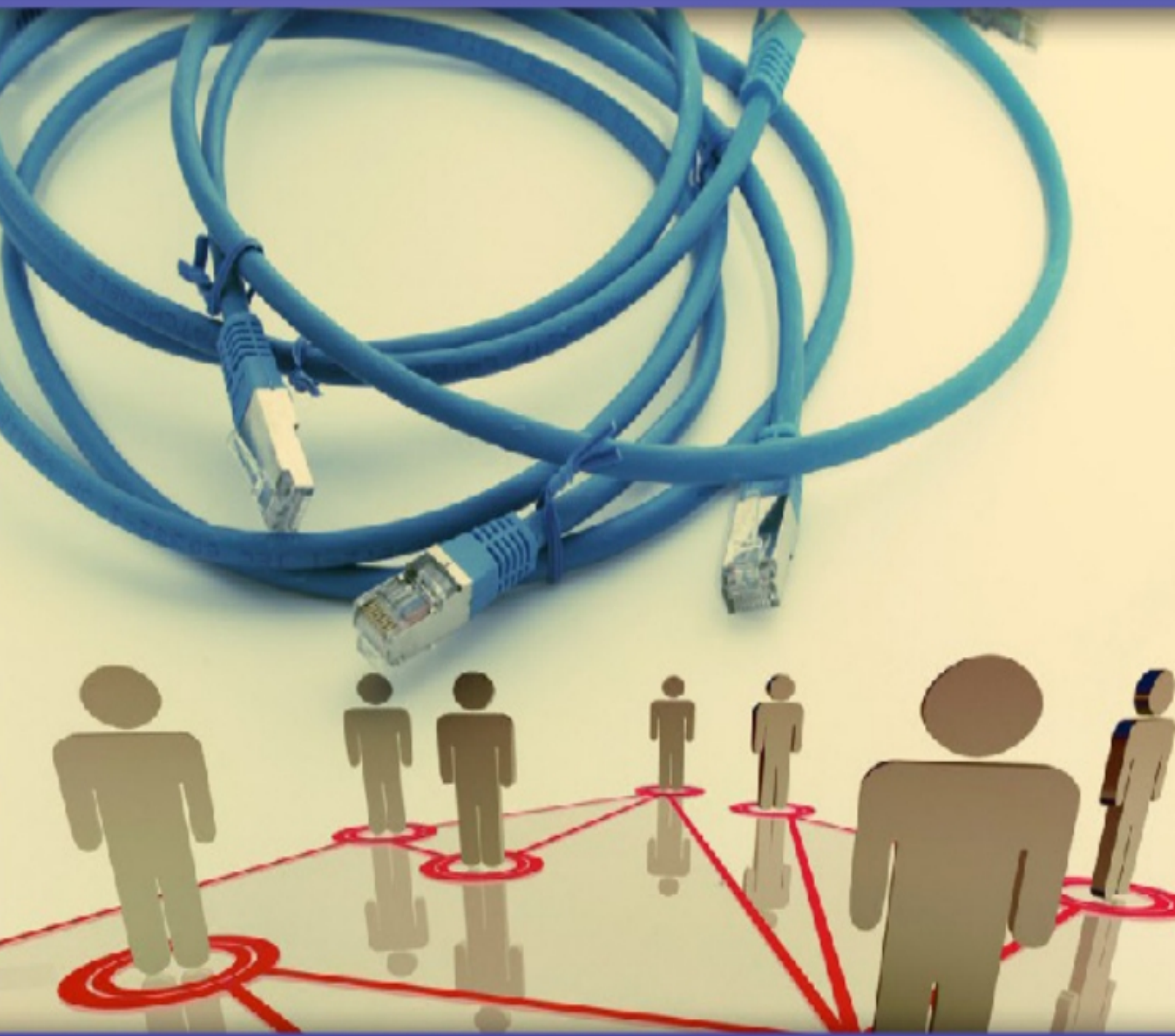
Petter Gottschalk

Policing Cyber Crime



Petter Gottschalk

Policing Cyber Crime

Policing Cyber Crime

ISBN 978-87-7681-679-7

Contents

Introduction

The risk of computer crime has become a global issue affecting almost all countries. Salifu (2008) argues that the Internet is a "double-edged sword" providing many opportunities for individuals and organizations to develop and prosper, but at the same time has brought with it new opportunities to commit crime. For example, Nigeria-related financial crime is extensive and 122 out of 138 countries at an Interpol meeting complained about Nigerian involvement in financial fraud in their countries. The most notorious type attempted daily on office workers all over the world, is the so-called advance fee fraud. The sender will seek to involve the recipient in a scheme to earn millions of dollars if the recipient pays an advance fee (Ampratwum, 2009).

Computer crime is an overwhelming problem worldwide. It has brought an array of new crime activities and actors and, consequently, a series of new challenges in the fight against this new threat (Picard, 2009). Policing computer crime is a knowledge-intensive challenge indeed because of the innovative aspect of many kinds of computer crime.

Cyberspace presents a challenging new frontier for criminology, police science, law enforcement and policing. Virtual reality and computer-mediated communications challenge the traditional discourse of criminology and police work, introducing new forms of deviance, crime, and social control. Since the 1990s, academics and practitioners have observed how cyberspace has emerged as a new field of criminal activity. Cyberspace is changing the nature and scope of offending and victimization. A new discipline named cyber criminology is emerging. Jaishankar (2007) defines cyber criminology as the study of causation of crimes that occur in the cyberspace and its impact in the physical space.

1. Cyber Crime Defined

Employees of the organization commit most computer crime, and the crime occurs inside company walls (Hagen et al., 2008: Nykodym et al, 2005). However, in our perspective of financial crime introduced in this chapter, we will define computer crime as a profit-oriented crime rather than a damage-oriented crime, thereby excluding the traditional focus of dissatisfied and frustrated employees wanting to harm their own employers.

1.1 Computer Crime Technology

Computer crime is defined as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution (Laudon and Laudon, 2010). The initial role of information and communication technology was to improve the efficiency and effectiveness of organizations. However, the quest of efficiency and effectiveness serves more obscure goals as fraudsters exploit the electronic dimension for personal profits. Computer crime is an overwhelming problem that has brought an array of new crime types (Picard, 2009). Examples of computer-related crimes include sabotage, software piracy, and stealing personal data (Pickett and Pickett, 2002).

In computer crime terminology, the term cracker is typically used to denote a hacker with a criminal intent. No one knows the magnitude of the computer crime problem – how many systems are invaded, how many people engage in the practice, or the total economic damage. According to Laudon and Laudon (2010), the most economically damaging kinds of computer crime are denial-of-service attacks, where customer orders might be rerouted to another supplier.

Eleven men in five countries carried out one of the worst data thefts for credit card fraud ever (Laudon and Laudon, 2010: 326):

> In early August 2008, U.S. federal prosecutors charged 11 men in five countries, including the United States, Ukraine, and China, with stealing more than 41 million credit and debit card numbers. This is now the biggest known theft of credit card numbers in history. The thieves focused on major retail chains such as OfficeMax, Barnes & Noble, BJ's Wholesale Club, the Sports Authority, and T.J. Marxx.
>
> The thieves drove around and scanned the wireless networks of these retailers to identify network vulnerabilities and then installed sniffer programs obtained from overseas collaborators. The sniffer programs tapped into the retailers' networks for processing credit cards, intercepting customers' debit and credit card numbers and PINs (personal identification numbers). The thieves then sent that information to computers in the Ukraine, Latvia, and the United States. They sold the credit card numbers online and imprinted other stolen numbers on the magnetic stripes of blank cards so they could withdraw thousands of dollars from ATM machines. Albert Gonzales of Miami was identified as a principal organizer of the ring.

The conspirators began their largest theft in July 2005, when they identified a vulnerable network at a Marshall's department store in Miami and used it to install a sniffer program on the computers of the chain's parent company, TJX. They were able to access the central TJX database, which stored customer transactions for T.J. Marxx, Marshalls, HomeGoods, and A.J. Wright stores in the United States and Puerto Rico, and for Winners and HomeSense stores in Canada. Fifteen months later, TJX reported that the intruders had stolen records with up to 45 million credit and debit card numbers.

TJX was still using the old Wired Equivalent Privacy (WEP) encryption system, which is relatively easy for hackers to crack. Other companies had switched to the more secure Wi-Fi Protected Access (WPA) standard with more complex encryption, but TJX did not make the change. An auditor later found that TJX had also neglected to install firewalls and data encryption on many of the computers using the wireless network, and did not properly install another layer of security software it had purchased. TJX acknowledged in a Securities and Exchange Commission filing that it transmitted credit card data to banks without encryption, violating credit card company guidelines.

