Understanding the Offender/Environment Dynamic for Computer Crimes

Willison, Robert Andrew

Document Version
Final published version

Publication date:
2005

Working Paper

UNDERSTANDING THE OFFENDER/ENVIRONMENT DYNAMIC FOR COMPUTER CRIMES

By

Robert Willison

No. 04 - 2005

Institut for Informatik

Handelshøjskolen
i København

Howitzvej 60
2000 Frederiksberg

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

Department of Informatics

Copenhagen
Business School

Howitzvej 60
DK-2000 Frederiksberg
Denmark

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

UNDERSTANDING THE OFFENDER/ENVIRONMENT DYNAMIC FOR COMPUTER CRIMES

There is currently a paucity of literature focusing on the relationship between the actions of staff members, who perpetrate some form of computer abuse, and the organisational environment in which such actions take place. A greater understanding of such a relationship may complement existing security practices by possibly highlighting new areas for safeguard implementation. To help facilitate a greater understanding of the offender/environment dynamic, this paper assesses the feasibility of applying criminological theory to the IS security context. More specifically, three theories are advanced, which focus on the offender's behaviour in a criminal setting. Drawing on an account of the Barings Bank collapse, events highlighted in the case study are used to assess whether concepts central to the theories are supported by the data. It is noted that while one of the theories is to be found wanting in terms of conceptual sophistication, the case can be made for the further exploration of applying all three in the IS security context.

INTRODUCTION

There is currently little written about the relationship between the actual criminal actions of staff members, who perpetrate some form of computer abuse, and the organisational environment in which such actions take place (Willison, 2002). Insights into such a relationship may complement existing IS security practices by possibly highlighting additional areas in which safeguards could be introduced. More specifically, if insights are afforded into the actions of dishonest staff, prior to the actual perpetration of a crime, then organisations may be able to expand their preventive scope. Rather than relying solely on technical safeguards such as intrusion detection tools and password systems to help stop the commission of a computer crime, other safeguards designed to prevent criminal behaviour, prior to perpetration, would prove to be a useful addition in the preventive armoury of IS security practitioners. In an attempt to facilitate a clear understanding of the offender/environment dynamic, this paper assesses the feasibility of applying criminological theory to the IS security context. Three theories are advanced which specifically address the offender's behaviour in the criminal setting. The paper opens with a description of the criminological approaches, which include routine activity theory, environmental criminology and the rational choice perspective. This is followed by an account of the collapse of Barings Bank. Events highlighted in the account are then drawn on in the discussion and analysis section, to assess whether concepts central to the theories are supported by the data. The paper concludes by summarising the findings and discussing further research possibilities offered by the three criminological schools of thought.

CRIMINOLOGICAL THEORY AND IS SECURITY

In an attempt to provide new insights into the relationship between the criminal actions of dishonest employees and their workplace environment, criminology would appear to be a potentially fruitful body of knowledge from which to draw upon. Clarke (1997) notes how:

> Most criminological theories have been concerned with explaining why certain individuals or groups, exposed to particular psychological or social influences, or with particular inherited traits, are more likely to become involved in delinquency or crime (Clarke, 1997: 2).

However, in the last four decades, a number of like-minded theories have emerged which, rather than focusing on how people become criminals, address the actual criminal act (Clarke, 1997). Included in this group are routine activity theory, environmental criminology and the rational choice perspective. These theories focus on the relationship between the offender and the actual environment in which the crime takes place and it is for this reason that they are advanced as potentially useful schools of thought for IS security research. As a first step in assessing the feasibility of applying the theories to the IS security context, this section of the paper describes the three approaches.

Routine Activity

Routine Activity Theory is a relative newcomer to the field of criminology (Felson, 1992, 1994). Cohen and Felson (1979) discuss how changes in what they describe as 'routine activities' of society's members have impacted on the levels of direct-contact

