Working paper no. 04 - 2006

Understanding the Perpetration of Employee Computer Crime in the Organisational Context

by

Robert Willison

Copenhagen
Business School
HANDELSHØJSKOLEN

Department of Informatics
Howitzvej 60
DK - 2000 Frederiksberg

Understanding the Perpetration of Employee Computer Crime in the Organisational Context

While hackers and viruses fuel the IS security concerns for organisations, the problems posed by employee computer crime should not be underestimated. Indeed, a growing number of IS security researchers have turned their attention to the 'insider' threat. However, to date, there has been a lack of insight into the relationship between the actual behaviour of offenders during the perpetration of computer crime, and the organisational context in which the behaviour takes place. To address this deficiency, this paper 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. In addition, 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 the offender/context relationship during the perpetration of computer crime. By so doing, practitioners may use these insights to inform and enhance the selection of safeguards in a bid to improve prevention programmes.

Keywords: IS Security; criminology; employee computer crime; perpetration.

1. 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; Ernst &Young, 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. For 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 relationship between the actual behaviour of offenders during the perpetration of computer crime, and the organisational context in which such behaviour takes place. To address this oversight, this paper focuses on the stages an offender must go through in order for a crime to be committed i.e. the procedural stages. Two criminological theories, entitled the Rational Choice Perspective (Clarke and Cornish, 2000) and Situational Crime Prevention (Clarke, 1997), are advanced to support analysis of the stages comprising employee computer crime. Rather than focussing on 'why' and 'how' people become criminals, these theories focus on the perpetration of crime. It is argued that the Rational Choice

Perspective and Situational Crime Prevention may complement existing security strategies by potentially offering a theoretical basis by which to identify offender behaviour in all of the procedural stages, and the associated criminal choices which underpin their actions. In so doing, practitioners may use these insights to inform and enhance the selection of safeguards to prevent the successful perpetration of employee computer crime.

The proceeding section of the paper reviews the existing IS security literature related to the area of employee computer crime. This is followed by a discussion which centres on the difference between those criminological theories which focuses on the criminal act as opposed to theories of criminality. The discussion serves 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.

2. Employees and computer crime

Within the field of IS security, there are a number of studies related to the area of employee computer crime. This section of the paper, therefore, reviews this literature, which can be seen to fall into five areas and covers safeguards, deterring offenders, criminal intentions, attributes for offending and the criminal environment.

2.1 Safeguards

Several writers have discussed the range of controls which can be used as a safeguard against computer crime by employees (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 limit 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. While the aforementioned papers have proven useful in discussing the need for a focus on the behavioural as well as technical safeguards for IS security, such discussions are held at a high level, and offer little guidance for practitioners, when considering the choice and application of suitable controls for specific contexts.

2.2 Deterring offenders

A number of researchers have focused specifically on the deterrent effect 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, several have applied General Deterrence Theory to the IS security domain (Hoffer and Straub, 1989; Straub, 1990; Straub et al, 1992; 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)

Given the above, deterrent safeguards advanced by writers in the IS security field include, for example, detection and monitoring activities (Hoffer and Straub, 1989; Straub et al. 1992), security awareness programmes (Straub and Welke, 1998) and codes of ethics (Harrington, 1996).

General Deterrence Theory provides valuable insights into the deterrent effect of safeguards, but as soon as the offender moves beyond the point of deterrence and embarks on a criminal act the theory is limited. Admittedly, writers in the IS security field have discussed General Deterrence Theory in terms of preventive controls and the relationship with computer criminals. Indeed, Straub and Welke (1998) argue IS security countermeasures consist of four separate, but related, activities which include i) deterrence, ii) prevention, iii) detection and iv) recovery. These four areas are designed to enhance IS security by reducing systems risk. As noted, the initial aim of an IS security countermeasures 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. Similarly, if preventive controls proved ineffective then detection activities are required, and so on. However, with regards to the explanatory value of General Deterrence Theory, preventive controls are discussed only in terms of their deterrent effect. As Straub and Welke note:

> … all of these organizational responses [the four elements of the safeguard strategy] lead to a downstream effect of deterring future computer abuse … From the perspective

> of general deterrence theory, these four kinds of defense can contribute dynamically to a subsequent deterrent effect. That is, potential abusers become convinced of the certainty and severity of punishment for committing certain acts when the effectiveness of the systems security is obvious or when it is communicated to them (Straub and Welke, 1998, p. 446).

