Criminology of Computer Crime

Sarah Lowman

May 2010

1 Introduction

With the huge growth in computer connectivity and usage over the last decade there has never been such a wealth of opportunity for prospective criminals. While motives tend not to change, the variety and number of opportunities for cyber crime are constantly growing (Grabosky, 2000). Given the increase in computer and internet-based crime, it is surprising to note that "*there have been very few attempts to develop and apply criminological theories to the concept of digital crime*" (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006).

Criminology is the scientific study of crime, criminal behaviour and law enforcement. It draws from many different areas, including psychology, sociology and law. This paper will be split into two parts, each of which will explore an important aspect of criminology as it relates to computer crime. The first part will focus on offender profiling, and the second will describe several of the key criminological, psychological and social theories that try to explain criminal behaviour. It is impossible to stereotype every computer criminal, just as it is difficult to compare serial killers to petty thieves. Therefore, this paper will look in detail at just one type of computer criminal – the insider employee, for convenience hereafter referred to as *insider criminals* or *insiders*.

Offender profiling is a controversial area, with many opposing views, and profiling insiders is no different. For example, whilst some claim insider criminals display several common characteristics (Shaw, Ruby, & Post, 1998), some studies have shown insiders *"did not share a common profile, were not necessarily problem employees, and showed considerable variability in their range of technical knowledge*" (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). The first part of this paper will discuss some of the opposing opinions, describe the different types of inside attacks and attackers, and highlight possible ways of detecting and preventing insider attacks.

There are many different criminological theories. Two classic ones are *rational choice* and *routine activity*. Rational choice theory states that committing a crime is a rational choice made because the benefits outweigh the potential negative consequences. Routine activity stems from rational choice and states that crime is normal and inevitable. In contrast, psychological theories explore how *moral development* and *personality disorders* affect criminal behaviour. Social theories look at how society (especially class) may affect crime; the most prominent example is *strain theory*, which asserts that criminality stems from a lack of opportunity to meet social expectations. This paper will explain these differing schools of thought and relate them to insider crime.

2 Insider Crime

The difficulty starts with the definition of an insider. Schultz defines insiders as "*employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth*" (Schultz E. , 2002), but Pfleeger also includes "*a former insider, now using previously conferred access credentials not revoked when the insider status ended or using access credentials secretly created while an insider to give access later*" (Pfleeger, 2007). These definitions make it difficult to pinpoint personalities, behaviours and motives associated with insider crime as their scope is so wide, essentially covering everybody associated with an organisation. For the purposes of this essay, an insider will be a current technical employee of a business company. An 'insider attack' can be defined as "*the intentional misuse of computer systems by users who are authorized to access those systems and networks*" (Schultz & Shumway, 2001).

Insider attacks accounted for an estimated loss of $170 million in 2002 for theft of proprietary information such as customer and product databases and R&D data (Nykodym, Taylor, & Vilela, 2005)[1] and it has been claimed that 60% to 70% of all computer crime directed toward companies is committed by insiders (Demers, 2001). Although a lot of research papers tend to agree that insider crime is more prevalent than outsider crime, others directly oppose this. Schultz argues that this "myth" is attributed to old data: when computers were clunky and few and far between, the internet didn't exist as it does today and the number of people with the technical ability to produce outside attacks was small (Schultz E. , 2002). It is difficult to get realistic statistics on insider attacks. This may be due to under-reporting of the crimes because

[1] Although they do not give their definition of insider criminals or an insider attack, making it difficult to relate this number to the definition used in this paper.

companies fear negative publicity or because the resulting damage was too small to warrant criminal charges (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). Insider attacks are also much harder to spot than external security breaches: since the employee already has the authorisation to access the data or systems, the theft of business data may go unnoticed for a long time or never be detected. What seems to be generally agreed is that insider attacks are more successful than outsider attacks, and pose a much larger risk.

The risk to companies is vast – the financial loss can be devastating. The American firm Ellery Systems became insolvent in 1994 when a Chinese employee transferred the company's entire proprietary source code to another company in China. The foreign competition drove Ellery Systems to bankruptcy. The FBI dropped the case against the employee in question due to insufficient evidence (Magnan, 2000). Publicity about insider criminality can also damage an organisation's reputation (Cappelli, Moore, Shimeall, & Trzeciak, 2006) and result in increased liability.