predatory crimes, i.e. crimes where one or more persons directly take or damage the person or property of another. These activities include the provision of food, shelter, leisure, work, child-rearing, and sexual outlets. It is argued that these forms of behaviour influence direct-contact predatory crime rates by impacting on the convergence in time and space, of the three elements required for a crime to occur. These elements consist of a likely offender, a suitable target, and the absence of a capable guardian, who, if present, would be in a position to stop a criminal act. As the name suggests, the offender is the individual who may, or may not, decide to perpetrate a crime. A target may be a person or object that is attacked or taken by the offender. This might include, for instance, a man the offender wants to rob or a car he wishes to steal. What also determines a target is whether or not the entity, which forms the basis for a target, either lacks or has present, a capable guardian. Thus for example, a house where the owner is present is afforded a capable guardian. If, however, the owner is at work, the property lacks a capable guardian and consequently represents much more of a target to the potential offender. Cohen and Felson (1979) assert that it takes merely the absence of one of these three elements for a crime not to occur. Drawing on U.S.A. census data and victimisation surveys, they reveal how between 1960-1970, daytime residential burglary increased by 16%. They partly explain this rise by noting how the decade also witnessed an increase of females in the workforce and a rise in the number of individuals living along. As a consequence, there was a related rise in the number of properties left vacant and lacking a capable guardian during the working day.

Routine activity theory continues to mature (Felson, 1986). In an attempt to accommodate Hirschi's (1969) social control theory, Felson (1986) proposes the

incorporation of another element, that of the 'intimate handler', to illustrate how people can act as a 'brake' on the activities of offenders. In his book *Causes of Delinquency*, Hirschi (1969) argues that there are four factors that constitute a social bond between an individual and society. These include commitments, attachments, involvements and beliefs. Felson uses the word 'handle' to summarise the four elements. By doing so Hirschi argues that the social bond (and hence handle) is a key element in informal social control. The 'intimate handler' represents the individual who is able to exert this form of social control. The handler is normally someone who is recognised by, and has sufficient knowledge, of the potential offender. Hence the mere presence of a person known to the potential offender may act as a form of 'handling', and consequently a deterrent, by reminding the offender of their social bonds. By incorporating the concept of the handled offender and the intimate handler into routine activity theory, Felson argues that just as a target must be lacking a capable guardian for the commission of a crime, so too must the offender be lacking an intimate handler.

Furthermore, as a means of enhancing its contribution to crime prevention, Clarke (1992) advocates that routine activity theory could incorporate the category of 'crime facilitators'. These relate to items such as cars, guns, and credit cards, which act as tools for specific crimes - as well as dis-inhibitors such as alcohol, which facilitate the precipitation of crimes. Clarke (1992) argues that if we appreciate how these facilitators are used, it may be possible to identify points were safeguards can be introduced.

Environmental Criminology

Environmental criminology has provided considerable insight into the 'search' patterns of offenders and illustrated how the majority of crimes are committed within areas visited by offenders during their routine work and leisure pursuits (Brantingham and Brantingham, 1984, 1991, 1993; Bottoms and Wiles, 2002). Offenders develop an 'action space' in which these everyday pursuits take place and through such activities acquire a detailed knowledge of this environment, leading to what these authors describe as an 'awareness space'. Like the rational choice perspective, Brantingham and Brantingham (1991) argue that the motivated individual engages in a 'multi-staged decision process' prior to the commission - or not as the case may be - of a crime. Such a process is informed through knowledge gathered from the offender's awareness space. Furthermore, they argue that a specific environment emits cues relating to its spatial, cultural, legal and psychological characteristics. With experience, an offender is able to discern certain sequences and configurations of these cues associated with a 'good' target.

Rational Choice Perspective

The rational choice perspective focuses on the decision-making processes of offenders (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Clarke and Cornish, 2000). The approach assumes that crimes are chosen by the offender, as a suitable course of action, with the intention of deriving some type of benefit. 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. Of further importance to the rational choice perspective is the division of criminal choices into two groups, viz., 'involvement' and 'event' decisions. The former refers to decisions an offender makes regarding their criminal careers. The latter refers to those decisions made during the actual commission of a crime. These decisions are based on the offender's perceptions of the situation. Hence, the decision to carry out a particular criminal act emerges from a reasoning that the associated risks and efforts are outweighed by the perceived rewards. In other words, the decision to carry out a particular criminal act represents an assessment by the offender that the particular situation offers an opportunity. Given this, an opportunity can be seen as a subjective relationship between an offender and their environment.

The approach further assumes that choices are characterised by what is termed 'bounded' or 'limited' rationality. In other words, criminal decision making is at times less than perfect, as a consequence of the conditions under which decisions are made. With the associated risks and uncertainty in offending, criminals may make decisions without the knowledge of all the potential costs and benefits (i.e. the risks, efforts and rewards). Devoid of all the necessary information, offenders may resort to 'rules of thumb' when perpetrating offences, or rely on a tried and tested general approach that may be called into action when unexpected situations arise.