However, as noted, General Deterrence Theory is unable to provide any theoretical insights into the actual act of perpetration, and the behaviour of offenders during such an act.

2.3 Criminal intentions

In a bid to enhance theoretical explanations of insider computer crime several writers have focussed on the criminal intentions of individuals. Drawing on the theory of planned behaviour (Ajzen, 1991), Lee and Lee (2002) focus on the three factors, which according to advocates of the theory, form the intentions for behaviour. These include attitudes toward the behaviour, subjective norms and perceived behavioural control. Advancing their own interpretation of these three factors, Lee and Lee (2002) propose the use of criminological theory. More specifically, they argue Social Bond Theory, Social Learning Theory and General Deterrence Theory can help explain how attitudes towards behaviour, subjective norms and perceived behavioural controls are formed. For example, according to the theory of planned behaviour subjective norms refers to the social pressure that is placed on individuals, by their referent peers in the performance (or not, as the case may be) of specific behaviour. Lee and Lee (2002), therefore advocate the use of Social Learning Theory to explain this phenomenon. Used in the study of how individuals form criminal tendencies, this theory notes the influence of peers in transmitting delinquent values.

Lee et al (2004) also couch their work within the theory of planned behaviour. They advance ‘an integrative model of computer abuse’ based on General Deterrence Theory and Social Control Theory (Hirschi, 1969). The latter examines how four factors – attachments, commitment, involvement and belief – constitute a social bond between an individual and society. This bond in effect acts as a form of social control. Based on their interpretation of the theory, Lee et al (2004) propose that the factors which constitute a social bond can be used to represent ‘organizational trust’. Drawing on General Deterrence Theory and Social Bond Theory, Lee et al develop a number of constructs and hypothesis to examine the influence of deterrence and ‘organisational trust’ on the intentions to commit computer abuse. Based on the results of their study, they contend that the development of social bonds in the form of organisational trust could be one method of reducing the intentions for computer abuse.

Hence, Lee and Lee (2002) and Lee et al (2004) have advocated the used of criminological theories to help explain how criminal intentions are formed. While these theories may assist in understanding this phenomenon, this is not the same as explaining the criminal act (Ekblom; 1994; Clarke, 1997). What are also required are complementary theories, which assist in the understanding of the offender/context relationship during perpetration.

2.4 Attributes for Offending

Other writers have considered the offender in terms of a series of attributes they require for the perpetration of computer crime (Parker, 1976, 1981, 1998; Wood, 2002). Parker (1998) argues practitioners need to consider all forms of what he calls ‘cyber-criminals’ in terms of their skills, knowledge, resources, authority and motives (SKRAM). In other words, what skills, knowledge etc. does an offender require for the commission of computer crime, and what are the implications for organisational 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 methods to avoid risk, the associated tactics and the processes involved in perpetration. Indeed, given the nature of this paper, the latter is particularly relevant. However, Wood fails to explain how risk avoidance methods, tactics and the processes involved in perpetration should be researched. In addition, no theory is advanced to help examine these three factors. This is also the case in terms of the attributes for offending, where Parker (1998) and Wood (2002) offer no guidance in terms of their study and no relevant theories are proposed.