Computer crime, often used synonymous with cyber crime, refers to any crime that involves a computer and a network, where the computer has played a part in the commission of a crime. Internet crime, as the third crime label, refers to criminal exploitation of the Internet. In our perspective of profit-oriented crime, crime is facilitated by computer networks or devices, where the primary target is not computer networks and devices, but rather independent of the computer network or device.

1.2 Computer Crime on the Internet

Cyber crime is a term used for attacks on the cyber security infrastructure of business organizations that can have several goals. One goal pursued by criminals is to gain unauthorized access to the target's sensitive information. Most businesses are vitally dependent on their proprietary information, including new product information, employment records, price lists and sales figures. According to Gallaher et al. (2008), an attacker may derive direct economic benefits from gaining access to and/or selling such information, or may inflict damage on an organization by impacting upon it. Once access has been attained, attackers can not only extract and use or sell confidential information, they can also modify or delete sensitive information, resulting in significant consequences for their targets.

Cyber crime is any crime committed over a computer network. Cyber crime is not limited to outside attacks. The most common type of cyber criminals, according to Nykodym et al. (2005), is occurring within their own walls. However, most of these crime types are innocent and petty. Examples include reading newspapers online, following sporting events while at work, or gambling online. Most of the perpetrators are between 30 and 35 years old. Some of the crime types are serious, for example theft. Persons over 35 years do the most damage.

Cyber crime and computer crime are both related to Internet crime. The Internet is a “double-edged sword” that provides many opportunities for individuals and organizations to develop. At the same time, the Internet has brought with it new opportunities to commit crime. Salifu (2008) argues that Internet crime has become a global issue that requires full cooperation and participation of both developing and developed countries at the international level.

Click fraud occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its product. Click fraud has become a serious problem at Google and other web sites that feature pay-per-click online advertising. Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor’s ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking (Pickett and Pickett, 2002).

1.3 Financial Computer Crime

In this book, computer crime is classified as financial crime (Fletcher, 2007). Financial crime can be defined as crime against property, involving the unlawful conversion of property belonging to another to one’s own personal use and benefit. Financial crime is sometimes labeled economic crime (Larsson, 2006). Financial crime is profit-driven crime to gain access to and control over property that belonged to someone else. Pickett and Pickett (2002) define financial crime as the use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities. They use the terms financial crime, white-collar crime, and fraud interchangeably.

The term financial crime expresses different concepts depending on the jurisdiction and the context. Nevertheless, Henning (2009) argues that financial crime generally describes a variety of crimes against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit, more often than not involving fraud but also bribery, corruption, money laundering, embezzlement, insider trading, tax violations, cyber attacks and the like. Criminal gain for personal benefit seems to be one of the core characteristics of financial crime.

Financial crime often involves fraud. Financial crime is carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud, and health care fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering. Embezzlement and theft of labor union property and falsification of union records used to facilitate or conceal such larcenies remain the most frequently prosecuted Labor-Management Reporting and Disclosure Act offences in the US (Toner, 2009).

Financial crime sometimes, but not always, involves criminal acts such as elder abuse, armed robbery, burglary, and even murder. Victims range from individuals to institutions, corporations, governments and entire economies.

Interpol (2009) argues that financial and high-tech crimes – currency counterfeiting, money laundering, intellectual property crime, payment card fraud, computer virus attacks and cyber-terrorism, for example – can affect all levels of society.

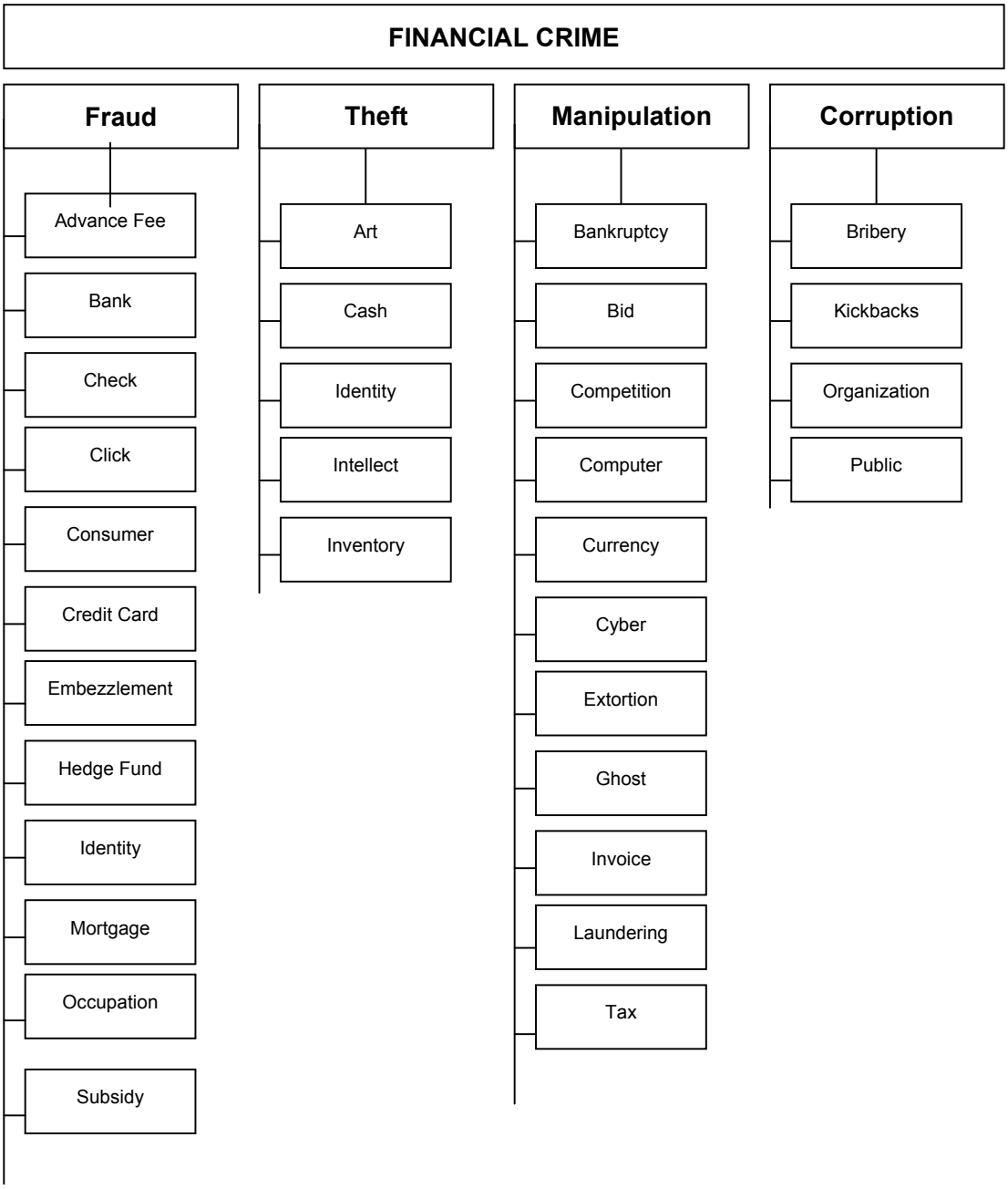


Figure 1. Main categories and sub categories of financial crime

We find a great variety of criminal activities that can be classified as financial crime. Figure 1 illustrates a structure among financial crime categories defined as main categories and sub categories of financial crime. The four main categories are labeled corruption, fraud, theft, and manipulation respectively. Within each main category there are a number of subcategories.

In Figure 1, computer crime is classified as a sub category of manipulation as a main category. Manipulation can be defined as a means of gaining illegal control or influence over others' activities, means and results. In addition to this direct kind of computer crime, we find indirect forms of computer crime, where computer technology is an important element of the crime. We have already mentioned examples such as identity fraud; click fraud, and credit card fraud that can be found under the main category of fraud in Figure 1.

By defining computer crime as financial crime and sometimes even as white-collar crime, as discussed below, we focus on the profit-orientation of such crime. This definition excludes incidents of computer crime to cause damage without a gain. Even if malware infection, hacking and other incidents are frequently reported in the popular press (Hagen et al., 2008), these kinds of computer crime are only of interest here if they have a profit motive. Computer crime is here profit-driven crime to gain access to and control over property that belonged to someone else.

Profit-driven crime by criminals should be understood mainly in economic rather than sociological or criminological terms. In an attempt to formulate a general *theory of profit-driven crime*, Naylor (2003) proposed a typology that shifts the focus from actors to actions by distinguishing between market crime, predatory crime, and commercial crime. The theory of profit-driven crime for white-collar crime suggests that financial crimes are opportunity driven, where executives and managers identify opportunities for illegal gain. Opportunity is a flexible characteristic of financial crime and varies depending on the type of criminals involved (Michel, 2008).

