* • Rental agreements • Harassment codes • Hotel registration
2. *Control access to facilities:* • Entry phones • Electronic card access • Baggage screening	*7. Assist natural surveillance:* • Improved street lighting • Defensible space design • Support whistleblowers	*12. Remove targets:* • Removable car radio • Women's refuges • Pre-paid cards for pay phone	*17. Avoid disputes:* • Separate enclosures for rival soccer fans • Reduce crowding in pubs • Fixed cab fares	*22.Post instructions:* • "No Parking" • "Private Property" • "Extinguish camp fires"
3. *Screen exits:* • Ticket needed for exit • Export documents • Electronic merchandise tags	*8. Reduce anonymity:* • Taxi driver IDs • "How's my driving?" decals • School uniforms	*13.Indentify property:* • Property making • Vehicle licensing and parts marking • Cattle branding	*18.Reduce emotional arousal:* • Controls on violent pornography • Enforce good behaviour on soccer field	*23.Alert conscience:* • Roadside speed display boards • Signatures for customs declarations
4. *Deflect offenders:* • Street closures • Separate bathrooms for women • Disperse pubs	9. *Utilize place managers:* • CCTV for double-deck buses • Two clerks for convenience stores • Reward vigilance	*14.Discrupt markets:* • Monitor pawn shops • Controls on classified ads • License street vendors	*19.Neutralise peer pressure:* • "Idiots drink and drive" • "It's ok to say No" • Disperse troublemakers at school	*24.Assist compliance:* • Easy library checkout • Public lavatories • Litter bins
5. *Control tools/weapons:* • "Smart" guns • Disabling stolen cell phones • Restrict spray paint sales to juveniles	*10. Strengthen formal surveillance:* • Red light cameras • Burglar alarms • Security guards	*15.Deny benefits:* • Ink merchandise tags • Graffiti cleaning • Speed humps	*20. Discourage imitation:* • Rapid repair of vandalism • V-chips in TVs • Censor details of modus operandi	*25.Control drugs and alcohol:* • Breathalysers in pubs • Servers intervention • Alcohol-free events

(Cornish and Clarke, 2003)

Hence, Poyner and Webb (1991) assert that preventive measures, needed for tackling burglary of domestic electronic goods, differ from those required to prevent the burglary of household cash or jewellery, owing to the differences in the way these crimes are committed.

The Application of the Rational Choice Perspective to IS Security

While underpinning the techniques advocated by SCP, at a broader level the rational choice perspective provides a framework for helping to explain all forms of crime. The framework acts as a basis for modelling criminal decision making (Clarke and Cornish, 2000).

Involvement Decisions

As previously considered, involvement and event decisions form the two main groups encompassed by the rational choice framework. The former focuses on three stages of the criminal career, which include initiation, habituation and desistance. The extent to which modelling these three stages would provide prevention insights for the IS security field is problematic. This is largely due to the fact that these stages are themselves influenced by 'background factors', 'current life circumstances' and 'situational variables'. Clouding the issue further is the role played by 'background factors'. Citing computer fraud as a case in point, Cornish and Clarke (1986) note how with certain forms of crime, the offender's 'background factors' (which include upbringing, social class, ethnicity, educational opportunities etc.) appear to have little influence on involvement decisions. Hence, attempting to model the three stages of involvement decisions may prove difficult

and ultimately fruitless. However, it is believed that greater inroads can be made into modelling the criminal behaviour associated with event decisions.

Event Decisions

These types of choices are made during the commission process and are framed within a crime specific focus. Early research into this area focussed on the choices made in terms of the criminal target, but, as a result of theoretical advancements, it was realised that the commission of a crime involves a sequence of event decisions. Clarke and Cornish (2000) note, for example, how:

> In the case of suburban burglary, the event may be sparked by some random occurrence, such as two burglars meeting up, both of whom need money … Plans begin to be made and a car or van may be stolen for transport. The next step involves travelling to the neighbourhood selected and identifying a house to enter. Ideally, this holds the promise of good pickings without the chance of being disturbed by the owners. A point of entry that it not too difficult or risky must then be found. Getting into the house and rapidly choosing the goods to steal follow this stage. The goods must then be carried to the car without being seen by neighbours or passers-by. Afterwards, they may have to be stashed safely while a purchaser is found. Finally, they must be conveyed to the buyer and exchanged for cash.
>
> (Clarke and Cornish, 2000, p. 31).

