Northumbria Research Link

Overcoming the insider: reducing employee computer crime through situational crime prevention

Information security has become increasingly important for organizations, 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. This figure may not appear high, but the impact of crime perpetrated by insiders can be profound. Donn Parker7 argues that 'cyber-criminals' should be considered in terms of their criminal attributes, which include skills, knowledge, resources, access and motives (SKRAM). It is as a consequence of such attributes, acquired within the organization, that employers can pose a major threat. Hence, employees use skills gained through their legitimate work duties for illegitimate gain. A knowledge of security vulnerabilities can be exploited, utilising resources and access are provided by companies. It may even be the case that the motive is created by the organization in the form of employee disgruntlement. These criminal attributes aid offenders in the pursuit of their criminal acts, which in the extreme can bring down an organization.

In the main, companies have addressed the insider threat through a workforce, which is made aware of its information security responsibilities and acts accordingly. Thus, security policies and complementary education and awareness programmes are now commonplace for organizations. That said, little progress has been made in understanding the insider threat from an offender's perspective. As organizations attempt to grapple with the behavior of dishonest employees, criminology potentially offers a body of knowledge for addressing this problem. It is suggested that Situational Crime Prevention (SCP), a relative newcomer to criminology, can help enhance initiatives aimed at addressing the insider threat.

In this article, we discuss how recent criminological developments that focus on the criminal act, represent a departure from traditional criminology, which examines the causes of criminality. As part of these recent developments we discuss SCP. After defining this approach, we illustrate how it can inform and enhance information security practices.

In recent years, 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. Simply to explain how people develop a criminal disposition is only half the equation. What is also required is an explanation of how crimes are perpetrated. Criminological approaches, which focus on the criminal act, would appear to offer more to information security practitioners than their dispositional counterparts. Accordingly, the SCP approach can offer additional tools for practitioners in their fight against insider computer crime.

SCP Defined

SCP embodies the implementation of opportunity reducing techniques that target specific forms of crime; impact on the immediate environment via its design, management, or manipulation; and 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.4 A number of points derive from this definition. As mentioned, SCP's focus is crime specific. Rather than discussing 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. 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 of-fender views certain crimes in an unfavourable light.

SCP also recognises 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." Attempts, therefore, 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 behavior. 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. One such example includes the use of measures designed to reduce convenience store robbery. In a bid to address this problem, a series of studies in the U.S. examined the environmental influences which could help to mitigate this type of crime.6 From these studies, it emerged that a number of measures could be introduced into the immediate context as an aid to prevention. These included ensuring two or more clerks are on duty (especially during the night shifts); good cash handling methods (such as limiting the amount of money on store, utilising time-release safes) and improving exterior visibility (involving the removal of obstructions which inhibit the ability to look into or out of the store).

With specific regard to the techniques advanced by SCP, these have developed in line with the evolution of the approach itself. Hence an original 8 were succeeded by 12, then 16, to the position whereby 25 techniques are currently proposed. Associated with the 25 techniques (see Table 1)4 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. Included in Table 1 are two types of examples. Examples from the traditional SCP application areas are cited in bold. Examples of the techniques with regard to information security are cited in italics. In terms of the emboldened techniques, examples include target hardening (such as anti-robbery screens in banks and post offices to increase the effort), strengthening formal surveillance (such as security guards to increase the risks), removing targets (such as removable car radios to reduce the rewards), avoiding disputes (such as reduce crowding in public houses to reduce provocations) and the setting of rules (such as harassment codes to re-move excuses).

Table 1: Twenty–five Techniques of situational prevention

Increase The Effort	Increase The Risks	Reduce The Rewards	Reduce Provocation	Remove Excuses
1. Target harden: • Anti-robbery screens • *Physical locks for pcs*	*6. Extend guardianship:* • "Cocoon" neighbourhood watch • *Staff chaperoning of visitors*	*11. Conceal targets:* • Gender-neutral phone directories • *Minimise ID of offices*	*16. Reduce frustrations and stress:* • Efficient queues and polite service	*21. Set rules:* • Harassment codes • *Information security policies*
2. Control access to facilities: • Entry phones • *Swipe cards for office*	*7. Assist natural surveillance:* • Improved street lighting • *Open plan offices*	*12. Remove targets:* • Removable car radios • *Clear desk and computer screens*	*17. Avoid disputes:* • Reduce crowding in pubs	*22. Post instructions:* • "No Parking"
3. Screen exits: • Export documents • *Reception desks*	*8. Reduce anonymity:* • taxi driver ids • *ID tags for staff*	*13. Identify property:* • Cattle branding • *Property marking*	*18. Reduce emotional arousal:* Controls on violent pornography	*23. Alert conscience:* • Roadside speed display boards
4. Deflect offenders: • Street closures • *Segregation of duties*	*9. Utilize place managers:* • Two clerks for convenience stores • *Management supervision*	*14. Disrupt markets:* • Monitor pawn shops	*19. Neutralise peer pressure:* • Disperse troublemakers at school	*24. Assist compliance:* • Easy library checkout • *Security education for staff*
5. Control tools/weapons: • Disabling stolen cell Phones • *Deletion of access rights for ex-employees*	*10. Strengthen formal surveillance:* • Security guards • *Intrusion detection*	*15. Deny benefits:* • Ink merchandise tags • *Encryption*	*20. Discourage imitation:* • Censor details of modus operandi • *Prompt software patching*	*25. Control drugs and alcohol:* • Alcohol-free events

Table 2: universal script example

SCENE FUNCTION	SCRIPT ACTION
Preparation	Deliberately gaining access to the organization
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 and systems
Exit	Leave offices

Applying situational crime prevention to information security

From an information security perspective, the 25 techniques can potentially be used by practitioners, when 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. As noted, in Table 1 are examples (in italics) from the information security field. Examples include controlling access to facilities (such as swipe cards for office access to increase the effort), extending guardianship (such as staff chaperoning of visitors to increase the risks), denying benefits (such as clear desk and computer screens for reducing rewards), and setting rules (such as information security policies to remove excuses).