2.5 The Organisational Context

Closely related to the attributes for offending is the consideration of the organisational context in which computer crime takes place (Becker, 1981; Sherizen, 1995). Becker (1981) for example, argues for a focus on the organisational surroundings, 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 he provides a classification of seven 'criminogenic environments'. By this, Becker means that if the context of an organisation reflects one (or more) of the seven types, then the organisation will be vulnerable to various forms of computer crime. So for example, one of the seven types, 'the land of opportunity', represents an organisational context in which dishonest employees exploit security loopholes spotted during the course of their daily work activities. Unfortunately, Becker (1981) does not elaborate on how the offender's perceptions are formed, in terms of the organisational context, and hence how some environments are judged as criminogenic as opposed to others.

Although the literature concerned with employee computer crime has proven useful in highlighting this problem and offering guidance for practitioners, there are, as noted, certain deficiencies. The following section of the paper discusses the differences between those criminological theories which focus on the criminal act as opposed to theories of criminality. The discussion serves 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, which it is argued can help in addressing the deficiencies discussed in the literature review.

3. Criminological theories of crime and criminality

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. As Clarke (2004) notes:

> When prevention and control are the objectives, research will need to focus more on *how* crime is committed and less on *why* it is committed. Understanding the steps in the process of committing crime, and understanding the conditions that facilitate its commission, helps us to see how we can intervene to frustrate crime (Clarke, 2004, p. 59).

Two closely related criminological theories entitled the Rational Choice Perspective (Clarke and Cornish, 2000) and Situational Crime Prevention (Clarke, 1997) have proved central to understanding 'the process of committing crime'. It is for this reason that these approaches, are advanced in this paper for their application to the IS security field. In addition, these two schools of thought may offer a theoretical basis on which to analyse 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, practitioners may potentially use these insights to inform and enhance the selection of safeguards to prevent the successful perpetration of employee computer crime.

The two approaches will now be described, followed by a discussion of how they may be applied to address the procedural stages of computer crime.

4. The Rational Choice Perspective and Situational Crime Prevention

4.1 Rational Choice Perspective

Central to the Rational Choice Perspective advocated by Clarke and Cornish (2000), are a number of propositions. 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, preparation for the crime and target selection.

4.2 Situational Crime Prevention

Situational Crime Prevention 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 for 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

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)

excuses such as ‘everybody else does it’, ‘I’m just borrowing it’, etc (Clarke, 1997). Situational Crime Prevention 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 Situational Crime Prevention’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. 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.

5. The Application of the Rational Choice Perspective to IS Security

While underpinning the techniques advocated by Situational Crime Prevention, 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).

5.1 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 are additional problems related to the category of '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.

5.2 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 concentrated 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 influence the potential offender’s choices, leading to the cessation of the criminal act.

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, p. 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)

Aside from utilising the knowledge of IS security practitioners, two additional sources 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 and practitioner knowledge. 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.

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 Situational Crime Prevention 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 script's 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 permits 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 (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.

6. The Application of Situational Crime Prevention to IS Security

The twenty-five techniques advocated by Situational Crime Prevention could be adopted by practitioners to complement script analysis. Using the Situational Crime Prevention techniques as a guide potentially enables the practitioner to consider new and alternative safeguard options for influencing the offender's decision-making processes. In conjunction with the script analysis the techniques 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 techniques allow for consideration of alternative safeguards per each stage.

Some of the SCP techniques are already implicitly used in the organisational context. Examples include property marking (to *identify property*), clear desk/screen policies (to *remove targets*), anti-virus detection (to *target harden*) and firewalls (to *screen exits*). However in a bid to enhance the selection of safeguards for each stage, existing IS security controls could be categorised according to the 25 techniques. Table 4 represents a first attempt to classify some of the safeguards cited in the 'Information Technology - Security Techniques – Code of Practice for Information Security Management ISO/IEC 17799: 2005', according to the 25 techniques.