As the burglary example illustrates, other decisions are made at the various stages of the whole commission process. If the stages and the associated decisions can be identified, the preventive scope for many diverse contexts could feasibly be extended. Safeguards

could be implemented which impact on the potential offender's choices and criminal acts, therefore, deterred.

In an attempt to correctly identify the stages in the commission process, Cornish (1994a, 1994b) advances the concept of crime scripts. The origins of this concept can be found in the field of cognitive science, which has addressed the production and understanding of sequences of events and actions (Gardner, 1985). More specifically scripts:

> … constitute one of a family of hypothesised knowledge structures, or schemata, long considered by cognitive psychologists and cognitive social psychologists to organise our knowledge of people and events in ways which guide our understanding of other's behaviour, and our own actions. The script is generally viewed as being a special type of schema, known as an 'event' schema, since it organizes our knowledge about how to understand and enact commonplace behavioural processes or routines.
> (Cornish, 1994a, p. 32).

The concept derives its name from the recognition of how knowledge about processes and routines takes a specific form, similar to a theatrical script (Schank and Abelson, 1977). An example of such a process is the 'restaurant script', which organises an individual's knowledge about what to do in such a context. The sections of the script include entering the establishment, finding a table, ordering, eating, paying the bill and leaving. As the example illustrates, scripts comprise event sequences extended over time. The events in the sequence are interrelated given that events at the early stages of a script afford the occurrence of later ones. For example, in the restaurant script a customer cannot order until they have found a table.

Hence the scripts concept focuses on behavioural processes involved in rational goal-oriented actions. Moreover, the concept affords 'concrete explanations about specific actions in specific domains' (Hewstone, 1989: 103). Given this, Cornish argues that the script concept can act as a useful tool for analysing the 'event' stages in the commission of a specific crime i.e. scripts can be used to address the procedural stages of an offence. As he notes:

> A script-theoretic approach offers a way of generating, organising and systematising knowledge about the procedural aspects and procedural requirements of crime commission. It has the potential to provide more appropriately crime-specific accounts of crime commission, and to extend this analysis to all the stages of the crime-commission sequence.
>
> (Cornish, 1994b, p. 160)

Two sources of information can be used to generate crime scripts. They include offender accounts and secondary sources of data such as published research, security surveys, newspaper accounts etc. While there are obvious practical problems associated with obtaining offender accounts, preliminary efforts could be initiated by the construction of 'draft' scripts through the use of secondary sources. To aid in their development, Cornish (1994a, 1994b) argues that the *universal script* can act as a useful guiding framework. Common to all scripts are a set of generalised scenes, which form the basis of the universal script. The separate elements of this type of script are sequential in order and together they provide a framework that could be used by researchers or practitioners for

modelling the commission of a specific crime. In essence, each 'scene/function' stage of the universal script can be viewed as a procedural stage of a crime.

One advantage of the universal script is that modelling can proceed, regardless of the levels of existing information about the offence in question. Table 2 provides the example of a 'subway mugging' universal script. Under the 'scene/function' heading are listed the procedural stages of the universal script. The second column cites the corresponding criminal behaviour for each stage. Once the crime scripts have been generated, clearer insights are provided into the procedural stages of the particular offence. The practitioner is then given the ability to systematically implement the appropriate controls once granted a greater understanding of a particular crime.

Table 2 Subway Mugging Script

SCENE / FUNCTION	SCRIPT FUNCTION
PREPARATION	Meet and agree on hunting ground
ENTRY	Entry into underground system
PRE-CONDITION	Travel to hunting ground
PRE-CONDITION	Waiting/circulating at hunting ground
INSTRUMENTAL PRE-CONDITION	Selecting victim and circumstance
INSTRUMENTAL INITIATION	Closing–in/preparation
INSTRUMENTAL ACTUALIZATION	Striking at victim
INSTRUMENTAL ACTUALIZATION	Pressing home attack
DOING	Take money, jewelry, etc.
POST-CONDITION	Escape from scene
EXIT	Exit from system

(Cornish, 1994b)

An example of a computer crime script is illustrated in Table 3. Based on details cited in the 1998 UK Audit Report (Audit Commission, 1998) the crime in question involved a

local council employee who committed computer fraud. Taking advantage of poor access security (colleagues failed to lock their computers when leaving the office for a substantial period of time), the employee would wait until other members of staff had vacated the office. He would then access their computers to process the fraud. In total £15,000 was embezzled, through the setting-up, inputting and authorisation of fictitious invoices.