3 Offender Profiling

Offender profiling (also known as *criminal profiling*, *criminological profiling*, *behavioural profiling* or *criminal investigative analysis*) is an important part of criminology which tries to identify the perpetrator of a crime based on the nature of the offence and the style in which it was committed. Profiling can also provide ways to detect and prevent criminal behaviour, however many profiling techniques have been criticized for being too stereotypical or too broad (Rogers, 2003). Established techniques and profiles exist for non-computer related crimes such as serial killers (Hickey, 2009) and terrorists (Charlesworth, 2003); however there has been growing interest in profiles for computer crime (Pfleeger, 2007). Areas which suit profiling include hacking (Hollinger, 1991), child pornography (Krone, 2004), software copyright infringement (Hinduja, 2003), cyber stalking (Wood & Wood, 2002) and insider employee computer crime (Nykodym, Taylor, & Vilela, 2005) to name a few. The profiling of insider computer crime is a relatively new field and numerous theories and frameworks exist, many of which directly contradict each other.

3.1 Type of Attacks and Attackers

Nykodym, Taylor and Vilela divide insider crime into four categories: *espionage*, *theft*, *sabotage*, and *personal abuse of the organizational network* (Nykodym, Taylor, & Vilela, 2005). The fourth category includes time-wasting from surfing the internet and online gambling, and is by far the

most common 'crime'. Clearly, this category is not a criminal offense like the other three, but can result in disciplinary action against the employee. A further categorisation divides theft into two subcategories: theft for financial gain (*fraud*) and *theft of intellectual property for [their own] business advantage* (Trzeciak, Moore, Cappelli, Caron, & Shaw, 2009).

3.1.1 Spies and Saboteurs

Although there is a lot of overlap between espionage and theft, theft is for personal use whilst espionage is when an insider is employed by a competitor to obtain confidential information. Spies usually must be placed high in the organisation, possibly as a manager or senior manager, to have access to secret information. For this reason, spies tend to be older, perhaps in their 50s. Spies also have a tendency to be very secretive and careful and try and blend in as much as possible (Nykodym, Taylor, & Vilela, 2005).

Saboteurs fall into two categories: those who, like spies, are hired by another company to commit sabotage, and those who have a personal vendetta against their employer. Saboteurs (if within the company) tend to be younger employees, generally between 25 and 40, that have enough experience to understand how the computer systems work, but do not yet have a high management position (Nykodym, Taylor, & Vilela, 2005).

A study of those who commit insider espionage and sabotage revealed some common personal predispositions such as "*maladaptive reactions to stress, financial and personal needs leading to personal conflicts and rule violations, chronic disgruntlement, strong reactions to organizational sanctions, concealment of rule violations, and a propensity for escalation during work-related conflicts*" (Band, Cappelli, Fischer, Moore, Shaw, & Trzeciak, 2006). Their personal needs include a need for ego satisfaction, power over other people, attention or self-esteem reinforcement, money to feed gambling or alcoholism and an angry desire for revenge. The study observed two factors that escalated malicious thoughts or troubling behaviour into crime: 1) sanctions directed at the offender which intensified the desire for revenge and 2) the perception that the rewards of committing the crime were greater than the consequences if caught. The triggers that caused the attack were usually stressful events such as interpersonal conflicts between staff or termination of employment (Shaw & Fischer, 2005).

Saboteurs are more likely to have previous history of rule violations, but not have any concerning mental health issues, whilst spies are more likely to have mental health issues and money problems (Band, Cappelli, Fischer, Moore, Shaw, & Trzeciak, 2006).

3.1.2 Thieves

The thieves who steal for monetary gain tend to show very strong age-related patterns. Criminals stealing less than $100,000 tend to be male or female, 20 – 25 years old and be low in the organisational hierarchy. Criminals embezzling between $100,000 and $1million tend to be 25 – 30 year old males, and above $1 million tend to be over 35, male and in management (Nykodym, Taylor, & Vilela, 2005). The older and higher up in the chain of command the attacker is, the more they tend to steal because they are confident and comfortable in their position. 51% of attackers in an embezzlement survey had been employed for 11 or more years at the company, and most attackers did not have a criminal record nor any drug problems (Solarz, 1987). Their crimes are not driven by hate or revenge like spies or saboteurs, but by greed.

