Copenhagen
Business School
HANDELSHØJSKOLEN

Overcoming the insider: reducing employee computer crime through Situational Crime Prevention

by

Robert Willison & Mikko Siponen

Department of Informatics
Howitzvej 60
DK - 2000 Frederiksberg

WORKING PAPER NO. 11-2006

Dr. Robert Willison * and Professor Mikko Siponen, msiponen@tols16.oulu.fi

* Corresponding author
Dr. Robert Willison
Department of Informatics
Copenhagen Business School,
Howitzvej 60,
DK-2000 Frederiksberg,
Denmark.
E-mail: rw.inf@cbs.dk
Phone: 0045 3815 2388
Fax: 0045 3815 2401

Overcoming the insider: reducing employee computer crime through Situational Crime Prevention

Abstract

Employee computer crime represents a substantial threat for organisations. Yet information security researchers and practitioners currently lack a clear understanding of how these crimes are perpetrated, which, as a consequence, hinders security efforts. We argue that recent developments in criminology can assist in addressing the insider threat. More specifically, we demonstrate how an approach, entitled Situational Crime Prevention, can not only enhance an understanding of employee computer crime, but also strengthen security practices which are designed to address this problem.

Introduction

Information security has become increasingly important for organisations, given their dependence on ICT. Not surprisingly, therefore, the external threats posed by hackers and viruses have received extensive coverage in the mass-media. Yet numerous security surveys also point to the 'insider' threat of employee computer crime. In 2006, for example, the Global Security Survey by Deloitte reports that 28% of respondent organizations encountered considerable internal computer fraud [5]. Although this number may not appear high, the impact of crime perpetrated by insiders can be profound. Donn Parker [6] argues for the need to consider 'cyber-

criminals' in terms of their criminal attributes, which include skills, knowledge, resources, access and motives (SKRAM). What makes dishonest employees such a devastating threat is often the high quality of these attributes which are gleaned from the organisation. Hence, employees use skills gained through their legitimate work duties for illegitimate gain. Knowledge of security loopholes can be exploited and resources and access are provided by companies as a matter of course. It may even be the case that the motive is created by the organisation in the form of employee disgruntlement. Having such a high quality of criminal attributes aids the offender in the pursuit of criminal acts, which in the extreme, can bring down an organisation.

Traditionally companies have addressed the insider threat through a workforce who are aware of their information security responsibilities, and act accordingly. Thus, security policies and complementary education and awareness programmes are now commonplace for organisations. That said, little progress has been made in understanding the insider threat from an offender's perspective. With organisations attempting to grapple with the behaviour of dishonest employees, would not criminology appear to be a useful body of knowledge from which to draw? We argue that Situational Crime Prevention [1], a relative newcomer to criminology, can help enhance initiatives aimed at addressing the insider threat.

The next section of this article, discusses how recent criminological developments, which focus on the criminal act, represents a departure from traditional criminology which examines the causes of criminality. As part of these 'recent developments' we discuss Situational Crime Prevention. After defining this approach we then move on to illustrate how it can inform and enhance information security practices.

Advances in criminology

Traditionally, within criminology, considerable efforts have been spent on developing 'dispositional' explanations, which focus on the causes of criminality. Such explanations 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 consequence more inclined to criminal behaviour. In recent years, however, a number of criminologists have criticised their discipline for assuming that the task of explaining the causes of criminality is the same as explaining the criminal act. Hence, they argue that simply to explain how people develop a criminal disposition is only half the equation. What is further required is an explanation of how crimes are perpetrated. We argue that these criminological approaches, which focus on the criminal act, appear to offer more for information security practitioners, compared with their dispositional counterparts. In particular, one approach, entitled Situational Crime Prevention, will now be discussed. It is believed that SCP can offer additional tools for practitioners in their fight against insider computer crime.