Table 3 Computer 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	------

As noted, with each corresponding script action there is the aim of implementing corresponding controls. However, unlike the more traditional crimes addressed by SCP

and the Rational Choice Perspective, employee computer abuse which is perpetrated in the organisational context can be termed 'specialized access crimes' (Felson, 2002). In other words, only those people who have access to the environment are in a position to commit the crime. It is, therefore, difficult to implement 'entry' and 'exit' controls, for staff who have access to the criminal context as a result of their employment. But, as noted earlier, the elements of a script are interrelated and the scripts actions in a prior stage afford the existence in a later one. In Table 3, therefore, the 'entry' into the organisation is achieved by 'deliberately gaining access to the organisation'. Hence, specialized access crimes can involve either i) long range planning, whereby an individual deliberately applies for a job with the intention of committing an offence, or ii) where an individual applies for a job without criminal intent, but later on, for whatever reason (e.g. becomes disgruntled, develops an addiction, marriage breakdown etc.), decides to perpetrate a crime. Table 3 presupposes the former. Therefore, an appropriate control at the 'Preparation' stage would be the screening of prospective employees.

While the discussion of the 'entry' into environments, which enable specialised access crimes, may appear pedantic, it is precisely this attention to detail which helps to produce effective scripts.

Using the universal framework as a guide to script creation invites consideration of all the procedural aspects of the offence ensuring that no aspect of the commission process is overlooked. In addition the universal script affords examination of the process from the offender's viewpoint and actions. In this way, common-sense 'knowledge' about crime

commission can potentially be debunked and a more rigorous understanding of the commission process can be afforded to those addressing IS security. Ignoring the realities of such behaviour, may result in failing to apply appropriate safeguards or applying safeguards which are inappropriate. Corresponding controls, therefore, can only be implemented if the actions which warrant their application are correctly identified.

While examining offender behaviour, scripts also draw attention to the required attributes for perpetration. As noted, Parker (1976, 1981, 1998) and Wood (2002) have stressed the need to consider the offender in terms of certain attributes such as skills, knowledge, access and resources. The scripts method can enhance this analysis owing to its focus on the offender/context relationship. Hence, offender attributes are more clearly identified as specific contexts plays a large role in defining and delimiting them. So, for example, in the local council fraud, the rogue employee presumably required accounting skills and knowledge of the particular invoicing system. By systematically working through the script stages practitioners could feasibly acquire greater insights into attributes required by the offender. This would hopefully enhance prevention programmes by looking at ways of denying access to such attributes.

The Application of SCP to IS Security

The twenty five techniques advocated by SCP could be adopted by practitioners to complement script analysis. Indeed, to some extent, these techniques are already implicitly used by organisations to enhance their IS security. Examples include property

identification (for computer equipment), removing targets (clear-desk policies), target hardening (a-drive locks), and access controls (for computing resources and organisational physical security). As shown, existing IS security controls can easily be categorised according to the SCP techniques.

While the existing SCP techniques are already partially employed in the IS domain, using the SCP techniques as a guide potentially enables the practitioner to systematically, and explicitly, consider all the alternative safeguard options for influencing the offender's decision making processes. Hence, the practitioner can consider each of the five techniques for increasing the effort, increasing the risk, reducing the rewards, reducing provocations and removing excuses. Using the SCP techniques in conjunction with the script analysis may therefore enable the practitioner to optimise safeguard selection in the following manner. First, the scripts analysis can help in identifying all the stages in the commission process, and secondly, the SCP techniques allow for consideration of alternative safeguards per each stage.