One advantage that SCP has over existing information security approaches is that the former focuses on crime from the offender's perspective. Considerable crime prevention experience plus input from fields such as sociology and psychology, has led to the development of the 25 techniques. As illustrated in Table 1, some of the boxes currently contain no information security examples. They therefore offer potentially fruitful areas for safeguard innovation and exploitation. For example, whether or not it is feasible to develop safeguards that "reduce frustrations and stress" and "avoid disputes," remains to be seen, but at least the techniques offer a systematic basis for this consideration.

To continue with the subject of safe-guards, information security practitioners face the perennial problem of deciding which controls should be selected for addressing certain risks. Yet this 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, this group of practitioners have used crime 'scripts.' These scripts enhance an understanding of the perpetration of crime. More specifically, any crime is made up of a series of stages. Crime scripts enable the analysis of offender behavior at each of these stages and with regard to the context in which such behavior takes place. Hence a clearer understanding of offender behavior affords a clearer understanding of which safeguards to implement. The scripts approach has already been used to analyse a number of different crimes, including public transport offences, body switching (the stealing of motor vehicles for resale purposes) and cheque fraud.

For information security purposes, the development of organization specific scripts could potentially be based on input from security practitioners and other relevant parties such as departmental staff. To assist in their development the use of what is termed a 'universal script' has been proposed.[2,8,9] In essence, this form of script provides a framework that helps to distinguish between the script's stages and, subsequently, the corresponding criminal actions. Table 2 displays the universal script framework, and an illustrative example of computer crime. The example is taken from the 1998 U.K. 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 staff had vacated the office, the dishonest employee would then access all the PCs in order to process the fraud. Hence, in the first column of Table 2, under the heading Scene Function are cited the different elements of the script. Each element can be seen as a different stage in the commission process and, could, therefore, guide practitioners in identifying the corresponding criminal behavior, which is listed in Table 2 under the heading Script Action.

As the name suggests, the first element of the universal script concerns any 'Preparation' undertaken by the offender. In this instance, it is assumed that the corresponding script action involved deliberately gaining access to the organization. As a consequence, this meant that the proceeding 'Entry' stage in the universal script was achieved by the employee who was 'Already Authorized' in terms of access to the work environment. Once 'Entry' is achieved, 'Precondition' relates to the circumstances that are required prior to the actual criminal act. In the computer crime example, this involved the offender 'Waiting for employees' absence from offices.' The next three scene functions relate to the actual perpetration of the criminal act and are required to allow the main action of the script i.e. the authorization of fictitious invoices in the 'Doing' stage. Hence, be-fore this is achieved, there must be an 'Instrumental Precondition' ('Access colleagues' computers'), 'Instrumental Initiation' ('Access programmes') and 'Instrumental Actualization' ('False customer account construction'). As noted, once these stages are achieved, the 'Doing' stage ('Authorization of fictitious invoices') can occur. After this, 'Post Condition' relates to exiting the programmes and system, which in turn allows for offender to 'Exit' by leaving the offices.

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)				Information security polices (21) security education (24)
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					

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 behavior in the process can feasibly be identified. Once this is achieved the next goal is to implement the appropriate controls.

To improve the selection of safeguards, 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. The selection of safeguards is improved as the behavior of the offender has been identified through the development of a crime script. Therefore, a clearer understanding of offender behavior will lead to the identification of appropriate controls aimed at its prevention. In addition, with scripts helping to identify all the stages of the com-mission 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). Not all the techniques cited in Table 1 are incorporated in Table 3, but this is to be expected given that differ-ent crimes will require different controls for their prevention. However, the merging of the techniques, together with crime scripts, provides a systematic schema for practitioners.

Scripts also allow consideration of the interrelationship between the security behavior of staff, safeguards, and the criminal behavior of dishonest employees. As employees now play a central role in enforcing security, appreciating the interplay between their behavior and controls is of paramount importance. Password systems are a good example of how poor security behavior (such as, writing passwords down, sharing them with colleagues) of employees can invalidate any protection that such systems were designed to offer. The example of computer input fraud discussed earlier also illustrates how – even though the technical segregation of the system was working properly - the behavior of fellow members of staff left the system vulnerable and open to fraud by the rogue employee. By considering the criminal behavior 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 intro-duction of redundant controls, which come into play when the original safe-guard, for whatever reason, does not work properly. For example, the 'Instrumental Pre-condition' for the fraud involved accessing colleagues' computers. Here, 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, Parker7 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 should this 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 it 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 previously discussed, 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 by his col-leagues failing to lock down their PC's. Therefore, practitioners could feasibly identify the choice-structuring proper-ties through the creation of scripts and their 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. We have shown 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, NY, 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, NY, 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, NY, 1989, 103-117.
4.   Cornish, D., and 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, and D. Cornish, Eds, Criminal Justice Press, NY, 151-196.
5.   Deloitte 2006 Global Security Survey.
6.   Hunter, R., and Ray Jeffrey, C. Preventing convenience
store robbery through environmental design. In R.
Clarke, Ed. Situational Crime Prevention: Successful
Case Studies (2nd ed.) Harrow and Heston, NY, 1997.
7.   Parker, D. Fighting Computer Crime: A New
Framework for Protecting Information. Wiley Computer Publishing, NY, 1998.
8.   Willison, R. Understanding the perpetration of employee computer crime in the organizational 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.