While it proved relatively easy to find examples for some of the twenty five categories, this was not the case for others which have a limited number or no examples cited. However, this is to be expected given that these techniques (and their associated controls) have been used and developed in a number of diverse contexts in a bid to reduce the opportunities for crime. Hence, the extent to which safeguards based on 'Reduce Emotional Arousal' and 'Disrupt Markets' are suitable for the organisational context is debatable, but this does not mean that they should be rejected outright. Rather they should be examined in future research by looking at how the controls, which fall under these headings, have been used and their potential for the IS context considered. Indeed, just through constructing the table the author thought of several other controls, which are not cited in the standard, but could be incorporated into the classification. These safeguards are underlined in Table 4. So, for example, the classification of controls under category number 11 entitled 'Conceal Targets' include the measure 'Reduce Website Details'. The latter relates to the threat posed by social engineers. This group of computer criminals target personnel in organisations.

Table 4: IS Security Safeguards Categorised According to the 25 SCP techniques

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
6. Target harden: a) Anti-virus detection for PCs b) Security education for staff c) Physical locks for PCs	*6. Extend guardianship:* a) Staff chaperoning of visitors. b) Supervision of staff in secure areas c) Guardianship of mobile facilities outside offices.	*11. Conceal targets:* a) Minimise ID of offices b) Conceal use of PCs when travelling c) Reduce website details	*16.Reduce frustrations and stress:*	*21.Set rules:* a) IS security polices b) Disciplinary procedures c) Conflicts of interest guidelines
7. *Control access to facilities:* a) Swipe card for office access b) Physical locks for doors c) Password systems	*7. Assist natural surveillance:* a) Open plan offices b) Support whistleblowers	*12. Remove targets:* a) Clear desk and computer screens b) Paper shredders c) Secure disposal of old PCs d) Regulate use of DSB devices	*17. Avoid disputes:*	*22.Post instructions:* a) Email disclaimers
8. *Screen exits:* a) Firewalls b) Security guards c) Reception desks	*8. Reduce anonymity:* a) ID tags for staff b) Audit trails c) Event logging	*13.Indentify property:* a) Property marking b) Digital signatures	*18.Reduce emotional arousal:*	*23.Alert conscience:* a) Copying software is illegal
9. *Deflect offenders:* a) Segregation of duties b) Confidentiality agreements c) Personnel screening	*9. Utilize place managers:* a) Management supervision b) Two person sign-off c) Monitoring by systems admin’r	*14.Discrupt markets:*	*19.Neutralise peer pressure:*	*24.Assist compliance:* a) Security education for staff b) Single sign-on
10. *Control tools/weapons:* a) Password mgt systems b) Download controls c) Deletion of access rights for ex-employees	*10. Strengthen formal surveillance:* a) Intrusion detection systems b) Security guards	*15.Deny benefits:* a) Encryption b) Property marking c) Software dongles	*20. Discourage imitation:* a) Rapid repair for web defacement b) Prompt software patching	*25.Control drugs and alcohol:* a) Drug testing

Adopting the false identity of an employee, a journalist, supplier etc. the social engineer acquires potentially lucrative information from the organisation, based usually on telephone calls with the target (an unwitting member of staff). Unfortunately organisations often aid social engineers by placing far too much information on their websites about employees, their job responsibilities and the department in which they work. Social engineers can either adopt the persona of someone cited on a website, or use their details to sound more credible to the target. Hence, by reducing website details organisations can potentially 'conceal targets'.

As noted, the Situational Crime Prevention techniques encompass areas of prevention which are relatively unexplored by IS security practitioners and whose exploitation may prove fruitful. One area that appears to offer great potential is the category 'Remove Excuses'. An earlier categorisation of the techniques focussed on attempts to increase the risks and efforts and reduce 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 consider how some offenders assess their own morality, and how they 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.

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).