Situational Crime Prevention Defined

The catalyst for the development of Situational Crime Prevention was a series of studies undertaken by the UK Home Office Research Unit (the British government's criminological research department) in the late 1960s and early 1970s. These studies examined whether the rehabilitation of offenders was a suitable form of crime control. Unfortunately, the research cast doubt on the validity of rehabilitation, leading workers in the Unit to explore other crime control options. One such area that appeared to offer promise was ironically first noticed during the course of the

rehabilitation studies of probation hostels and training schools. Both the hostels and schools focussed on youth offenders. It was noted how the likelihood of individuals absconding or re-offending seemed to be dependent more on the type of regime, rather than on the youths' personalities or backgrounds. It was surmised that if their deviant behaviour could be regulated by making changes to certain situational factors, there was the further possibility that other forms of crime could be controlled in the same manner. This body of work allowed for a much more dynamic view of crime, compared to that advanced by dispositional theories. Contrary to the latter, criminal conduct appeared to be influenced by variations in opportunity, transitory pressures and inducements.

From these origins Situational Crime Prevention has emerged. Hence, 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 circumstances, measures are introduced to induce change in the relevant environments with the aim of reducing opportunities for crime. A more formal definition of SCP notes how the approach comprises the implementation of opportunity reducing techniques that a) target specific forms of crime; b) impact on the immediate environment via its design, management, or manipulation, and c) aim to either increase the effort and risks of crime, or to render crime less rewarding or excusable, or to reduce provocative phenomena in the immediate context [1]. A number of points derive from this definition. As mentioned, SCP's focus is crime specific. Avoiding a discussion of crime prevention at the level of, for example 'burglary' or 'robbery', greater emphasis is placed on those specific crimes which fall into these broader categories. Consequently, preventive measures must be tailored to

these specific crimes. So, for example, the preventive measures for tackling the burglary of domestic electronic goods, differ from those required to prevent the burglary of household cash or jewellery.

The definition of SCP further notes how, in a bid to disrupt the commission of specific crimes, safeguards are introduced into the immediate environment. Such actions are designed to impact on the offender's perceptions of the potential costs and benefits of crime commission. The decision to commence and pursue the commission of a criminal act would be based on the offender's favourable evaluation of the situation. The obvious goal, therefore, of those individuals who apply SCP techniques, is to implement safeguards to the point where the offender views certain crimes in an unfavourable light.

The definition of SCP further notes how as part of the criminal decision making process, offenders consider the associated moral costs. However, in a bid to nullify any feelings of guilt associated with a crime, offenders may try to negate such feelings through the construction of excuses such as 'everybody else does it', 'they deserve it' etc. Given this, attempts to stop offenders using such methods may at times prove a useful preventive safeguard. Finally, SCP theorists have further acknowledged how the immediate environment may not only afford potential opportunities, but also help in provoking criminal behaviour. Therefore, a number of techniques have been developed to mitigate such phenomena.

In attempting to reduce the opportunities for crime, a pivotal role is played, not as might be expected, by the criminal justice system, but by a plethora of public and

private agencies, including manufacturing businesses, schools, local parks, entertainment facilities, hospitals, public houses, shopping centres, and the like. Hence, many cases can now be cited where preventive measures have been successfully implemented. Examples include surveillance systems for parks and underground stations, controls on alcohol at music festivals and sporting fixtures, conflict management training for 'bouncers', and street closure/traffic schemes for residential neighbourhoods.

The number of techniques advanced by SCP has developed in line with the evolution of the approach itself. Hence the original eight were succeeded by twelve, then sixteen, to the position whereby twenty-five techniques are currently proposed. As can be seen in Table 1[4], associated with the techniques are five major aims – increase the effort, increase the risks, reduce the rewards, reduce provocation, remove excuses - and under each of the aims are listed five techniques for opportunity reduction. Examples of the techniques include target hardening (e.g. anti-robbery screens in banks and post offices to increase the effort), reducing anonymity (e.g. taxi driver IDs to increase the risks), concealing targets (e.g. unmarked bullion trucks to reduce the rewards), avoiding disputes (e.g. reduce crowding in public houses to reduce provocation) and the setting of rules (e.g. harassment codes: to remove excuses).