1.4 White-Collar Computer Crime

Computer crime can occur within white-collar crime, which is a special domain of financial crime. White-collar crime can be defined in terms of the offense, the offender or both. If white-collar crime is defined in terms of the offense, it means crime against property for personal or organizational gain. It is a property crime committed by non-physical means and by concealment or deception (Benson and Simpson, 2009). If white-collar crime is defined in terms of the offender, it means crime committed by upper class members of society for personal or organizational gain. It is individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organizations (Hansen, 2009).

If white-collar crime is defined in terms of both perspectives, white-collar crime has the following characteristics:

- White-collar crime is crime against property for personal or organizational gain, which is committed by non-physical means and by concealment or deception. It is deceitful, it is intentional, it breaches trust, and it involves losses.

- White-collar criminals are individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organization. They are persons of respectability and high social status who commit crime in the course of their occupation.

The most economically disadvantaged members of society are not the only ones committing crime. Members of the privileged socioeconomic class are also engaged in criminal behavior. The types of crime may differ from those of the lower classes, such as lawyers helping criminal clients launder their money, executives bribe public officials to achieve public contracts, or accountants manipulating balance sheet to avoid taxes. Another important difference between the two offenders is that the elite criminal is much less likely to be apprehended or punished due to his or her social status (Brightman, 2009).

Edwin Sutherland introduced the concept of "white-collar" crime in 1939. According to Brightman (2009), Sutherland's theory was controversial, particularly since many of the academicians in the audience fancied themselves as member so the upper echelon of American society. Despite his critics, Sutherland's theory of white-collar criminality served as the catalyst for an area of research that continues today.

In contrast to Sutherland, Brightman (2009) differs slightly regarding the definition of white-collar crime. While societal status may still determine access to wealth and property, he argues that the term white-collar crime should be broader in scope and include virtually any non-violent act committed for financial gain, regardless of one's social status. For example, access to technology, such as personal computers and the Internet, now allows individuals from all social classes to buy and sell stocks or engage in similar activities that were once the bastion of the financial elite.

Salifu (2008) provides support for our perspective of computer crime as profit-oriented crime, financial crime and sometimes even white-collar crime by arguing that economic reason lies at the heart of Internet crime. While there can be a number of motives, such as power, lust, revenge, adventure and the desire to check illegal boundaries and the likelihood of being caught, the most obvious motive is greed and profit. Far more computer crime is motivated by greed and the prospect of financial gain than any other motive.

White-collar crime represents a serious threat to corporate reputation. Nevertheless, there are surprisingly many corporations that are involved in white-collar crime. For example in Sweden, Alalehto (2010) found that 40 percent of the top-ranked corporations in the Swedish business world have been involved in white-collar crime in the last decade. These corporations had decisions against them, such as court decisions, administrative law, objection, or settlement.

1.5 Crime Offender or Victim

Most studies seem to apply the victim perspective of computer crime (Hagen et al., 2008). This perspective implies that an individual, a group, an organization or a society is the victim of crime. In this book, we will apply the offender perspective as well. The offender perspective implies that an individual, a group, an organization or a society is the criminal responsible for computer crime.

In the victim perspective, a survey revealed that next to malware infection and theft of IT equipment, hacking was the most commonly reported computer crime incident. The findings of Hagen et al. (2008) document that computer crime cause extra work for the victim and loss of earnings as well. Several of the reported crime incidents in their study could be countered by improved access control and data protection measures in addition to awareness raising activities. Their survey revealed that there are large differences in security practices between large and small enterprises, even when it comes to measures one might have thought that all enterprises independent of size would have implemented.

2. Cyber Crime Cases

2.1 Fake Websites

Fake websites have become increasingly pervasive and trustworthy in their appearance, generating billions of dollars in fraudulent revenue at the expense of unsuspecting Internet users. Abbasi et al. (2010) found that the growth in profitable fake websites is attributable to several factors, including their authentic appearance, a lack of user awareness regarding them, and the ability of fraudsters to undermine many existing mechanisms for protecting against them. The design and appearance of these websites makes it difficult for users to manually identify them as fake. Distinctions can be made between spoof sites and concocted sites. A spoof site is an imitation of an existing commercial website such as eBay or PayPal. A concocted site is a deceptive website attempting to create the impression of a legitimate, unique and trustworthy entity.

Detecting fake websites is difficult. There is a need for both fraud cues as well as problem-specific knowledge. Fraud cues are important design elements of fake websites that may serve as indicators of their lack of authenticity. First, fake websites often use automatic content generation techniques to mass-produce fake web pages. Next, fraud cues include information, navigation, and visual design. Information in terms of web page text often contains fraud cues stemming from information design elements. Navigation in terms of linkage information and URL names for a website can provide relevant fraud cues relating to navigation design characteristics. For example, it is argued that 70 percent of ".biz" domain pages are fake sites. Fake websites frequently use images from existing legitimate or prior fake websites. For example spoof sites copy company logos from the websites they are mimicking. The fact that it is copied can be detected in the system (Abbasi et al., 2010).

In addition to fraud cues, there is a need for problem-specific knowledge. Problem-specific knowledge regarding the unique properties of fake websites includes stylistic similarities and content duplication (Abbasi et al., 2010).

Abbasi et al. (2010) developed a prototype system for fake website detection. The system is based on statistical learning theory. Statistical learning theory is a computational learning theory that attempts to explain the learning process from a statistical point of view. The researchers conducted a series of experiments, comparing the prototype system against several existing fake website detection systems on a test sample encompassing 900 websites. The results indicate that systems grounded in statistical learning theory can more accurately detect various categories of fake websites by utilizing richer sets of fraud cues in combination with problem-specific knowledge.

A variation of fake websites is fraudulent email solicitation where the sender of an email claims an association with known and reputable corporations or organizational entities. For example, one email from the "Microsoft/AOL Award Team" notified its winners of a sweepstake by stating, "The prestigious Microsoft and AOL has set out and successfully organized a Sweepstakes marking the end of year anniversary we rolled out over 100,000.000.00 for our new year Anniversary Draw" (Nhan et al., 2009). The email proceeded to ask for the potential victim's personal information.

Nhan et al. (2009) examined 476 fraudulent email solicitations, and found that the three most frequently alleged organizational associations were Microsoft, America Online, and PayPal. Fraudsters also attempt to establish trust through associating with credit-issuing financial corporations and authoritative organizations and groups.

2.2 Money Laundering

Money laundering is an important activity for most criminal activity (Abramova, 2007; Council of Europe, 2007; Elvins, 2003). Money laundering means the securing of the proceeds of a criminal act. The proceeds must be integrated into the legal economy before the perpetrators can use it. The purpose of laundering is to make it appear as if the proceeds were acquired legally, as well as disguises its illegal origins (Financial Intelligence Unit, 2008). Money laundering takes place within all types of profit-motivated crime, such as embezzlement, fraud, misappropriation, corruption, robbery, distribution of narcotic drugs and trafficking in human beings (Økokrim, 2008).

Money laundering has often been characterized as a three-stage process that requires (1) moving the funds from direct association with the crime, (2) disguising the trail to foil pursuit, and (3) making them available to the criminal once again with their occupational and geographic origins hidden from view. The first stage is the most risky one for the criminals, since money from crime is introduced into the financial system. Stage 1 is often called the placement stage. Stage 2 is often called the layering stage, in which money is moved in order to disguise or remove direct links to the offence committed. The money may be channeled through several transactions, which could involve a number of accounts, financial institutions, companies and funs as well as the use of professionals such as lawyers, brokers and consultants as intermediaries. Stage 3 is often called the integration stage, where a legitimate basis for asset origin has been created. The money is made available to the criminal and can be used freely for private consumption, luxury purchases, real estate investment or investment in legal businesses.

Money laundering has also been described as a five-stage process: placement, layering, integration, justification, and embedding (Stedje, 2004).

It has also been suggested that money laundering falls outside of the category of financial crime. Since money-laundering activities may use the same financial system that is used for the perpetration of core financial crime, its overlap with the latter is apparent (Stedje, 2004).

According to Joyce (2005), criminal money is frequently removed from the country in which the crime occurred to be cycled through the international payment system to obscure any audit trail. The third stage of money laundering is done in different ways. For example, a credit card might be issued by offshore banks, casino 'winning' can be cashed out, capital gains on option and stock trading might occur, and real estate sale might cause profit.