7. 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 relationship between the actual behaviour of offenders during the perpetration of computer crime, and the organisational context in which such behaviour takes 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 Situational Crime Prevention 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 Situational Crime Prevention 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, 2005), 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, the Rational Choice Perspective and Situational Crime Prevention can both complement existing security practices. The scripts approach can help in understanding the offender/context relationship. Through a greater understanding of offender choices and the associated behaviour, consideration can then be given to appropriate safeguards. As noted, the opportunity reducing techniques advanced by Situational Crime Prevention 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 scripts in the organisational context.

As part of the script development process, future research could also encompass the use of the twenty-five SCP techniques. Would the practitioners view the schema as restricting or a useful brainstorming tool in the process of safeguard selection? Could the techniques encourage innovation in the area of IS security prevention and facilitate the incorporation of controls in areas previously not considered?

In relation to the above, and as noted, the Situational Crime Prevention techniques cover aspects of prevention which are relatively unexplored by IS security researchers. The category of techniques entitled ‘removing excuses’ is a case in point. Underpinned by rationalization theories advanced by Sykes and Matza (1957) and Bandura (1976, 1977), these 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

Agnew, R. (1995). Testing the Leading Crime Theories: An Alternative Strategy Focusing on Motivational Processes. *Journal of Research in Crime and Delinquency, 32*(4), 363-398.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

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, & A. Bandura (Eds.), *Analysis of Delinquency and Aggression* (pp. 202-232). Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.

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

Baskerville, R., & 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.

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.

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* (2^{nd} ed.). Albany, NY: Harrow and Heston.

Clarke, R. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research, 10*(1), 55-63.

Clarke, R. and Cornish, D. (1985). Modelling Offender's Decisions : A Framework for Policy and Research. In M. Tonry, & N. Morris (Eds.), *Crime and Justice : An Annual Review of Research*. (Vol. 6) (pp.147-185). Chicago: University of Chicago Press.

Clarke, R. and Cornish, D. (2000). Rational Choice. In R. Paternoster, & R. Bachman (Eds.), *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory* (pp. 27-41). Los Angeles, CA: Roxbury Publishing Company.

Clarke, R., & Homel, R. (1997). A Revised Classification of Situational Crime Prevention Techniques. In S. Lab (Ed.) *Crime Prevention at a Crossroads* (pp. 21-35). Cincinnati: Anderson Publishing Co.

Cornish, D. (1994a). Crime as Scripts. In Zahm, D., & P. Cromwell (Eds.), *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis* (pp. 30-45). 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) (pp. 151-196). Monsey, NY: Criminal Justice Press.

Cornish, D., & Clarke, R. (1986). Situational Prevention, Displacement of Crime and Rational Choice Theory. In K. Heal, & G. Laycock (Eds.), *Situational Crime Prevention: From Theory into Practice* (pp. 1-16). London: H.M.S.O.

Cornish, D., & Clarke, R. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. In M. Smith, & D. Cornish (Eds.), *Theory for Practice in Situational Crime Prevention.* Crime Prevention Studies, (Vol. 16) (pp.151-196). 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

Ernst &Young. (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) (pp. 185-232). Monsey, NY. Criminal Justice Press.

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., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

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.

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

ISO BS17799. (2005). Information Technology – Security Techniques – Codes of Practice for Information Security Management. Switzerland: International Organization for Standardization.

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

Lee, J., & Lee. Y. (2002). A Holistic Model of Computer Abuse Within Organizations. *Information Management & Computer Security*, *10*(2), 57-63.

Lee, S., Lee, S., & Yoo, S. (2004). *An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories, 41*(6), 707-718.

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

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.

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

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

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, 15*(4), 339-375.

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

Straub, D., Carlson, P., & Jones, E. (1992). Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security. In G. Gable, & W. Caelli (Eds.), *IT Security: The Needs for International Cooperation* (pp. 309-324). Amsterdam: Elsevier Science Publishers.

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

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

Sykes, G., & Matza, D. (1957). Techniques of Neutralisation: A Theory of Delinquency. *American Sociological Review 22*(6), 664-670.

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) (pp.115-132).