At first glance, the application of the aforementioned theories to the IS security context may appear ill-suited, but as Baskerville (1994) notes:

> We should consider human (social) aspects as well as the technological security of computer-based information. It is this broad 'systems management' view that is poorly researched yet critical to the development of safe organizational information resources (Baskerville, 1994, p. 385).

This message is echoed by Dhillon and Backhouse (2001), who argue that the majority of IS security writings are essentially technocratic in nature. Early risk analysis and security evaluation approaches, followed by more recent evaluation and design methods, are founded on functionalist conceptions influenced traditionally by systems theory. These tools and techniques have a limited scope, primarily focusing on issues of managing access control. The Achilles' heel of these safeguards is their conception of reality. Given how much of the early work on security was developed by the US military, it is perhaps not surprising that these safeguards were based on, and reflect, the reality that exists in a military environment. Organisational structures which mimic this environment, that is, which are hierarchical and with centralised information processing, may accommodate such tools and techniques. But as Dhillon and Backhouse note:

> … problems arise when organisational structures become flatter and more organism like in their nature. When this happens a broader vision for addressing security concerns is needed which address social grouping and the behaviour of people.
>
> (Dhillon & Backhouse, 2001, p. 145)

Hence the devolution of computing power within, and between, organisations has led to the need for every member of an organisation to be responsible for security. Such devolution, however, has obviously led to more people having access to computers. The vast majority of organisational staff will use these resources for purely legitimate reasons, but a small minority will use them for illegal gain. If we subscribe to Dhillon and Backhouse's (2001) argument that 'a broader vision for addressing security concerns is needed which address social grouping and the behaviour of people', should we be attempting to understand not only how people are central to the enforcement of security, but also how they attempt to overcome it through criminal behaviour in the organisational setting?

The following section describes the major factors that led to the collapse of Barings bank. This case study is used as a basis for assessing the feasibility of applying the three criminological theories to the IS security context.

CASE STUDY: THE COLLAPSE OF BARINGS BANK

On the 26th February 1995, administrators were appointed by the High Court in London (UK) to manage the affairs of Baring Plc. following the identification of substantial losses incurred by a related overseas subsidiary known as Baring Futures Singapore. This section of the paper provides an account of the major factors that were instrumental in the collapse of Barings. The purpose of the account is two fold. First the reader is afforded an understanding of the collapse. Secondly, data drawn from this case study is then used in the 'Discussion and Analysis' section to assess

whether events highlighted in the account support concepts, which are central to the three criminological theories. Two points should be noted here. First, given the limitations on space, the account is simplified, highlighting areas most obviously covered by the theories. Secondly, the account is based on the Bank of England: *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings* (BoBS, 1995) and Stephen Fay's *The Collapse of Barings* (Fay, 1996)

Brief History and Background of Barings Bank

Prior to its collapse, Baring Brothers & Co. had been the oldest merchant bank in the City's square mile. Founded initially as a partnership in 1762, the bank had managed to remain independent and privately controlled. After a near fatal business venture in Argentina, Baring Brothers & Co. was established in 1890 to succeed the partnership. In 1985 the share capital of Baring Brothers & Co. was acquired by Barings plc, which became the parent company of the Barings Group. Apart from Baring Brothers & Co., the other two principal operating companies of Barings plc were Baring Securities Limited and Baring Asset Management, which played no part in the collapse (and hence will not be referred to again in this account). Baring Securities Limited had commenced business in 1984, specialising in Far East Securities. The company expanded rapidly. In the first five years of trading, Baring Securities Limited opened nineteen subsidiary offices. Aside from the traditional business activities carried out by Baring Brothers & Co., Baring Securities Limited represented Barings first involvement in the securities business.

Creation and Management of Baring Futures Singapore

Baring Futures Singapore was one of the new offices that opened during the expansion of Baring Securities Limited, and was formed to specialise in exchange-traded futures and options (i.e. these were Baring Futures Singapore's bank products). More precisely, Baring Futures Singapore would execute client business on the Singaporean Stock Exchange (SIMEX) on behalf of Baring Securities Limited and Baring Securities Japan. This client business, also referred to as 'agency' business, was managed by Mike Killian (Head of Global Equity Futures and Options Sales) in Tokyo. Baring Futures Singapore would accumulate profits through commission charged to clients.