Table 1: Twenty –five Techniques of Situational Prevention [4]

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

Applying Situational Crime Prevention to Information Security

From an information security perspective, the twenty-five techniques can potentially be used by security practitioners for considering safeguard options for influencing the offender's decision making process. Indeed, many of the techniques advanced by SCP are already implicitly used by practitioners. Obvious examples include screening exits (e.g. firewalls), removing targets (e.g. clear desk and screen policies), assisting compliance (e.g. single-sign on), target-hardening (e.g. anti-virus detection) and controlling tools/weapons (e.g. password management systems).

In terms of safeguards, information security practitioners face the perennial problem of deciding which controls should be selected for addressing certain risks. Yet, this problem is also a potential stumbling block for crime prevention practitioners, who may have identified the particular crime which needs addressing, but are unsure about which controls to use. In response, the use of crime 'scripts' has been proposed [2, 7, 8, 9]. Originally developed in the field of cognitive science, scripts focus on the behavioural processes involved in rational goal-oriented behaviour. More specifically, scripts are able to enhance understanding of specific behaviour in specific contexts. Given this, scripts have been proposed as a useful tool for examining criminal behaviour. In particular the use of what is termed a 'universal script', has been advanced for helping to correctly identify all the stages in the commission process of a crime and the associated criminal behaviour. Their development could be based potentially on input from security practitioners and other relevant parties such as departmental staff.

Table 2 provides an example of a universal script. In the first column under the heading 'Scene/Function' is cited the different elements of the script. Each element can be seen as a stage in the commission process. In order to more clearly illustrate the stages, column two under the heading 'Script Action' provides some specific content relating to an example of computer crime. The example is taken from the 1998 UK Audit Report entitled 'Ghost in the Machine: An Analysis of IT Fraud and Abuse'. A dishonest local council employee was able to commit computer input fraud by using an invoice system. Although there was a technical segregation – different employees had different access to parts of the system via their PCs – security vulnerabilities were created due to the fact that the offender's colleagues failed to lock-down their computers. Waiting until all the other staff had vacated the office, the dishonest employee would then access all the PCs in order to process the fraud.

Table 2: Universal Script example

SCENCE FUNCTION	SCRIPT ACTION
Preparation	Deliberately gaining access to the organisation
Entry	Already authorised as employee
Pre-condition	Wait for employees absence from offices.
Instrumental Pre-Condition	Access colleagues' computers
Instrumental Initiation	Access programmes
Instrumental Actualization	False customer account construction
Doing	Authorisation of fictitious invoices
Post Condition	Exit programmes
Exit	Exit system

One benefit of developing a script is that it encourages practitioners to consider all the stages of crime commission. In this way, all the criminal behaviour in the process can feasibly be identified. Once this is achieved the next goal is to implement the appropriate controls.

To enhance safeguard selection, crime scripts can be merged with the 25 SCP techniques [8]. Table 3 provides an example of such a merging based on the example of computer crime cited earlier and illustrated in Table 2. Safeguard selection is enhanced as the behaviour of the offender has been identified through the development of the crime script. In addition, with scripts helping to identify all the stages of the commission process and the corresponding criminal actions, this further helps to ensure the optimum use of safeguards. The numbers cited next to each control refer to the type of SCP technique (see Table 1). It is true that no controls are cited under the headings 'Reduce the Rewards', 'Reduce Provocation' and 'Remove Excuses'. To some extent this is to be expected given that the techniques have been developed to address a number of different crimes in a number of different contexts. However, the merging of the techniques, together with crime scripts, provides a systematic schema for practitioners. Such a schema could be used as a brainstorming tool for the consideration of other controls.

Table 3 : The Merger of a computer fraud script with the twenty–five Situational Crime Prevention techniques [8]

Scene function	Script action	Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
Preparation	Deliberately gaining access to organisation	Prospective employment screening (4)				
Entry	Already authorised as employee	----				
Pre-condition	Wait for employees absence from offices	Physical segregation of duties (4) Staggered breaks (4)	Signing in/out of offices (8)			
Instrumental Pre-condition	Access colleagues' computers	System time outs (2) Biometric fingerprint authentication (2)				
Instrumental Initiation	Access programmes	Password use for access to specific programmes (2)				
Instrumental Actualization	False customer account construction		Two person sign-off on new accounts (9)			
Doing	Authorisation of fictitious invoices		Audit of computer logs (8) Budget monitoring (8)			
Post Condition	Exit programmes		----			
Exit	Exit system		User event viewer (8)			
Doing Later	Spend the transferred money					