In addition, the SCP techniques encompass areas of prevention which are relatively unexplored by IS security practitioners and whose exploitation may prove fruitful. For example, one of these areas encompasses the SCP techniques entitled 'removing excuses'. An earlier categorisation of the techniques focussed on attempts to increase the risks and efforts and reduced the rewards of crime (Clarke, 1992). Here, the measures tended to rely on the physical manipulation of the criminal environment in an attempt to reduce the opportunities for crime. More recently, however, the rational choice

perspective has developed to encompass recognition of how some offenders assess their own morality, and are often able to absolve themselves of the guilt and shame associated with criminal acts. Such absolution is achieved by individuals rationalising their actions in a manner which helps neutralise these negative emotions. Common examples of these rationalisations include 'I was just borrowing it' and 'everybody else does it'. Support for this assertion comes from earlier criminological and psychological research (Sykes and Matza, 1957; Bandura, 1976, 1977). Focusing on the area of juvenile delinquency, Sykes and Matza, (1957) identify five 'techniques of neutralisation'. Similarly, Bandura (1976, 1977) in attempting to explain the maintenance of aggressive behaviour, discusses how 'self-reinforcing' influences which help to regulate an individual's conduct, can be divorced from aggressive actions. He argues that this is achieved through 'cognitive disengagement', and identifies ten forms. Hence, a group of measures aimed at 'removing excuses' (i.e. the rationalisations) has been advocated (Clarke and Homel, 1997; Clarke, 1997). If offenders can be stopped from rationalising and excusing their criminal actions in specific settings, then they will be open to feelings of guilt and shame.

As noted earlier, there has been some consideration of these rationalisation in the IS security field (Harrington, 1996, Sherizen, 1995), but a more systematic consideration and exploitation of these techniques may complement existing prevention practices. For example, Cornish and Clarke (2003) advance five types of 'removing excuses' techniques, but similar work in this area has been undertaken by Worltey (1996) who identifies four broad strategies through which IS security methods could possibly be enhanced. These areas include 'rule setting', 'clarifying responsibility', 'clarifying

consequences' and 'increasing victim worth'. So, for example, with regard to 'increasing victim worth', such a strategy recognises how offenders find it easier to perpetrate crimes if they perceive their victims to be 'unworthy', 'sub-human', 'outsiders', 'anonymous', or 'deserving of the fate'. The prevention strategy entails attempts to reduce depersonalization and develop an emotional bond between potential offenders and victims. Wortley notes how it is not just individuals but also organisations which are open to this form of offender derogation. Discussing the example of organisational fraud, he argues:

> Employee share schemes, incentive schemes and general attention to reducing job dissatisfaction may increase in employees a sense of attachment to a company and inhibit their ability to portray the company in ways that justify acting fraudulently against it (Wortley, 1996, pp. 122-123).

Conclusion

IS security represents a growing concern for organisations. While external threats require due consideration, the threat posed by rogue employees should not be ignored. From an academic perspective a modest but growing number of texts have addressed the insider threat. However, to date, there has been a lack of attention given to the interactive relationship between offender choices made during the actual perpetration of computer crimes, and the context in which such crimes take place. To address this deficiency the rational choice perspective and situational crime prevention are advanced in this paper, for addressing the procedural stages of crime. Central to the rational choice perspective

is an examination of criminal decisions. Event decisions encompass those choices made by the offender during the crime commission process. By using the scripts method, the various related stages of this process could feasibly be identified. In this way, the goal would be to identify the offender behaviour per each stage and implement controls accordingly. Hence the IS security strategy would aim to disrupt the criminal act through the implementation of safeguards which influence the offender's choices and prevent successful perpetration.

The SCP techniques, based on the conceptualisation of the offender as advocated by the rational choice perspective, could feasibly be used to complement the scripts method. While some of the techniques are already employed in the IS domain, consideration of the complete range advanced by SCP potentially enables the practitioner to systematically, and explicitly, consider all the alternative safeguard options for influencing the offender's decision making processes.

Currently organisations can draw on a number of means for guidance on safeguard selection. These include the use of risk assessment techniques (Peltier, 2004), international standards, such as ISO BS17799 (ISO BS17799, 2000), or the 'baseline security' approach (Parker, 1998), where controls are selected based on best practice principles. Irrespective of whether an organisation uses one or more of these means, by RCP and SCP can both complement existing security practices. The scripts approach can help in understanding the offender/context relationship. Through a greater understanding of the offender choices and the associated behaviour, consideration can then be given to

appropriate safeguards. As noted, the opportunity reducing techniques advanced by SCP can potentially act as a guide for practitioners by enabling them to systematically consider all the safeguard options for influencing the offender's decision making process.