Those who steal intellectual property (IP) may also want money, but these criminals generally have longer term ambitions such as "*stealing the information to get a new job, to succeed in a new job with a competing business, to start a competing business, or to give the stolen data to a foreign government or organization*" (Trzeciak, Moore, Cappelli, Caron, & Shaw, 2009). Trzecciak, Moore, Cappelli, Caron and Shaw's case studies indicated a strong sense of entitlement – with nearly 75% justifying their actions by claiming they had contributed to or signed an agreement regarding the stolen IP. The sense of entitlement was especially acute when the insider perceived their role to be crucial to the firm. A lack of loyalty to the company played a large role, with dissatisfaction contributing to 39% of the case study cases.

3.2 Schultz Detection Framework

Although the above profiles give useful insight, all of the information is based on retrospective studies and the authors do not provide guidelines for helping detect and pre-empt insider crimes. There are many detection frameworks available that are intended to help with this by providing a set of employee-related warning signs. Schultz proposes a six point detection framework to identify any suspicious behaviour, particularly for those who have a technical background. These can be weighted and turned into a probability to assess the likelihood of an employee committing a crime (Schultz E. , 2002). The six points are: deliberate markers, meaningful errors, preparatory behaviour, correlated usage patterns, verbal behaviour and personality traits.

Attackers sometimes leave deliberate 'markers' to make statements. Markers can vary in size or obviousness, and can be unrelated to the final crime. Unsigned passive aggressive notes or flooding their manager's mail from anonymous sources are examples (Schultz E. , 2002).

Attackers can make mistakes and may leave behind evidence in error logs even if they have tried to delete other logs files, especially if they are doing something that is outside their normal technical role. These errors might provide clues to what the attacker has done or will do. Therefore, effort should be put into analysing error files (Schultz E. , 2002).

In a 2005 case study of insider attacks in the financial sector, it was observed that most of the attacks were planned in advance (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). The planning included "*stealing administrative level passwords, copying information from a home computer onto the organization's system, and approaching a former co-worker for help in changing financial data*" (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). Schultz also notes preparatory behaviour to be key in detecting attacks, and so more importance should be given to investigating any unusual commands carried out on system servers (Schultz E. , 2002)

Correlated usage patterns are any patterns that are found on multiple machines. These patterns are not noticeable on just one machine, but may reveal the intentions of an attacker when discovered across several machines (Schultz E. , 2002). For example using a search command on several machines to find a particular file could show intent to steal it.

Changes in verbal behaviour, such as an employee becoming more aggressive and angry, can provide indications that an attack is imminent (Schultz E. , 2002). This could include hostile emails, or asking for elevated privileges to systems or data.

Finally, Schultz suggests that there are many specific personalities associated with those more likely to commit insider crime (Schultz E. , 2002). These include "*computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical 'flexibility', a mixed sense of loyalty, entitlement, and lack of empathy"* (Shaw, Ruby, & Post, 1998). Other studies have also shown a correlation between computer dependency and cyber crime (Nykodym, Ariss, & Kurtz, 2008). Hackers and those who steal intellectual property may have ethical 'flexibility', often believing that if electronic data is not held sufficiently secure or is freely distributable then it is fair game. This seems to be a growing view amongst the younger generation, which may have an impact on new and future employees (Hollinger, 1991).

The view that future attackers have common personality traits is controversial, and there are studies that seem to contradict it. A 2005 study (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005) revealed that only 19% of insider criminals were perceived by others as "disgruntled employees". It also found that insiders came from a variety of different racial and ethnic backgrounds and had a wide range of family situations, with 54% single and 31% married. Interestingly, 27% had prior arrests (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005), which contradicts Solarz's work (mentioned earlier) on insider embezzlement (Solarz, 1987).

The Schultz framework can be used in conjunction with many other frameworks, including the Insider Threat Prediction Model (Magklaras & Furnell, 2001), which categorises employees as either harmless, suspicious, potential accidental threat or possible intentional threat. Those who are a 'potential accidental threat' show signs that they may commit computer misuse accidentally; those who are a 'possible intentional threat' show signs that they may initiate an attack at some point, and those who are 'suspicious' show some indeterminate evidence of suspicious activities.