The proceeds of criminal acts could be generated from organized crime such as drug trafficking, people smuggling, people trafficking, proceeds from robberies or money acquired by embezzlement, tax evasion, fraud, abuse of company structures, insider trading or corruption. The Financial Intelligence Unit (2008) in Norway argues that most criminal acts are motivated by profit. When crime generates significant proceeds, the perpetrators need to find a way to control the assets without attracting attention to them selves or the offence committed. Thus, the money laundering process is decisive in order to enjoy the proceeds without arousing suspicion.

The proceeds of crime find their ways into different sectors of the economy. A survey in Canada indicates that deposit institutions are the single largest recipient, having being identified in 114 of the 149 proceeds of crime (POC) cases (Schneider, 2004). While the insurance sector was implicated in almost 65 percent of all cases, in the vast majority the offender did not explicitly seek out the insurance sector as a laundering device. Instead, because motor vehicles, homes, companies, and marine vessels were purchased with the proceeds of crime, it was often necessary to purchase insurance for these assets.

When banks are implicated in money laundering, the computer crime is carried out in terms of financial transactions. Proceeds of crime are deposited in the bank and then transferred in such a way that trails are disguised before the money is made available to the criminal again. While it may harm a bank's reputation if it is disclosed that it handles criminal money, as we will see later in this book, criminal money may represent good business for the bank (Harvey and Lau, 2009).

2.3 Bank Fraud

Fisher (2008) describes a US banking fraud case. It involved Jeffrey Brett Goodin, of Azusa, California who was sentenced to 70 months imprisonment as a result of his fraudulent activities. Goodin had sent thousands of e-mails to America Online (AOL's) users that appeared to be from AOL's billing department and prompted customers to send personal and credit card information, which he then used to make unauthorized purchases. The e-mails referred the AOL customers to one of several web pages where the victims could in-put their personal and credit information. Goodin controlled these web pages, allowing him to collect the information that enabled him and others to make unauthorized charges on the AOL users' credit or debit cards.

Bank fraud is a criminal offence of knowingly executing a scheme to defraud a financial institution. For example in China, bank fraud is expected to increase both in complexity and in quantity as criminals keep upgrading their fraud methods and techniques. Owing to the strong penal emphasis of Chinese criminal law, harsh punishment including death penalty and life imprisonment has been used frequently for serious bank fraud and corruption. Cheng and Ma (2009) found, however, that the harshness of the law has not resulted in making the struggle against criminals more effective. The uncertain law and inconsistent enforcement practices have made offenders more fatalistic about the matter, simply hoping they will not be the unlucky ones to get caught.

Financial fraud in the banking sector is criminal acts often linked to financial instruments, in that investors are deceived into investing money in a financial instrument that is said to yield a high profit. Investors loose their money because no investment actually takes place, the instrument does not exist, the investment cannot produce the promised profit or it is a very high-risk investment unknown to the investor. The money is usually divided between the person who talked the investor into the deal and the various middlemen, who all played a part in the scheme (Økokrim, 2008).

Picard (2009) found that IT systems in banks facilitate the commitment of fraud and, at the same time, complicates the investigation. Therefore, there is an attractive opportunity for fraud associated with low risk. What looks like an opportunity from the criminal standpoint represents an inherent risk from within organizations. One opportunity issue concerns the internal operations of a bank. Fraud aims at internal operations and exploits the many weaknesses or avoids the limited controls in place.

Fisher (2008) argues that a system with one-day check clearance in the UK would increase the exposure to cyber crime. He undertook a comparative analysis of the UK and US check-clearance systems, examined the enhanced vulnerability to fraud occasioned by a one-day check clearance system and considered the resulting evidential difficulties encountered in US check fraud prosecution. The introduction of one-day check clearance in the USA heralded an increase in cyber crime banking fraud and a reduction of the ability of the prosecuting authorities to bring cases to court because of the paucity of documentary evidence.

2.4 Advance Fee Fraud

As mentioned in the Introduction, Nigeria-related financial crime is extensive and 122 out of 138 countries at an Interpol meeting complained about Nigerian involvement in financial fraud in their countries. The most notorious type attempted daily on office workers all over the world, is the so-called advance fee fraud. The sender will seek to involve the recipient in a scheme to earn millions of dollars if the recipient pays an advance fee (Ampratwum, 2009).

Fraud can be defined as intentional misrepresentation for the purpose of gain. It is a typical financial crime, often carried out by white-collar criminals. Fraud has existed since the origin of recorded history. The nature of fraud expanded with the introduction of Internet communications, electronic commerce (e-commerce) and electronic business (e-business). Much evidence suggests that technology-based fraud is increasing rapidly in frequency despite law enforcement efforts (Nhan et al., 2009).

Nigerian criminals are approaching potential victims of advance fee fraud e-mail without prior contact. Victims' addresses are obtained from telephone and e-mail directories, business journals, magazines, and newspapers. A typical advance fraud letter describes the need to move funds out of Nigeria or some other sub-Saharan African country, usually the recovery of contractual funds, crude oil shipments or inheritance from late kings or governors (Ampratwum, 2009). This is an external kind of fraud, where advance-fee fraudsters attempt to secure a prepaid commission for an arrangement that is never actually fulfilled or work that is never done.

Victims are often naïve and greedy, or at worst prepared to abet serious criminal offences such as looting public money from a poor African state. The advance fee fraud has been around for centuries, most famously in the form of the Spanish prisoner scam (Ampratwum, 2009: 68):

> In this, a wealthy merchant would be contacted by a stranger who was seeking help in smuggling a fictitious family member out of a Spanish jail. In exchange for funding the "rescue" the merchant was promised a reward, which of course, never materialized.

Advance fee fraud is expanding quickly on the Internet. Chang (2008) finds that this kind of fraud is a current epidemic that rakes in hundreds of millions of dollars per year. The advent of the Internet and proliferation of its use in the last decades makes it an attractive medium for communicating the fraud, enabling a worldwide reach. Advance fee fraudsters tend to employ specific methods that exploit the bounded rationality and automatic behavior of victims. Methods include assertion of authority and expert power, referencing respected persons and organizations, providing partial proof of legitimacy, creating urgency, and implying scarcity and privilege.

Holt and Graves (2007) studied schemes applied in advance fee fraud e-mail. Their study explored the mechanisms employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages. Their findings demonstrate that multiple writing techniques are used to generate responses and information from victims. Half of the messages also requested that the recipient forwarded their personal information to the sender, thereby enabling identity theft as well.

The findings by Holt and Graves (2007) suggest that fraudsters employ deceptively simple messages in an attempt to identify and victimize individuals. Fraudsters utilize unique phrases throughout each e-mail to increase the plausibility of their messages and likelihood of responses. For example, most messages have an enticing subject line that may compel an individual to open the e-mail. Frequent subject lines include "Urgent Attention", "Read and Reply as soon as possible", "Attention Friend", and "From Dr. Mariam Abacha". Lottery notifications typically employ expressions such as "Congratulations" or "Attention Winner", while business messages use expressions like "Payment Agent Needed".

The body of the e-mail allows the scammer to create a false impression of professionalism by providing business credentials and statements about the need for trust and confidentiality. Fraudsters may also increase the plausibility of their claims by tying the story to current events, or through the use of religious phrases or emotional language in the messages. In addition to confidentiality, the senders request that they be contacted as quickly as possible. Half of the e-mails examined by Holt and Graves (2007) asked the recipient to provide the sender with personal information.

Nhan et al. (2009) studied fraudulent email solicitation. They analyzed the nature of the solicitation, the nature of the solicitor, and the information asked of the target. Their research was based on two email accounts that captured a total of 476 unsolicited emails identified as suspect in intent over a three-month period. The large majority of emails originated from the United Kingdom (37%) Nigeria (33%). Emails also cam from Taiwan, Russia, China, the Ivory Coast, and France. Many solicitors claimed to be a bank officer (29%), lawyer (27%), and politician (17%).

To generate the trust of targeted victims, solicitors typically generate and include a presentation expected to be appealing to the victim's concern for others. Therefore, many offenders include alleged personal information in their emails. Most commonly, solicitors mentioned that they were married (32%), or they were sick (23%). Others reported being a victim of some social or political event (15%), having children (12%), being somehow related to a victim of a tragic incident (10%), or being the heir (7%) who will soon collect a large sum of money that they will allegedly share (Nhan et al., 2009).

2.5 Malicious Agents

The primary motivation of malicious agents attacking information systems has changed over time from pride and prestige to financial gain (Galbreth and Shor, 2010). A malicious agent is a computer program that operates on behalf of a potential intruder to aid in attacking a system or network. While a computer virus traditionally was the most prominent representative of the malicious agent species, spying agents have become more common. Spying agents transmit sensitive information from the organization to the author of the agent. Another kind of agent is the remotely controlled agents, which provides the attacker with complete control of the victim’s machine.