Scripts also afford consideration of the interrelationship between the security behaviour of staff, safeguards, and the criminal behaviour of dishonest employees. As employees now play a central role in enforcing security, appreciating the interplay between their behaviour and controls is of paramount importance. Password systems are a good example of how poor security behaviour (i.e. writing passwords down, sharing them with colleagues) of employees can invalidate any protection that such systems were designed to offer. The computer input fraud example also illustrates how, although the technical segregation of the system was working properly, the behaviour of fellow members of staff left the system vulnerable and open to fraud by the rogue employee. By considering the criminal behaviour at each scene, the requisite controls, and the security actions of staff, practitioners can consider more clearly their security options. One option, for example, may be to consider the introduction of redundant controls, which come into play when the original safeguard, for whatever reason, does not work properly. So, for example, the 'Instrumental Pre-condition' for the fraud involved 'accessing colleagues' computers'. As noted, staff members created vulnerabilities by failing to lock down their computers. Practitioners might therefore consider introducing the 'redundant' control of system time-outs.

Another advantage offered by crime scripts concerns the consideration of the criminal attributes required by offenders for perpetration [8]. As noted, Parker [6] argues the need to consider 'cyber-criminals' in terms of their skill, knowledge, resources, access and motives. This, however, leads to the question of how this should be achieved? Scripts offer a solution to this problem as they are able to place the offender in the criminal

context. This is important as is the context which largely dictates and defines criminal attributes. Criminologists who advocate the use of SCP techniques refer to these attributes as 'choice-structuring properties' [3]. By this, they mean those features of criminal activity which make such activity not only available, but also attractive to the offender. In the case of computer crime discussed above, the rogue employee perceived criminal activity as 'available' given his daily workings with the invoicing system and the skills and knowledge that had been acquired as a consequence. These skills and knowledge were complemented by the fact that the offender was aware of the vulnerability created through his colleagues failing to lock down their PC's. Hence practitioners could feasibly elicit the choice-structuring properties through the creation of scripts and its ability to afford consideration of the offender in the criminal context. One source of prevention might therefore stem from scrutinising the choice-structuring properties and examining methods which deny access to them. In this sense certain criminal activity would be less 'available' and 'attractive' to potential offenders.

Conclusion

While there is an obvious need for organizations to address external security threats, the problems posed by insider computer crime should not be underestimated. Unfortunately, current research and practice lack a clear understanding of how such crimes are actually perpetrated. In order to obtain such an understanding we argue strongly for the need to view computer crime from a criminological perspective. Common to every crime is the role of the offender and with recent developments in criminology, there are not only explanations as to the causes of criminality, but also how crime is committed. Hence we

have illustrated how SCP can provide insights and tools for understanding and addressing the insider threat. This criminological approach is but one of a number which examine the criminal act and provide explanations and practical knowledge about crime prevention. However, unless researchers and practitioners recognise the potential for viewing computer crime from a criminological perspective, this knowledge cannot be exploited and the benefits will be lost.

References

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

2. Cornish, D. The Procedural Analysis of Offending and its Relevance for Situational Prevention. In *Crime Prevention Studies* (Vol. 3), R. Clarke, Ed. Criminal Justice Press, New York, 1994, 151-196.

3. Cornish, D. and Clarke, R. Crime Specialisation, Crime Displacement and Rational Choice Theory. In *Criminal Behavior and the Justice System: Psychological Perspective*, H. Wegener, F. Losel, and J. Haisch, Eds. Springer-Verlag, New York, 1989, 103-117.

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

5. Deloitte 2006 Global Security Survey.

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

7. Willison, R. Understanding the Offender/Environment Dynamic for Computer Crimes. *Information Technology & People*. *19*, 2 (2006) 170-186.

8. Willison, R. Understanding the Perpetration of Employee Computer Crime in the Organisational Context. *Information and Organization*. *16*, 4 (2006) 304-324.

9. Willison, R., and Backhouse, J. Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective. *European Journal of Information Systems*. *15*, 4 (2006) 403-414.