Nick Leeson, a pivotal figure in the collapse of Barings, was asked by Killian to apply for the post of settlements manager. Leeson had acquired the necessary experience through working in the settlement's section of a Baring Securities Limited department, which specialised in Japanese futures and options. He accepted the offer, and his name, once submitted to the Management Committee, was approved.

Previously in 1987, Baring Securities had opened their first Singaporean office in the form of Baring Securities Singapore. The managing director of Baring Securities Singapore was James Bax. He oversaw a business which traded equities (but not derivatives) on SIMEX. Bax's second-in-command was Simon Jones, who acted as the Chief Operating Officer of Baring Securities Singapore. This position included responsibility for the back office, which settled Baring Securities Singapore's equity trading.

Leeson moved to Singapore in early March 1992. Initial problems in the management of Baring Futures Singapore were created shortly afterwards, by the actions of Ian Martin (Baring Securities Limited's Finance Director). Despite the fact that Mike Killian had asked Leeson to run the back office (i.e., the settlements section) of Baring Futures Singapore, Martin instructed Jones and Killian that Leeson would be in charge of the front and back offices. By so doing, Martin was breaching one of the golden rules of management, which states that there should be a strict segregation of duties between trading and settlement.

The supervisory failings with regard to Barings Futures Singapore were compounded by the actions of Jones and Bax, who took little interest in the new subsidiary, despite the fact that both were, on paper at least, responsible for Leeson at a regional level.

Mike Killian further rejected the idea that there was a reporting line between himself and Leeson. Yet this runs contrary to what Leeson argues, who cites Killian as one of the people who managed him in 1992. Hence from the very start of Leeson's employment at Baring Futures Singapore, there was considerable confusion over two key areas: first, what his job responsibilities were, and secondly, who managed him.

In early 1993 Leeson started trading on SIMEX in conjunction with Baring Securities Japan's Tokyo traders who (since the collapse of the Japanese stock market in 1990) made their money through a type of trading called 'arbitrage', otherwise known as 'switching'. This section of Baring's business was known as equity derivatives. Unlike Killian's business, the trading undertaken by the Baring Securities Japan

traders and Leeson was conducted solely to make profits for Barings and not clients, and can therefore be classified as proprietary trading. The manager in charge of the switching business was Fernado Gueller, based in Japan.

When Peter Norris became CEO of Baring Securities Limited in March 1993, one of his first decisions was to make the Financial Products Group of Baring Brothers & Co. responsible for the equity derivatives business (i.e., switching). The actual hand-over of this business did not take place until late 1993. The manager in charge of the Financial Products Group was Ron Baker.

Unauthorised Trading Activities Conducted by Baring Futures Singapore

Leeson was engaged in substantial unauthorised trading on SIMEX through the taking of proprietary positions in futures and options. This section addresses the trading through a brief examination of the history of the account (88888) used to book and record the deals.

Account 88888

Unauthorised trading of futures commenced very shortly after the opening of 88888 and carried on until the collapse in late February of 1995. This trading went largely unnoticed for almost two years and eight months. The only capacity in which Baring Futures Singapore was authorised to transact options was with regard to agency trading. However, in October 1992 Leeson started to sell options, and continued to do so until 23rd February, 1995.

At the year-end 1992, losses incurred through the unauthorised trading were relatively minor, standing at £2 million. One year later, they had grown to £23 million, and by 31st December 1994, the figure amounted to £208 million. In the space of the following three months, however, this figure had almost quadrupled to a staggering £827 million.

Failure of Internal Controls

The ability of Leeson to establish substantial unauthorised trading positions on SIMEX was afforded by failures in the management, financial, and operating controls in Barings. In addition, these failures were evident in Singapore, Tokyo, and London and included the following areas:

- Failures in the managerial supervision of Leeson.
- Lack of segregation between the front and back offices of Baring Futures Singapore.
- Insufficient action taken by Barings management in response to warning signals.
- No risk management or compliance function in Singapore.
- Weak financial and operational control over the activities and funding of Baring Futures Singapore at Group level.

DISCUSSION AND ANALYSIS

In attempting to assess the feasibility of applying the three criminological theories to the IS security context, this section of the paper examines whether events highlighted in the case study support those concepts which are central to the theories.