Software is classified as malicious software (malware) based on the perceived intent of the creator rather than any particular features. Malware for profit includes spy ware, botnets, keystroke loggers, and dialers. In a botnet, the malware logs in to a chat system, while a key logger intercepts the user’s keystrokes when entering a password, credit card number, or other information that may be exploited. Malicious software can automate a variety of attacks for criminals and is partially responsible for the global increase in cyber crime (Bossler and Holt, 2009).

Bossler and Holt (2009) applied routine activities theory to study malicious agents. According to routine activities theory, direct-contact predatory victimization occurs with the convergence in both space and time of three components: a motivated offender, the absence of a capable guardian, and a suitable target. As opposed to the physical world, the virtual world often ignores the times of criminal activities. Therefore, the activities of potential victims and the websites or files they come in contact with are more important than the times of such activities.

2.6 Stock Robot Manipulation

A computer program was able to manipulate a stock-trading robot linked to Oslo Stock Exchange in Norway. The program generated fake buying and selling orders that terminated each other, while at the same time influencing stock prices. Then the program performs real buying and selling orders where stocks were bought at low prices and sold at high prices. This kind of stock value manipulation is illegal in Norway, and two stock traders were caught in 2010 (DN, 2010).

2.7 Identity Theft

Miri-Lavassani et al. (2009) found that identity fraud is the fastest growing white-collar crime in many countries, especially in developed countries. In 2008, the number of identity fraud victims increased by 22 percent to 9.9 million victims.

Intelligence is important as a source of information for crime analysis. An example of crime analysis is the identity fraud measurement model developed by Miri-Lavassani (2009). The five-dimensional measurement model is concerned with: (i) types of identity fraud, (ii) impact of identity fraud, (iii) methods of identity fraud, (iv) transnational identity fraud, and (v) business identity fraud risks. Financial institutions in Canada were surveyed for empirical data collection. Factor analysis was employed on the data for evaluating dimensions and contents of each dimension in the model, resulting in a four-dimensional rather than five-dimensional measurement model, where methods of identity fraud includes transnational identity fraud.

Types of identity fraud reflect the way in which identity thieves use the stolen or forged identities of other individuals to commit unlawful acts without the knowledge of the victims. Types of identity fraud can be measured by the numbers of credit card fraud; unauthorized use of utilities or services; insurance fraud; investment fraud; fraudulent loans and mortgages; bank fraud; new credit cards and utility (internet, phone, etc.) applied for, insurance policies issued, bank accounts opened by identity thieves; misuse of existing credit cards, utility insurance policies, and bank accounts by identity thieves.

Impact of identity fraud can be measured in terms of direct costs of identity fraud to business; direct costs of fraud to customers; direct non-financial impact of fraud on business (such as damaged reputation); direct non-financial impact of fraud on customers (such as damaged credit records and record history); the amount of time individual fraud victims spend to resolve problems; the amount of time business spend to resolve fraud problems; emotional and psychological impact of fraud on victims; and emotional and psychological impact of fraud on victims families.

Methods of identity fraud refer to the methods that have been used by identity thieves for acquiring the identifiers of identity fraud victims. Methods include main theft; filling fraudulent address changes; theft or loss of wallet or purse; phishing; vishing; employment records; theft by breaking and entering; theft through internet, computer viruses, spy ware, and worms; telephone solicitation; extortion or sabotage by an insider; and extortion or sabotage by an outsider. Transnational methods include measuring identity fraud incidents in the country while the identity thieves are located in other countries; and measuring worldwide identity fraud originating from Canada.

Business identity fraud risks includes the business itself; the employee of the organization; and other organizations and customers that work with the organization.

The study by Miri-Lavassani et al. (2009) resulted in a measurement model that includes 27 indicators and four factors. They argue that in the absence of a widely developed and employed identity theft measurement model, many misconceptions about the problem of identity fraud have emerged. One example is the biased perception that the use of the Internet for electronic business increases the risk of exposure to identity fraud.

2.8 Digital Piracy

Digital piracy is defined as the illegal copying of digital goods, software, digital documents, digital audio (including music and voice), and digital video for any other reason other than to backup without explicit permission from and compensation to the copyright holder (Higgins, 2007). The Internet facilitates digital piracy because the network allows crime to take place detached from the owner. For example, digital music piracy is committed through a multitude of modus operandi (Higgins et al., 2008). The issue of digital piracy has become a topic of immense concern, such that it has attracted the attention of legislators, academics as well as business executives (Moore and McMullan, 2009).

Higgins (2007) studied the links between low self-control, rational choice, value, and digital piracy. His results show that low self-control has direct and indirect effects on intentions to digital piracy. Further, his study shows that low self-control has indirect links with a modified version of situational factors such as value. These results indicate that low self-control and rational choice theory maybe compatible theories that can explain digital piracy.

For the established music recording and distribution industry, the appearance of Napster, the first peer-to-peer (P2P) network software, was a disruptive event with substantial impact. Napster was created in 1999 by the 18 year-old Shawn Fanning as a software application aimed at simplifying the process of finding and sharing music files online. The software application made it possible to replicate and circulate highly compressed music files at no cost. Napster network gained enormous popularity and generated an enormous selection of downloadable music. Millions of users connected to the network to share and swap copyright-protected music without explicit permission (Bachmann, 2007).

In 2003, the recording industry in the US initiated a number of lawsuits against P2P network users to stop them from illegally sharing music files. A lawsuit was also filed against Napster. The accusations against Napster, Inc. were based on the architecture of the system. Napster used centrally located and company owned servers to generate and maintain lists of connected users and the music files they provided (Bachmann, 2007: 214):

> While the actual file transactions were conducted directly between the users, these central servers also facilitated the connections between users and initiated the music file downloads.

Because of the centralized architecture, the recording industry defined Napster as a listing service that offered a search engine, a directory, an index, and links, and was thus seen as being ultimately responsible for the music file transactions and the copyright violations they caused.

In an empirical study of online music pirates, Bachmann (2007) found that file sharing and music downloading have to be analyzed separately when studying impacts of the enforcement of copyright laws on file sharing communities and the music downloading individuals. The results show that Internet users in the US are well aware of the circumstance that legal prosecution is only targeting the sharing of music files.

In a different study of online music pirates, Higgins et al. (2008) found that trajectories of digital piracy are tied to neutralization toward digital piracy. Neutralization includes denial of responsibility, denial of injury, denial of victim, condemnation of condemners, and appeal to higher loyalty. The findings of their study indicate that many individuals will take a deviant behavior from social controls to allow themselves to pirate music without developing a pirating identity. Individuals apply different forms of neutralization for a self-serving purpose as they detach themselves from the criminality of the behavior.

While Higgins et al. (2008) studied neutralization in relation to social control, Moore and McMullan (2009) studied neutralization in direct relation to digital piracy. They found that all participants in their study indicated support, though to varying extent, for neutralization techniques. One of the neutralization techniques found was that everyone else is doing it. However, only sixteen percent of the study participants indicated this technique, which surprised one of the study's authors as they expected more individuals to associate with this belief.

2.9 Intellectual Property Crime

Intellectual property crime is a serious financial concern for car manufacturers, luxury goods makers, media firms and drug companies. Most alarmingly according to Interpol (2009), is that counterfeiting endangers public health, especially in developing countries, where the World Health Organization estimates more than 60 percent of pharmaceuticals are fake goods.

Interpol (2009) launched a new database on international intellectual property crime, which was created to fill the void in seizure data collated by various international bodies and the private sector. Of 1,710 entities in the database, checks against other Interpol databases revealed links to credit card and currency counterfeiting, fraud, money laundering, theft, violent crimes and trafficking in human beings, weapons and drugs. This demonstrates the role of organized crime in large-scale counterfeiting and piracy.

Intellectual property's rising value in the production of wealth has been mirrored by its increasing vulnerability to crime. Snyder and Crescenzi (2009) found that intellectual property crime is often linked to cyber crime, and they explored the risks of crime inherent in intellectual capital and a distributed cyber environment to demonstrate that traditional legal remedies are largely ineffective to protect property rights. Unlike cash or paintings, for example, which require the criminal to enter a vault or museum and subsequently carry off the stolen objects, intellectual property crime requires only that the criminal make an electronic copy. The classic remedy in cases of theft is to return the property to its original owner. Today, downloaded movies and music files are as useful as the originals.