Future research could encompass the development of crime scripts through the use of the action research method (Mathiassen, 2002; Baskerville and Wood-Harper, 1998). More precisely research could involve the use of the universal script as the basis for such development. In this sense, the action research method would be used to evaluate the feasibility of developing script in the organisational context. .

As noted the SCP techniques cover aspects of prevention which are relatively unexplored by IS security researchers. The category of SCP techniques entitled 'removing excuses' is a case in point. Underpinned by rationalization theories advanced by Sykes and Matza (1957) and Bandura (1976, 1977), these SCP techniques represent potentially fruitful areas for future research.

Applying criminological theories to the IS context, has the potential for providing new perspectives and insights, for enhancing security strategies. While progress has been made in recognising and enhancing how employees are central to the security of an organisation (Siponen, 2005), focus should also be placed on how some staff overcome such security through criminal behaviour. To date the application of criminological theory to the IS security field has been minimal, but where better to find insight into crime and criminals than from a body of knowledge which examines precisely that.

References

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

Backhouse, J. and Dhillon, G. (1995) Managing Computer Crime: A Research Outlook. *Computers and Security* 14 (7): 645-651.

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.

Bandura, A. (1977) *Social Learning Theory*. Englewood Cliffs, NJ. Prentice Hall.

Baskerville, R and Wood-Harper, A. (1998) Diversity in Information Systems Action Research Methods. *European Journal of Information Systems* 7 (2): 235-246.

Becker, J. (1981) Who Are the Computer Criminals? *ACM SIGCAS Computers and Society* 12 (1): 18-20.

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

Braithwaite, J. and Makkai, T. (1991) Testing an Expected Utility Model of Corporate Deterrence. *Law and Society Review* 25: 7-39.

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

CSI/FBI (2004) Computer Crime and Security Survey. San Francisco. CSI.

Campbell, M. (1988) Ethics and Computer Security: Cause and Effect. *Proceedings of the 1988 ACM Sixteenth Annual Conference on Computer Science*. Atlanta, Georgia. United States.

Cardinali, R. (1995) Reinforcing Our Moral Vision: Examining the Relationship Between Unethical Behaviour and Computer Crime. *Work Study* 44 (8): 11-17.

Chatterjee, B. (2001) Last of the Rainmacs. Thinking About Pornography in Cyberspace. In D. Wall (ed.) *Crime and the Internet*. London. Routledge.

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

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.

Clarke, R. and Homel, R. (1997) A Revised Classification of Situational Crime Prevention Techniques. In S. Lab (ed.) *Crime Prevention at a Crossroads*. Cincinnati. Anderson Publishing Co.

Coleman, J. (1987) Toward an Integrated Theory of White-Collar Crime. *American Journal of Sociology* 93 (2): 406-439.

Cornish, D. (1994a) Crime as Scripts. In Zahm, D. and Cromwell, P. (eds.), *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. University of Miami, Coral Gables, Florida, 1993. Tallahassee, FL: Florida Statistical Analysis Center, Florida Criminal Justice Executive Institute, Florida Department of Law Enforcement.

Cornish, D. (1994b) 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.

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. and Clarke, R. (2003) Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. In M. Smith and D. Cornish (eds.), *Theory for Practice in Situational Crime Prevention*. Crime Prevention Studies, Vol. 16. Monsey, NY. Criminal Justice Press.

DTI/PWC (2004) Information Security Breaches Survey. London. PWC.

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

Dhillon, G., Silva, L. and Backhouse, J. (2004) Computer Crime at CEFORMA: A Case Study. International Journal of Information Management 24 (6): 551-561

Duff, L. and Gardiner, S. (1996) Computer Crime in the Global Village: Strategies for Control and Regulation – in Defence of the Hacker. *International Journal of the Sociology of the Law* 24. 211-218.

E&Y (2004) Global Information Security Survey.

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.

Ellison, L. (2001) Cyberstalking. Tackling Harassment on the Internet. In D. Wall (ed.) *Crime and the Internet*. London. Routledge.