Routine Activity Theory:

Intimate Handler/Unhandled Offender

With regard to the managerial supervision of Leeson, there is some overlap here with the theoretical concepts of the intimate handler and the handled offender. The fact that, on the whole, there was an absence of an intimate handler in the form of senior management, provided Leeson with the freedom to undertake his unauthorised trading.

However, there is a divergence between theory and data with regard to how supervision is actually enacted. With regard to the intimate handler, their presence is enough to act as a deterrent. But it was not just the mere physical absence of a manager, which aided Leeson in perpetrating his criminal activities. When Leeson was afforded some supervision, the evidence suggests that the management problem was compounded by the fact that Bax, Jones and Ron Baker (who was later responsible for managing Leeson at a product level) had very little understanding of the products (futures and options) he dealt in and the trading processes which underpinned this business. In this sense, supervision could not be executed properly owing to the ignorance of managers regarding the nature of business undertaken by Leeson and not, in the case of intimate handlers, owing to their absence.

Targets

The Barings case, highlights a possible variation on the targets concept inscribed in the model. Although there is no hard evidence to suggest it, the obvious assumption would be that Leeson carried out the unauthorised trading for personal financial gain. Hence the ‘target’ in this sense would have been the ability to undertake the

unauthorised trading, while the benefits represented monies derived from the unsanctioned business. However, in his book *The Collapse of Barings*, Fay (1996) argues that behind Leeson's illegal activities was the desire to become one of the elite traders on the floor of SIMEX. Leeson got to know some of these traders owing to the fact that the companies they worked for (First Continental Trading and Spear, Leeds and Kellogg) used Baring Futures Singapore for clearing their trades with SIMEX. Admiring the status and prestige associated with the elite brokers, Fay argues that Leeson was keen to emulate their activities and establish himself as a name on the trading floor. To do this, however, rather than taking the conventional route, Leeson carried out the unauthorised trading, creating fantastic 'profits' through dumping losses in account 88888.

In this sense, the benefit derived from trading was not the obvious one of money, but rather the benefits of prestige and status that were afforded the top traders. What the two benefits have in common is the nature of the target, which was the ability to undertake unauthorised trading. Although 'ability' has a comparatively intangible nature, it can still be viewed as consistent with routine activity theory, which views a target as one of the elements necessary for the commission of a crime. The data not only supports this proposition but, if we subscribe to Fay's (1996) argument, it can be seen to support the rational choice perspective, by illustrating how the 'benefits' of crime can come in many guises. In Leeson's case, as noted, his benefits were prestige and status.

Guardianship Factors

Compared with traditional applications, the issue of guardianship is far more complex when discussing the collapse of Barings. Indeed, a number of safeguard factors can provide guardianship in the banking environment, such as internal/external audit, compliance monitoring, risk management and the like. To some extent, these guardianship factors can be perceived as still in keeping with routine activity theory, given that their presence or absence would play a part in determining whether an entity represents a viable target.

However, it should be noted that the elements that are considered guardianship factors in the Barings case are of a far more complex nature than those traditionally recognised by routine activity theory. More specifically, *a priori* conditions need to be met before they can exist. Take for instance Baring Securities Limited's internal audit group. A management committee would have decided on its establishment, the size of the group, and the positions that would need to be created. The employment vacancies would be advertised, people interviewed and selected. Obviously, only after its inception could arrangements have been made for the group to carry out audits in Baring Securities Limited's various subsidiaries.

Of course, even if guardianship factors like the internal audit group are introduced into the banking context, there is no guarantee that their mere existence will provide effective guardianship over the target they purport to safeguard. Rather they have to exist and be working effectively. This last assertion can be seen as a slight departure from routine activity theory, which asserts that the existence of a capable guardian would deter a crime.

Facilitators

Clarke (1995) depicts facilitators as coming from the physical environment. However, the internal threat posed by staff, and the organisational environment in which they work, places a different spin on the concept. As Willison (2000) asserts:

> More interesting perhaps is the idea that potential offenders acquire facilitators in the course of their work. Unlike their physical counterparts, these facilitators are cognitive in nature, and … are assimilated by staff the day they begin working for a particular company.
> (Willison, 2000, pp. 104 -105)

Essentially these cognitive facilitators include those skills and knowledge that a person acquires to perform their jobs. A key point here is that, although on the whole these skills are used by employees for perfectly legal activities, they can also be used to help facilitate activities of an illegal nature. Perhaps not surprisingly, the BoBS report highlights numerous instances of Leeson using his skills in this manner. Indeed, all his criminal activities were underpinned by knowledge initially acquired to support legitimate work. This is clearly revealed by the very fact that the report makes the distinction between authorised and unauthorised trading.