2.10 Internet Gambling

Internet gambling is a global issue that has an effect upon all countries independent of their local laws prohibiting or allowing gambling to take place. Fidelie (2009) asked the question whether Internet gambling is an innocent activity or cyber crime. She found a very unclear legal status of Internet gambling. Gambling is an industry that has undergone many changes throughout its existence. Gambling is generally controlled by state governments in an exercise of their police powers. However, Internet gambling's interstate and international scope necessitates its governance by international law.

Pontell et al. (2007) studied the case of Antigua for illegal offshore Internet gambling. Antigua is a small Caribbean island that gained its independence from Britain in 1981. An Internet gambling site called World Sports Enterprise (WSE) was launched in 1997 and is located on the island. Customers were required to transmit $300 before they were permitted to gamble, and the WSE exacted ten percent off the top of each wager. In its first fifteen months of operation the company took in $3.5 million. It is argued that organized crime has infiltrated the Antiguan gambling endeavor and that underage participants are allowed to play.

Because of the great difficulty in banning Internet gambling, Fidelie (2009) recommends that governments all over the world should regulate and tax online business ventures. She suggests that because of the unclear legal status of Internet gambling, there must be a legislation explicitly defining what is and is not permissible activity, as well as an emphasis on regulation by world governments and self-regulation by the Internet gambling businesses.

3. Child Grooming Case

While we focus on white-collar financial crime in this book on computer crime, we must not forget that there are a number of other types of crime that are typical for cyber crime and Internet crime as well. Typical examples are hacking, child pornography and online child grooming. In this chapter, we present the case of child grooming as computer crime.

Internet use has grown considerably in the last decade. Information technology now forms a core part of the formal education system in many countries, ensuring that each new generation of Internet users is more adept than the last. Research studies in the UK suggest that the majority of young people aged 9-19 accessed the Internet at least once a day. The Internet provides the opportunity to interact with friends on social networking sites such as Myspace and Bebo and enables young people to access information in a way that previous generations would not have thought possible. The medium also allows users to post detailed personal information, which may be accessed by any site visitor and provides a platform for peer communication hitherto unknown (Davidson and Martellozzo, 2008). There is, however, increasing evidence that the Internet is used by some adults to access children and young people in order to groom them for the purposes of sexual abuse. Myspace have recently expelled 29,000 suspected sex offenders and is being sued in the United States by parents who claim that their children were contacted by sex offenders on the site and consequently abused (BBC, 2007). The Internet also plays a role in facilitating the production and distribution of indecent illegal images of children, which may encourage and complement online grooming.

3.1 Online Offenders

Recent advances in computer technology have been aiding sexual sex offenders, stalkers, child pornographers, child traffickers, and others with the intent of exploiting children (Kierkegaard, 2008: 41):

> Internet bulletin boards, chat rooms, private websites, and peer-to-peer networks are being used daily by pedophiles to meet unsuspecting children. Compounding the problem is the lack of direct governance by an international body, which will curb the illegal content and activity. Most countries already have laws protecting children, but what is needed is a concerted law enforcement and international legislation to combat child sex abuse.

Men who target young people online for sex are pedophiles (Kierkegaard, 2008; Wolak et al., 2008). According to Dunaigre (2001), the pedophile is an emblematic figure, made into a caricature and imbued with all the fears, anxieties and apprehensions rocking our society today. Pedophile acts are - according to the World Health Organization (WHO) - sexual behavior that an adult major (16 years or over), overwhelmingly of the male sex, acts out towards prepubescent children (13 years or under). According to the WHO, there must normally be a five-year age difference between the two, except in the case of pedophilic practices at the end of adolescence where what counts is more the difference in sexual maturity. However, the definition of criminal behavior varies among countries. As will become evident from reading this article, pedophile acts in Norway are sexual behavior that a person acts out towards children of 16 years or under. There is no minimum age definition for the grooming person in Norwegian criminal law, but age difference and difference in sexual maturity is included as criteria for criminal liability.

Wolak et al. (2009: 4) present two case examples of crimes by online sex offenders in the United States:

- Police in West Coast state found child pornography in the possession of the 22-year-old offender. The offender, who was from a North-eastern state, confessed to befriending a 13-year-old local boy online, traveling to the West Coast, and meeting him for sex. Prior to the meeting, the offender and victim had corresponded online for about six months. The offender had sent the victim nude images via web cam and e-mail and they had called and texted each other hundreds of times. When they met for sex, the offender took graphic pictures of the encounter. The victim believed he was in love with the offender. He lived alone with his father and was struggling to fit in and come to terms with being gay. The offender possessed large quantities of child pornography that he had downloaded from the Internet. He was sentenced to 10 years in prison.

- A 24-year-old man met a 14-year-old girl at a social networking site. He claimed to be 19. Their online conversation became romantic and sexual and the victim believed she was in love. They met several times for sex over a period of weeks. The offender took nude pictures of the victim and gave her alcohol and drugs. Her mother and stepfather found out and reported the crime to the police. The victim was lonely, had issues with drugs and alcohol, and problems at school and with her parents. She had posted provocative pictures of herself on her social networking site. She had met other men online and had sex with them. The offender was a suspect in another online enticement case. He was found guilty but had not been sentenced at time of the interview.

According to Davidson and Martellozzo (2008: 277), Internet sex offender behavior can include: "the construction of sites to be used for the exchange of information, experiences, and indecent images of children; the organization of criminal activities that seek to use children for prostitution purposes and that produce indecent images of children at a professional level; the organization of criminal activities that promote sexual tourism".

Child grooming is a process that commences with sexual sex offenders choosing a target area that is likely to attract children. In the physical world, this could be venues visited by children such as schools, shopping malls or playgrounds. A process of grooming then commences when offenders take a particular interest in the child and make them feel special with the intention of forming a bond. The Internet has greatly facilitated this process in the virtual world. Offenders now seek out their victims by visiting Internet relay chat (IRC) rooms from their home or Internet cafés at any time. Once a child victim is identified, the offender can invite it into a private area of the IRC to engage in private conversations on intimate personal details including the predator's sex life (Australian, 2008).

3.2 Internet Characteristics

The Internet is an international network of networks that connects people all over the world. Any computer can communicate with almost any other computer linked to the Internet. The Internet has created a universal technology platform on which to build all sorts of new products, services, communities and solutions. It is reshaping the way information technology is used by individuals and organizations. The Internet has provided an expedient mode of communication and access to a wealth of information (Dombrowski et al., 2007).

In less than two decades, the Internet has moved from a strange communications medium to an obvious tool in our homes, schools, workplaces and travels. It enables us to search information, perform routine tasks and communicate with others. The technological aspects of the Internet are developing at the same high speed as the number of users globally. The Internet provides a social context for us to meet with others and to exchange information (Quayle et al., 2006).

The World Wide Web is a system with universally accepted standards for storing, retrieving, formatting, changing and displaying information in a networked environment. Information is stored and displayed as electronic pages that can contain numbers, text, pictures, graphics, sound and video. These web pages can be linked electronically to other Web pages, independent of where they are located. Web pages can be viewed by any type of computer.

In a survey of young people in Norway between the ages 8 and 18 years old, 78 percent of the respondents said that they are involved in chatting. The use of chatting for communication is more common than the use of e-mail in this age group. In the age group 17-18 years old, all respondents said they do chatting. The percentage reporting that they have been plagued while chatting was 9 percent. Among chatters about one third has met persons in reality that they first met while chatting (Medietilsynet, 2008).

The Internet is a valuable tool; however, it can also be detrimental to the wellbeing of children due to numerous online hazards (Dombrowski et al., 2007: 153):

> There is the potential for children to be abused via cyberspace through online sexual solicitation and access to pornography. Indeed, the Internet is replete with inappropriate material, including pornography, chat rooms with adult themes and access to instant messaging wherein others could misrepresent themselves. Because children are actively utilizing the Internet where unknown others can have access to them or where they can be exposed to inappropriate sexual materials, they require safeguarding and education in safe Internet use.

Online grooming might be compared to online learning and other forms of online activity. The purpose of such analogies is to identify both similarities and differences. Learning on the Internet, for example, is structured as a formal and non-anonymous activity. To some it is scary rather than safe, because students are asked to expose their (lack of) knowledge on the Internet and share it with others. Active and extrovert students enjoy this, while other students choose to be passive on-lookers.

Generally, going online enables individuals to play a personality role, which might be more or less different from their real personality. There will always be a difference between your role in virtual reality and in real world. We play roles as adults and parents, or children and students, both in the real world and in virtual realities. However, in the virtual world we may find it easier to live our dreams and fantasies. In the type "second life" environments on the Internet, people tend to be unfaithful and to build their dream existence alone or with others.

What is then so special about being online? One answer to this question is that you can be in a different, informal and anonymous setting to live out dreams and fantasies.