3.3 Prevention

Although organisations can use a variety of profiling frameworks to help detect any suspicious activity, many organisations lack even basic prevention techniques that can stop many planned or opportunistic attacks. A lot of employees freely share their usernames and passwords, creating easy ways for attackers to gain access (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). Ensuring an organisational culture of security awareness and vigilance would not only help prevent this, but may additionally make attackers think twice before committing a crime.

Psychological screening before employees are hired may be an extreme step, but could be useful for jobs that require a high level of trust and access to important company data (Pfleeger, 2007). Equally, doing criminal checks would filter out those with a history of cybercrime or crimes against previous employers. However, without careful application, both of these procedures may have adverse effects, increasing the length of the interview process and giving the impression that the organisation is controlling and oppressive.

4 Theories of Crime

4.1 Criminological Theories

Rational choice theory was developed in the 1970s when the idea that there are exact crime-producing traits and factors which can be found and treated began to wane. Over a hundred years had been spent trying to find these crime-producing traits with little success, and new theories began to emerge to try and understand why people commit crimes. Rational choice theory argues that the offender makes a rational choice to commit the offence, and has weighed up the benefits of the crime against the cost of being caught and punished; therefore, to prevent crime, more emphasis should be put on punishment as a deterrent. American laws such as the "three strikes and you're out" are based on choice theory (Keel, 2005). With certain forms of crime, the offender's 'background factors' seem to have little influence on the rational choices the offender makes. These background factors include upbringing, education, social class and ethnicity (Cornish & Clarke, 1986).

Rational choice theory says that at each step during the commission of an insider crime, a choice is made about whether to continue. The attacker has to weigh up the benefits of the next step with the punishment if they are caught. Therefore, crimes could be prevented by working out the choices that need to be made at each stage and eliminating them or by making the punishments more severe (Willison, 2006b). A general problem is that the benefits of committing insider crime do seem to outweigh the punishments. For small crimes, the attacker may just be fired or a civil suit may follow, but no criminal record will be obtained. For criminal cases, most would be tried in the UK under the Computer Misuse Act 1990, which has a maximum prison sentence of 10 years, only recently changed from 5 years (Police and Justice Act, 2006). However it is quite rare for companies to prosecute, since this means publicly admitting the security breach. Large and prominent companies (especially those who deal with money, computers or security) will want to uphold their public image and reputation (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005).

Routine Activities theory is based on the Rational Choice theory and was developed by Lawrence Cohen and Marcus Felson (Cohen & Felson, 1979). They state crime is normal, and just requires opportunity. For example, they attribute a rise in petty theft to the simple fact that there is now more available to steal. They say crime occurs when three things converge: the offender must be motivated, there must be a suitable target and there must be the absence of a

capable guardian. A capable guardian either protects the target, or is the guardian of the offender (for example, a parent or teacher).

The absence of a guardian is usually the turning point for the offender as those who are motivated to commit crime will always find suitable targets. For insider crime, the guardian is unlikely to be the electronic protection mechanisms shielding the target, such as passwords and access rights, since insiders often *already* have the necessary access rights. The guardian in this case is likely to be their manager. According to the theory, if there is an absence of that manager, then there is freedom to undertake the insider crime. The absence of the employee's manager can refer to physical absence and the employee being left alone to work, or that the manager does not understand what the employee does and so is incapable of monitoring their actions (Willison, 2006a).

4.2 Psychological Theories

The psychological theory of Moral Development was developed by Lawrence Kohlberg, and assumes that individuals develop their moral reasoning in a series of sequential stages while growing up. The reasons for believing what is right and wrong are different at each stage until they settle during early adulthood (Kohlberg & Lickona, 1976). He reasoned that criminals frequently stop their moral development earlier than non-criminals. For example, a criminal may stay in stage 2, "hedonistic orientation stage" – when right and wrong correspond to one's own needs – rather than moving to stage 3, "interpersonal concordance stage" – when what is right and wrong are based on concern for others.

A lot of insider crime described earlier involves sabotage or stealing for personal gain and involves a sense of entitlement. These selfish crimes can be easily explained by the Moral Development theory. However, the ethics surrounding intellectual property is not as clear cut: many people may be at a conventional stage of moral development, yet still have difficulty with the notion that ideas they developed can be 'owned' by an organisation.