Environmental Criminology

Search Patterns of Offenders

Data from the case study appears to support this depiction of a potential offender as an individual who collates information from their awareness space and uses it for

criminal purposes. Leeson's 'awareness space' encompassed the offices he routinely worked in. These included not only Baring Futures Singapore and SIMEX, but also Baring Securities Limited (London) where he had worked prior to moving to the Far East. While performing his day-to-day duties, Leeson was able to note any weak links in the control environment.

Prior to the commencement of the unauthorised trading, Leeson opened account 88888 to help conceal his aberrant activities. He knew from his time in London, that as with other accounts, the trading details of account 88888 would be sent by Baring Futures Singapore to London in the form of four reports, which included a trade file, which gave details of the day's trading activity; a price file, which reported on closing settlements price; a margin file, listing the initial – and maintenance – margin details of each account; and the London gross file, which provided details of BFS's trading position. In order to stop details of account 88888 reaching London, Leeson instructed Dr. Edmund Wong, a computer consultant, to omit details of the account from three of the four daily trading reports. The exception was the margin file. Leeson was aware that the margin file represented a security vulnerability for Baring Securities Limited, simply because it was routinely ignored by staff in London. Conversely, for Leeson, the margin file represented no risk with regard to helping to uncover his unauthorised trading, given the oversight by staff in London. As a consequence, he was able to ignore it.

Of key importance here is the fact that Leeson worked for Barings. This represents a slight departure from the offender's circumstance traditionally found in the studies of environmental criminology. For example, Brantingham and Brantingham (1991) cite

the work of Dufala (1976) whose study addresses convenience store robberies in Tallahassee, Florida. Dufala reports how, for marketing purposes, the stores were situated near major roads. As a consequence, these stores also formed part of the awareness space of offenders who, like many other urban residents, lived nearby. Leeson's position, however, would be more comparable to that of a clerk in one of the shops. Hence, learning his trade and developing knowledge of his target took place in the same context.

A related point concerns the quality of information that the offender is able to garner. Although an offender's rationality is addressed in the next section of this chapter, the concept of bounded rationality ties in nicely with the offender's circumstance. Unlike the convenience store robbers studied by Dufala (1976), Leeson had access to a relatively high quality of information, which enabled him to assess more accurately potential risks, efforts and rewards. Access to such information was primarily due to the fact that he worked for Barings. His employment first with Baring Securities Limited and then Baring Futures Singapore also provided Leeson with both the necessary time and locations to collate the relevant information.

The Rational Choice Perspective

There is considerable evidence in the Barings case to support the rational choice perspective. Prior to the commencement of the unauthorised trading, Leeson clearly planned and executed actions that afforded the necessary conditions to initiate the unsanctioned business. One example concerns the manipulation of funding from London. When Leeson first started work at Baring Futures Singapore, he informed Gordon Bowser (Head of Futures and Options Settlements in London) that owing to

the manner in which SIMEX made margin calls (margin is a form of deposit which is paid when derivatives are traded), it would be difficult for Baring Futures Singapore to raise in time the appropriate monies to meet the requests. Leeson argued that it would be far easier if the funds could be advanced from London prior to the margin calls. What Bowser did not know was that the 'problem' of meeting SIMEX margin calls was pure fiction on Leeson's behalf. Unfortunately, Bowser believed him and agreed to the request. This meant that Leeson could call for funds from London without specifying the trading account to which the request related. Through his careful planning, Leeson had gained a 'safe' source of funding. The reconciliation between accounts and funding would have proved a useful safeguard, but by succeeding in gaining advanced funds prior to margin calls, Leeson knew this safeguard would be negated.

During the commission of the fraud, Leeson continued to demonstrate the actions of a rational offender. When losses began to accrue as a result of his unauthorised trading, these were placed in account 88888. In order to hide these losses, and in order to avoid detection, Leeson created false journal entries, generated fictitious transactions and sold a large number of options. From early 1993 he masked the month end balance of the account by making a journal adjustment, crediting 88888 with a sum which would leave the balance at zero. He would then make an additional journal adjustment by debiting the same amount to the SIMEX clearing bank account maintained by Baring Futures Singapore. After the month end reconciliation, the transaction was simply reversed. Although this technique was used on numerous occasions to hide the balance of account 88888, another method involved the selling of options. Leeson would simply take the premiums collected through the sale of

options, and offset this amount against the losses residing in 88888. In effect, he was in a position to manipulate his environment to reduce the risk of his fraud being uncovered.