3.3 Internet Relationships

The Internet is a special artifact system that has enormous technical and social positive impacts on modern society (Kierkegaard, 2008: 41):

> *The online environment enables access to a wealth of information and communication across both distance and time. There is a vast amount of data available on virtually every subject, making it an effective learning tool.*

However, the Internet is also a double-edged sword with negative and positive consequences (Kierkegaard, 2008: 41):

> *It has a potential for misuse and has generated societal concerns. Today, the danger for children is even greater because the Internet provides anonymity to predators.*

Recent advances in computer technology have been aiding sexual predators, stalkers, child pornographers, child traffickers, and others with the intent of exploiting children. While they have existed prior to the Internet, the advent of the new technology two decades ago has allowed for easier and faster distribution of pornographic materials and communication across national and international boundaries (Kierkegaard, 2008).

On the other hand, the Internet is not all negative concerning sexual communication (Calder, 2004: 3):

> *It can be used for healthy sexual expression. For example, the Internet offers the opportunity for the formulation of online or virtual communities where isolated or disenfranchised individuals e.g. gay males and lesbians can communicate with each other around sexual topics of shared interest; it offers educational potential; and it may allow for sexual experimentation in a safer forum, thus facilitating identity exploration and development.*

The Internet allows sex offenders instant access to other sex offenders worldwide, forums facilitate open discussion of their sexual desires, shared ideas about ways to lure victims, mutual support of their adult-child sex philosophies, instant access to potential child victims worldwide, disguised identities for approaching children, even to the point of presenting as a member of teen groups. Furthermore, the Internet allows potential offenders ready access to chat areas and social networking sites reserved for teenagers and children, to discover how to approach and who to target as potential victims. The Internet provides a means to identify and track down home contact information, and the Internet enables adults to build long-term virtual relationships with potential victims, prior to attempting to engage the child in physical contact.

Relationships are built using social software. Through the Internet, people are discovering and inventing new ways to share knowledge and interests. People communicate on the Internet with each other in a human voice. These conversations using social software are collectively referred to as social media, a wide-ranging terms than encompasses the practice and resulting output of all kinds of information created online by those who were previously consumers of that media (Cook, 2008: 7):

> *Philosophically, social media describes the way in which content (particularly news and opinion) has become democratized by the Internet and the role people now play not only in consuming information and conveying it to others, but also in creating and sharing content with them, be it textual, aural or visual.*

For this reason, social media is interchangeably referred to as consumer- or user-generated content. Social media is often defined by the categories of software tools that people use to undertake this consuming, conveying, creating and sharing content with each other, including blogs, pod casts, wikis and social networking that have found their place on the Internet (Cook, 2008).

Blogs in terms of online personal journals are one of the examples mentioned by Cook (2008), and Mitchell et al. (2008) phrased the following question: 'Are blogs putting youth at risk of online sexual solicitation or harassment?' They conducted a telephone survey of 1,500 youth Internet users, ages 10-17, in the USA. They found that 16 percent of youth Internet users reported blogging in the past year. Teenagers and girls were the most common bloggers, and bloggers were more likely than other youth to post personal information online.

However, Mitchell et al. (2008) found that bloggers were not more likely to interact with people they met online and did not know in person. Youth who interacted with people they met online, regardless of whether or not they blogged, had higher odds of receiving online sexual solicitations. Bloggers who did not interact with people they met online were at no increased risk for sexual solicitation. Moreover, posting personal information did not add to risk. The only difference found was related to harassment, since youthful bloggers were found to be at increased risk for online harassment, regardless of whether they also interacted with others online.

3.4 Grooming Legislation

The concept of sexual grooming is well documented in the sex offender literature (Finkelhor, 1984), and is now filtering into legislation policy, crime detection and prevention initiatives. A recent report in the Guardian Newspaper suggested that the Child Exploitation and Online Protection Centre in the UK receive an average of 4 phone calls per day from young people planning to meet people with whom they have developed an online, sexual relationship (25/02/2009).

Potential offenders using the Internet to perpetrate sexual offences against children fall into two principal categories: Those who use the Internet to target and 'groom' children for the purposes of sexual abuse (Finkelhor et al. 2000); and those who produce and/or download indecent illegal images of children from the Internet and distribute them. Recent legislation has sought to protect young people from Internet abuse through the introduction of a 'grooming' clause. This new offence category was introduced in the Sexual Offences Act (2003) in England and Wales (this section of the Act also applies to Northern Ireland). Section 15 makes 'meeting a child following sexual grooming' an offence; this applies to the Internet, to other technologies such as mobile phones and to the 'real world'.

'Grooming' involves a process of socialization through which a potential offender seeks to interact with a child under the age of 16, possibly sharing their hobbies and interests in an attempt to gain trust in order to prepare them for sexual abuse. The concept of 'grooming' is now also recognized in legislation in the UK. The Sexual Offences Act (2003) in England and Wales, and Northern Ireland and the Protection of Children and Prevention of Sexual Offences Act (2005) in Scotland include the offence of 'meeting a child following certain preliminary contact' (section 1). 'Preliminary contact' refers to occasions where a person arranges to meet a child who is under 16, having communicated with them on at least one previous occasion (in person, via the Internet or via other technologies), with the intention of performing sexual activity on the child.

Several countries are beginning to follow the UK in legislating against grooming behavior. Sexual grooming has also recently been added to the Crimes Amendment Act (2005) in New Zealand. In the US it is an offence to transmit information electronically about a child aged 16 or under, for the purpose of committing a sexual offence. The Australian Criminal Code makes similar restrictions, as does the Canadian Criminal Code. The legislation in the UK differs in that the sexual grooming offence applies both to the new technologies including the Internet and mobile phones, and also to the 'real world'; legislation in other countries addresses only electronic grooming via the Internet and mobile phones.

Norway is the only other European country to adopt the grooming legislation. The relevant sections in the General Civil Penal Code ("straffeloven") concerned with sexual offenders in Norway include Section 195: Any person who engages in sexual activity with a child who is under 14 years of age shall be liable to imprisonment for a term not exceeding 10 years. If the said activity was sexual intercourse the penalty shall be imprisonment for not less than 2 years, and Section 196: Any person who engages in sexual activity with a child who is under 16 years of age shall be liable to imprisonment for a term not exceeding 5 years. Section 201a is the new grooming section in Norwegian criminal law. This section was included in The General Civil Penal Code in April 2007. :

With fines or imprisonment of not more than 1 year is any person liable, who has agreed a meeting with a child who is under 16 years of age, and who with intention of committing an act as mentioned in sections 195, 196 or 200 second section has arrived at the meeting place or a place where the meeting place can be observed.

In Norwegian law the grooming section refers to *the intention of committing an act*. However, the perpetrator must actually appear for a meeting (sometimes a police trap), an intention to meet is not enough, it is possible that it should be but it is difficult to prove beyond doubt. Therefore, the legislation is phrased as follows: "...has arrived at the meeting place or a place where the meeting place can be observed". It is the potential scene of the crime, which is the meeting place where the offence is intended to take place, that the offender has arrived at, or the offender can observe the potential crime scene from where he is located. We refer to the potential offender and offender as "he", although little is known in the literature abut the gender of all online groomers.

3.5 European Policy

A recently published EU (2009) document entitled '*Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography'* sets out the shortcomings and vision in protecting young people form sexual abuse. The framework decision outlines the difficulty in protecting young people when there is such widespread variation in national criminal law and law enforcement practice in Europe. The situation is seen as exacerbated by the hidden nature of the offending and compounding issues such as victims' reluctance to report abuse.

The role of information technology in facilitating global abuse and sex offender networks is discussed. The EU suggest that '*developments in information technology have made these problems more acute by making it easier to produce and distribute child sexual abuse images while offering offenders anonymity and spreading responsibility across jurisdictions. Ease of travel and income differences fuel so-called child sex tourism, resulting often in child sex offenders committing offences abroad with impunity. Beyond difficulties of prosecution, organised crime can make considerable profits with little risk*' (p2).

Following this Framework decision it is likely that other European countries will follow the UK and Norwegian example by introducing grooming legislation and the 'viewing' of indecent child images will become an offence:

'*New forms of sexual abuse and exploitation facilitated by the use of IT would be criminalised. This includes knowingly obtaining access to child pornography, to cover cases*

where viewing child pornography from websites without downloading or storing the images

does not amount to "possession of" or "procuring" child pornography. Also the new offence

of "grooming" is incorporated closely following the wording agreed in the COE Convention'(p6).