Psychologists argue that certain personality disorders may influence crime. These include antisocial personality disorder, which is characterised by impulsivity, aggressiveness, recklessness, lack of remorse and repeated unethical or antisocial acts. Certain insiders may exhibit such traits, however "*the prevalence of antisocial personality disorder is lower among computer criminals than among other criminals*" (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006) since computer criminals tend to commit non-violent crime.

4.3 Sociological Theories

Sociological theories focus on social structure and why certain social classes or cultures are more likely to commit certain types of crime. A major social structure theory is Strain Theory. Strain Theory, which is also known as Blocked Opportunity Theory, states that everyone has goals given to them by society, but not everyone has equal opportunities to reach those goals. Some of the goals may be material wealth, education and an occupation. Those from lower classes may have less access to education and good jobs, so they are under *strain.*

One of the key Strain Theorists, Robert Merton, developed five modes of adaptation to strain: conformity, ritualism, innovation, retreatism and rebellion (Merton, 1968). A conformist accepts the cultural goals and accepts the institutionalised means to obtain them. A conformist is highly unlikely to commit any criminal acts. A ritualist rejects the cultural goals, but accepts the institutionalised means – i.e. they lower their aspirations, but still follow a normal path. Ritualists are also unlikely to commit any crimes. Innovators accept the goals, but not the normal way of getting them. Innovators may turn to crime to achieve their goals. Retreatists reject both the goals and the means to obtain them. They do not aspire to be successful, and do not really care about society's traditional goals. Retreatists may become criminals to support drug or drinking habits, but do not aspire to be financially successful. Finally, rebels reject the cultural goals and means and replace them with new goals and means. These new goals are often criminal and this adaptation is often taken on by gangs and cults.

Money laundering and corporate espionage fit neatly into the Strain Theory school of criminology – suggesting "*that crime and deviance is largely the result of blocked legitimate opportunities*" (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006), and these criminals are all 'innovators'. Whilst Merton used blocked opportunities to explain crime in the lower classes, there is relative deprivation experienced in the middle and upper classes. These people already have a certain degree of wealth and societal success, but engage in insider crime because they perceive a goal blockage to gaining further success via normal routes (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006).

5 Conclusions

Criminology is a large subject with many important areas. This essay picked several interesting criminological theories and related them to insider crime. Even within this limited scope, there

is much to say and there are many ideas that have not been covered. These include victimology – the study of victims of crime – and penology – the study of how societies repress criminal behaviour.

In terms of offender profiling, there is disagreement on what an 'insider' is, with a lot of authors using such a broad definition that it is difficult to develop a common profile. It is unclear whether a common profile even exists for insider criminals. There is also much contradictory evidence, with one study showing that almost all insider criminals were first time offenders whilst another found that a quarter had criminal records. There are detection and prevention techniques available, and by following security guidelines and being vigilant about picking up clues from potentially disgruntled employees, a lot of crimes can probably be prevented.

The main criminological theory discussed, Rational Choice, states that crime happens because the benefits of committing a crime outweigh the potential consequences. An offender has to make a rational choice by weighing the costs and benefits of their actions. The benefits of insider crime can seem high as it may appear there is little chance of being caught. Also, companies are often unwilling to press charges so they do not damage their reputations. The theory suggests that to prevent insider crimes, much heftier deterrents must be in place – something that is slowly happening with the increase of maximum prison sentences in the Computer Misuse Act.

All the criminological, psychological and social theories discussed here are well established, and many were proposed before computers were even considered as targets or accessories to crimes. Although the theories can be adjusted to fit, there aren't any criminological theories purposely crafted for computer crime and "*little theoretical development has occurred in the area of digital crime*" (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006). It is perhaps this reason why there is so much disagreement in the papers relating to insider crime, as this is a new field in criminology, and common ground has yet to be established.

Bibliography

Band, S., Cappelli, D., Fischer, L., Moore, A., Shaw, E., & Trzeciak, R. (2006). Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. *Software Engineering Institute Technical Report CMU/SEI-2006-TR-026, Carnegie Mellon University* .