CONCLUSION

This section concludes the paper by summarising the major findings of the discussion and analysis section and advances future research possibilities offered by the criminological theories.

Routine Activity Theory

Of the three approaches, routine activity theory appears to offer the least with regard to IS security. The concept of 'handling' can be seen to lack the necessary sophistication to theoretically accommodate and explain the supervisory failings in Barings. This lack of conceptual sophistication is further evident when discussing the issue of guardianship. A determining factor in the utility of both concepts is the complexity of the crime to which they are applied. Routine activity when first advocated restricted its application to 'direct contact predatory crimes' i.e. where one or more persons directly take or damage the person or property of another. This is a far cry from unauthorised trading on SIMEX. However, when discussing the usefulness of the aforementioned concepts, the issue of granularity should be introduced into the debate. The Barings case is extremely detailed, encompassing many individuals and organisations, and as noted the handling and guardianship

concepts find it difficult to accommodate such complexity. That said the concepts might prove more fruitful when applied to less complex cases of computer abuse.

The concept of targets is likewise drawn from routine activity theory. Traditionally, examples of this concept take a physical form, including cars to steal, banks to rob and houses to burgle. Although the target in the Barings case proved to be the ability to undertake trading, and hence represents a departure from its physical counterparts, this is still consistent with routine activity's theoretical proposition, which views a target as one of the elements necessary for the commission of a crime.

The final major input from routine activity relates to facilitators. While acknowledging the tangible nature of some facilitators, the case study supports the idea of intangible cognitive facilitators. Indeed, any understanding of computer crime must be able to account for and consider how cognitive facilitators are used for the commission of such crimes. In this sense, the facilitators concept is easily translated into the field of IS security.

Environmental Criminology

Like facilitators, the theoretical concepts of environmental criminology are easily translated into the IS security field. The Barings case provides supporting evidence, illustrating how knowledge of security provisions was used by Leeson to his advantage. The search patterns of offenders, married with cognitive facilitators, provide a useful theoretical grounding in understanding how a rogue employee combines knowledge of the environment with the skills acquired through work to perpetrate a fraud.

Rational Choice Perspective

Data from the case study further supports the idea of a rational offender. Leeson clearly planned and executed actions that allowed him to initiate his unauthorised trading. During the period in which his aberrant trading took place, he continued to demonstrate the actions of a rational offender. When losses accrued as a result of the trading, not only did Leeson place them in a specially designated account (88888), he also instigated actions to hide the losses and avoid detection.

Future Research

Given these findings, future research could involve the application of the theories to cases less complex in nature than Barings. Individual incidents of computer abuse would provide complementary findings for assessing the feasibility of applying the three theories to the IS security context. Routine Activity theory, in particular, may offer more fruitful findings when applied to less complex cases.

In addition, complementary criminological concepts could be imported to reinforce the use of the theories, and help to develop more informed prevention strategies. For example, the rational choice perspective underpins another criminological approach entitled Situational Crime Prevention (SCP). The latter aims to reduce the opportunities for crime by implementing measures into the environment, which a) target specific forms of crime; b) impact on the immediate environment via its design, management, or manipulation; c) aims to either increase the effort and risk of crime, or to render these less rewarding or excusable. SCP advocates a total of sixteen opportunity reducing techniques, which are divided equally among the four attendant

aims. Hence there are four techniques to either, increase effort, increase risk, reduce rewards or remove excuses for crime. Example of these techniques include the *controlling of facilitators* (e.g. gun control: to increase the effort), *entry/exit screening* (baggage screening: to increase the risks), *target removal* (e.g. removable car radios: to reduce the rewards), and *rule-setting* (e.g. harassment codes: to remove excuses), (Clarke, 1997).

What distinguishes the sixteen opportunity reducing techniques from traditional IS security controls is how (through the rational choice perspective) they are underpinned by a theoretical conceptualisation of the offender. Thus the controls are based on a conceptualisation of the offender as a rational decision maker. This theoretical underpinning is quite rare in IS security. Even the BS ISO/IEC 17799: 2000 (BS 7799-1:2000) Information Technology – Code of Practice for Information Security Management is based not on theoretical input, but rather best practice principles. The perception of a criminal based on the rational choice perspective could therefore be adopted by the IS security field, thereby providing a sound theoretical model of the offender. Such a move could be complemented by the possible incorporation of the opportunity-reducing techniques advanced by SCP.