Felson, M. (2002) *Crime and Everyday Life*. 3rd ed. Thousand Oaks, CA. Sage Publications Ltd.

Gardner, H. (1985) *The Mind's New Science: A History of the Cognitive Revolution*. New York, NY. Basic Books.

Gottfredson, M.R. and Hirschi, T. (1990) *A General Theory of Crime*. Stanford, CA. Stanford University Press.

Grabosky, P. and Smith, R. (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. New Brunswick, NJ. Transaction Publishers.

Grabosky, P., Smith, R. and Dempsey, G. (2001) *Electronic Theft: Unlawful Action in Cyberspace*. Cambridge University Press. Cambridge.

Harrington, S. (1995) Computer Crime and Abuse by IS Employees. Journal of Systems Management 46 (2): 6-11.

Harrington, S. (1996) The Effects of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions. *MIS Quarterly* 20 (3): 257-277.

Hewstone, M. (1989) *Causal Attribution: From Cognitive Processes to Collective Beliefs*. Oxford. Blackwell.

Hildreth, J. (1997) The Enemy Within: Detecting White Collar Crime. *International Review of Law Computers and Technology* 11 (2): 263-266.

Hoffer, J. and Straub, D. (1989) The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review* 30 (4): 35-43.

Hollinger, R. (1993) Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. *Security Journal* 4 (1): 2-12.

ISO 17799 (2000) Information Technology – Code of Practice for Information Security Management. British Standards Institute.

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

Levi, M. (1984) Giving Creditors the Business: Dilemmas and Contradictions in the Organisation of Fraud. *International Journal of the Sociology of Law* 12: 321-33.

Mathiassen, L. (2002) Collaborative Research Practice. *Information, Technology & People* 14 (4): 321-345.

Nelken, D. (2002) White Collar Crime. In M. Maguire, R. Morgan and R. Reiner (eds.) *The Oxford Handbook of Criminology*. Oxford. Oxford University Press.

Parker, D. (1976) *Crime by Computer*. New York. Charles Scribner's Sons.

Parker, D. (1981) *Computer Security Management*. Reston, Virginia. Reston Publishing Company, Inc.

Parker, D. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. New York. Wiley Computer Publishing.

Paternoster, R. and Simpson, S. (1993) A Rational Choice Theory of Corporate Crime. In R. Clarke and M. Felson (eds.) *Routine Activity and Rational Choice*. New Brunswick. Transaction Publishers.

Paternoster, R. and Simpson, S. (1996) Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review* 30 (3): 549-583.

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

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

Schnatterly, K. (2003) Increasing Firm Value Through Detection and Prevention of White-Collar Crime. *Strategic Management Journal* 24: 587-614.

Shaw, E., Ruby, K., Jerrold, M. and Post, M. (1998) The Insider Threat to Information Systems. *Security Awareness Bulletin* 2 : 27-46.

Sherizen, S. (1995) Can Computer Crime be Deterred? *Security Journal* 6 : 177-181.

Siponen, M. (2005) Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods. *Information and Organization*. Article in press.

Skinner, W. and Fream, A. (1997) A Social Learning Theory Analysis of Computer Crime Among College Students. Journal of Research in Crime and Delinquency 34 (4): 495-518.

Straub, D. (1990) Effective IS Security: An Empirical Study. *Information Systems Research* 1 (3) 255-276.

Straub, D., Carlson, P. and Jones, E. (1992) Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security. In Gable, G. and Caelli, W. (eds.) *IT Security: The Needs for International Cooperation*.

Straub, D. and Nance, W. (1990) Discovering and Disciplining Computer Abuse in Organisations: A Field Study. *MIS Quarterly* 14 (1): 45-60.

Straub, D. and Welke, R. (1998) Coping With Systems Risks: 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.

Tugular, T. and Spafford, E. (1997) A Framework for Characterization of Insider Computer Misuse. Unpublished paper, Purdue University.

Wood, B. (2002) *An Insider Threat Model for Adversary Simulation*. SRI International.

Wortley, R. (1996) Guilt, Shame and Situational Crime Prevention. In R. Homel (ed.) *The Politics and Practice of Situational Crime Prevention*. Crime Prevention Studies. Vol. 5.