Cappelli, D. M., Moore, A. P., Shimeall, T., & Trzeciak, R. (2006). Common sense guide to prevention and detection of insider threats. *Institute and CyLab of Carnegie Mellon University* , pp. 1-43.

CBSNews. (2003, September 18th). *Poll: Young Say File Sharing OK.* Retrieved from CBS News: http://www.cbsnews.com/stories/2003/09/18/opinion/polls/main573990.shtml

Charlesworth, W. R. (2003). Profiling Terrorists: A taxonomy of evolutionary, developmental and situational causes of a terrorist act. *Defense & Security Analysis. Volume 19. Issue 3* , pp. 241-264.

Cohen, L. E., & 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. B., & Clarke, R. V. (1986). Reasoning Criminal - Rational Choice Perspectives on Offending.

Demers, M. E. (2001). Prioritizing Internet Security. *Electronic News (North America). Volume 47. Issue 4* , pp. 46.

Grabosky, P. (2000). Computer crime: A criminological overview. *Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* Vienna: Citeseer.

Hickey, E. W. (2009). *Serial Murderers and their Victims.* Wadworth; International ed edition.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology. Volume 5. Issue 1* , pp. 49-61.

Hollinger, R. (1991). Hackers: computer heroes or electronic highwaymen? *ACM SIGCAS Computers and Society. Vol 21. Issue 1.* , pp. 6–17.

Keel, R. O. (2005). Rational Choice and Deterrence Theory. *Sociology of Deviant Behavior* .

Kohlberg, L., & Lickona, T. (1976). Moral stages and moralization: The cognitive-developmental approach. *Moral Development and Behavior: Theory, Research and Social Issues* .

Krone, T. (2004). A Typology of Online Child Pornography Offending. *Australian Institute of Criminology: Trends & Issues in crime and criminal justice. Number 279* .

Magklaras, G., & Furnell, S. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security. Volume 21. Issue 1* , pp. 62-73.

Magnan, S. W. (2000). *Safeguarding Information Operations*. Retrieved April 23rd, 2010, from CIA: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art08.html

Merton, R. K. (1968). Social Theory and Social Structure .

Nykodym, N., Ariss, S., & Kurtz, K. (2008). Computer Addiction and Cyber Crime. *Journal of Leadership, Accountability and Ethics* .

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer law & security report. Volume 21* , pp. 408-414.

Pfleeger, C. (2007). Reflections on the Insider Threat. *Insider Attack and Cyber Security* .

Police and Justice Act. (2006). Retrieved from http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060048_en.pdf

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D. M., & Moore, A. P. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. *TECHNICAL REPORT CMU/SEI-2004-TR-021* .

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security* , pp. 292-298.

Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security* , pp. 526-531.

Schultz, E., & Shumway, R. (2001). *Incident response: a strategic guide to handling system and network security breaches.* Indianapolis: Sams.

Shaw, E., & Fischer, L. (2005). Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders Analysis and Observations. *DEFENSE PERSONNEL SECURITY RESEARCH CENTER* .

Shaw, E., Ruby, K. G., & Post, J. M. (1998). The Insider Threat to Information Systems. *Security Awareness Bulletin. Issue 2* , pp. 170–186.

Solarz, A. (1987). Computer-related embezzlement. *Computers & Security. Volume 6. Issue 1* , pp. 49–53.

Taylor, R., Caeti, T., Loper, K., Fritsch, E., & Liederbach, J. (2006). Digital crime and digital terrorism: Chapter 3 - The Criminology of Computer Crime. Pearson/Prentice Hall.

Trzeciak, R., Moore, A. P., Cappelli, D. M., Caron, T. C., & Shaw, E. (2009). Insider Theft of Intellectual Property for Business Advantage: A Preliminary. *1st International Workshop on Managing Insider Security Threats* (pp. PP. 1-22). West Lafayette: Purdue University.

Willison, R. (2006a). Understanding the offender/environment dynamic for computer crimes. *Information Technology & People. Vol 19. Issue 2.* , pp.170–186.

Willison, R. (2006b). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization. Vol 16. Issue 4.* , pp. 304-324.

Wood, R. A., & Wood, N. L. (2002). Stalking the Stalker: A Profile of Offenders. *FBI Law Enforcement Bulletin. Volume 71. Issue 12* , pp. 1-12.