Crime 'scripts' (Cornish, 1994a, 1994b) is another example of a complementary criminological method which could possibly reinforce the application of the three theories. While the rational choice perspective examines offender 'event' decisions, crime scripts can help to elaborate on the commission process during which such decisions are made. As the name suggests, the concept compares a crime to a theatrical script. The method helps to break down a crime into individual, but related,

stages or ‘scenes’. Each identifiable stage allows for consideration of the specific context, ‘props’, the actions of the offender and their choices which underpin such actions. In conjunction with the rational choice perspective, the scripts concept can give a greater understanding of the procedural stages of a specific crime. Once this is achieved, security strategies can pinpoint controls to influence the decision-making process of the offender. As a complement to this process, the sixteen opportunity reducing techniques advanced by SCP could then be considered when addressing safeguard implementation.

A related and final point concerns the relationship between IS security and theory. One aim of this paper is to illustrate how the fertilisation generated by criminological theories when applied to IS can provide new perspectives and insights, leading to possible advancements in understanding the offender/context dynamic. Rather than relying on technical safeguards, a complementary approach would be to cultivate an understanding of the offender in their environment, and by so doing, identify potentially new areas for safeguard implementation. One of the general deficiencies of IS security is the lack of theory both used and advocated by academics in the field. The position taken in this paper is that in order to understand computer crime and computer criminals, the academic discipline, which can potentially offer substantial insight into this area is criminology. Given the multi-disciplined nature of criminology, drawing on subject which include psychology, sociology, law, social policy and economics, it can be seen to offer a voluminous body of knowledge which IS security academics can use. Failure to adopt appropriate theory for appropriate problems will deny the potential for new perspectives and insights. Criminology, for example, is a case in point. Although rarely used in IS security research, where better

to find insight into crime and criminals than from a field of study which examines precisely that?

BIBLIOGRAPHY

Baskerville, R. (1994) Research Directions in Information Systems Security. *International Journal of Information Management*, Vol 14 No 5, 385-387.

Board of Banking Supervision (1995) *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings*. HMSO. London.

Bottoms, A. and Wiles, P. (2002) Environmental Criminology. In M. Maguire, R. Morgan and R. Reiner (eds.), *The Oxford Handbook of Criminology* (3rd ed.). Oxford University Press. Oxford.

Brantingham, P. and Brantingham, P. (1984) *Patterns in Crime*. Macmillan. London.

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

Brantingham, P. and Brantingham, P. (1993) Environment, Routine and Situation: Toward a Pattern Theory of Crime. In R. Clarke and M. Felson (eds.), *Routine Activity and Rational Choice*, (Advances in Criminological Theory, vol. 5). Transaction Press. New Brunswick, NJ.

Burrell, G. and Morgan, G. (1979) *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*. Heinemann. London.

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

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

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

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

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

Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends : A Routine Activity Approach. *American Sociological Review*, Vol 44 No 4, pp 588-608.

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

Statistical Analysis Center, Florida Criminal Justice Executive Institute, Florida Department of Law Enforcement.

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

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

Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Toward Socio-Organisational Perspectives. *Information Systems Journal*, Vol 11 No 2, pp. 127-153.

Dufala, D. (1976) Convenience Stores: Armed Robbery and Physical Environmental Features. *American Behavioral Scientist*, Vol 20, pp. 227-246.

Fay, S. (1996) *The Collapse of Barings*. Richard Cohen Books. London.

Felson, M. (1986) Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes. In D. Cornish and R. Cornish (eds.*), The Reasoning Criminal : Rational Choice Perspectives on Offending*. New York. Springer-Verlag.

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

Felson, M. (1994) *Crime and Everyday Life: Insight and Implications for Society*. Pine Forge Press. Thousand Oaks, CA

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

Willison, R. (2000) Reducing Computer Fraud Through Situational Crime Prevention. In S. Qing and J. H.P. Eloff (eds.), *Information Security for Global Information Infrastructures*. Kluwer Academic Press. Boston.

Willison, R. (2002) *Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank.* PhD thesis. London School of Economics and Political Science.