Article 5 refers to online grooming as the 'solicitation of children for sexual purposes' (p5) and asks that each member state ensure that such conduct is punishable in law. This refers to cases involving children under the age of consent under national law (which varies considerably across Europe), where an adult arranges to meet for the purposes of sexual abuse via the means of '*an information system'* (p5).

Grooming legislation has been introduced in several countries but is now recognized in the EU Framework Decision (Article 5), the difficulty is of course that the framework is not in any way enforceable and countries may simply chose to 'opt out' particularly if their current legislative framework, particularly in respect of the age of consent, does not easily accommodate the recommended legislation.

3.6 Seventeen Internet Characteristics

We are all familiar with online services on the Internet. A typical example is online banking, where we complete our payments of bills at home. Most Norwegians have many years of personal experience using online services on the Internet. According to the United Nations (2008), Norway is ranked third in the world in terms of online services provided by the government. Sweden and Denmark are on the top of the list, and Norway is followed by the United States and the Netherlands. The United Kingdom is ranked tenth on the list.

A number of characteristics of the Internet for online services has been observed, which may shed light on methods potential offenders use to groom children. The following list was generated based on a literature review:

1. *Disconnected personal communication*. While communication on the Internet might be personal in content, it is not perceived as interpersonal in meaning. A typical example is e-mail, where the sender might feel completely disconnected from the time and place the receiver reads the e-mail message. Even when chatting in real time, sender and receiver may perceive both involvement and disconnectedness at the same time. Some may change their personality unconsciously when moving from face-to-face communication to e-mail communication (Weber, 2004). Internet grooming can be and often is different from 'real world' grooming in that potential offenders spend little time chatting and will come straight to the point, sometimes instantly, e.g. 'would you like to meet for sex'. This would suggest that the Internet might act to remove inhibitions associated with face-to-face contact, which can be explained by the disconnected nature of personal communication on the Internet, thereby avoiding unpleasant emotional states (Quayle et al., 2006). There are, however, some potential offenders who will still spend a considerable amount of time grooming a child online, particularly in peer to peer networks, in order to prepare them for abuse (Davidson, 2008). Generally, there are a number of distinguishing characteristics between the Internet and the real world as the two principally different forms of grooming.

2. *Mediating technology*. According to Afuah and Tucci (2003), the Internet is a mediating technology that interconnects parties that are independent. The interconnections can be business-to-business (B2B), business-to-consumer (B2C), government-to-business (G2B), person-to-person (P2P) or any other link between individuals and organizations. In the case of grooming, Internet serves as a mediating technology mainly for person-to-person (P2P) communication, but person-to-group (P2G) and group-to-person (G2P) do also occur. In relation to grooming, changes in interconnections occur over time, where an initial contact may start as person-to-group, for example group of teenagers, and then move into person-to-person, where the potential offender has singled out of potential victim.

3. *Universality*. The universality of the Internet refers to the Internet's ability to both enlarge and shrink the world. It enlarges the world because anyone anywhere in the world can potentially make his or her services, messages and requests available to anyone anywhere else in the world anytime. It shrinks the world in that distance is reduced on electronic highways (Afuah and Tucci, 2003). In the case of grooming, the Internet enables each grooming individual to potentially contact anyone, anywhere and anytime. Contact is established without the groomer having to travel physically, all he needs to do is to travel electronically. The Internet combines global communications with an incredible range of resources (Calder, 2004). The global reach enabled by the Internet permits grooming to cross cultural and national boundaries far more conveniently and cost effective than is true in traditional grooming (Laudon and Laudon, 2010). However, cultural and communication issues exist between jurisdictions that can limit the extent of universality perceived by users.

4. *Network externalities*. A technology or product exhibits network externalities when it becomes more valuable to users as more people take advantage of it. A classic example is the first person in Norway who got himself a telephone. Until a second person got a telephone, there was nobody in Norway to talk to on the phone. The value of the telephone for each subscriber increases with the number of subscribers. Similarly, the value of the Internet increases with the number of Internet users. The more people that are connected to a network within the Internet, the more valuable the network is to each user (Afuah and Tucci, 2003). The more children that are connected to a network, the more valuable the network is to each groomer, since he is able to reach and get in contact with more potential victims. Since Internet access is found in more and more homes all over the world, the number of potential victims rises accordingly.

5. *Distribution channel*. The Internet acts as a distribution channel for products that are information bits, such as software, music, video, news, tickets and money. There is a replacement effect if the Internet is used to serve the same deliveries, which were serviced by the old physical distribution channel. There is an extension effect if the Internet is used by more people and for new services (Afuah and Tucci, 2003). When grooming children, the potential offender may use the Internet not only for communications. He can also use it to send gifts and other digital items that the child might be interested in. He can also send digital items that the child is not always interested in, such as pornographic pictures and videos to test reactions.

6. *Time moderator*. The Internet has an ability to shrink and enlarge time. It shrinks time for people who want information when information sources are closed. It enlarges time when related work can be done at different points in time (Afuah and Tucci, 2003). Both dimensions of the Internet as a time moderator can be important in online victimization of children. When a child is offline, the groomer can leave messages and gifts for the child to pick up next time the child logs on.

7. *Low cost standard*. Individuals could not exploit the properties of the Internet if they adopt it. For two reasons, adoption has been easy. First and foremost important, the Internet and the web application are standards open to everyone and are very easy to use. Second, the cost of the Internet is a lot lower than that of earlier means of electronic communication (Afuah and Tucci, 2003). Given the low cost standard, access to the Internet is not limited to affluent or well-educated people. Both adults and children have access independent of social class in most countries. For a groomer, this enables access not only to a large number of children but also to a large variety of children. Universal technical standards of the Internet enables any computer to link with any other computer regardless of the technology platform each is using (Laudon and Laudon, 2010).

8. *Electronic double*. It is not the real person who is present on the Internet. It is a digital copy of the person who is present. The digital information about the person creates an image of the person, which we call the electronic double. The way in which a groomer is perceived by a child on the Internet is thus dependent both on the information the person provides and the image this information creates in the child's mind. Even if the groomer is completely honest in all communication with the child, the child may perceive the man as very different from reality and maybe similar to someone the child already knows. Also the man may perceive the child and create an electronic double of the child in his head, which can be far removed from reality, but which may serve his fantasy.

9. *Electronic double manipulation*. The electronic double created on the Internet represents an image of the real person. The real person can change his or her electronic double and make it more or less similar to the real self. The most obvious change is age, where a groomer may claim to be younger than he actually is. This requires consistency in all other information, so that the presented age matches other information about the person. Similarly, children may claim to be older than they actually are.

10. *Information asymmetry*. Information asymmetry is often reduced on the Internet. Information asymmetry exists when one party to a transaction has information that another party does not - information that is important to the transaction. The World Wide Web reduces such information asymmetries, as the other party can find the same information on the web (Afuah and Tucci, 2003). Neither the man nor the child has information monopoly in areas where information is available on the World Wide Web. However, the adult will typically be more knowledgeable than the child, leading to an information asymmetry between potential offender and potential victim, which can be explored and exploited by the potential offender.

11. *Infinite virtual capacity*. Access to the Internet is perceived as unlimited; you do not have to wait on hold or in a long line. For example, virtual communities like chatting houses have infinite capacity for members who can talk anytime of the day for as long as they want (Afuah and Tucci, 2003). However, in some parts of the world there are bandwidth and infrastructure limitations that reduce the virtual capacity. The amount of time online groomers spend in pursuit of children will depend on a number of factors such as available virtual capacity.

12. *Independence in time and space*. While a traditional meeting requires that participants are present at the same place at the same time, virtual meeting on the Internet is possible even if different participants are present at different places at different times. The online environment enables access to a wealth of information and communication across both distance and time (Kierkegaard, 2008). The independence in time and space is typically the case when using e-mail. When participating in a chat room, participants are required to respond within a short time frame, eliminating independence in time, but still keeping independence in space. On the mobile phone, SMS messages have the same characteristic of independence in time and space. Calder (2004) has suggested that the Internet promotes better social relationships as people will be freed from the constraints of time and place, however it could also limit social relationships to the virtual world and reinforce isolation. The relevance to Internet groomers can be found in both relationships and isolation sometimes practiced by potential offenders.

13. *Cyberspace*. Using the Internet is not just a supplement to or add-on to real life. It is also an enabler of an alternative life style in cyberspace with its own cyber culture. Cyberspace is an abstract space, rather than a physical space, where a culture has emerged from the use of computer networks for communication, entertainment and business. Cyber culture can for example be found in virtual communities, which is a group of people that primarily interact via communication media such as newsletters, telephone, e-mail, instant messages or as newsgroups, rather than face to face for social and other purposes (Whittaker, 2004). In terms of online grooming, both adults and children are sometimes members of virtual communities. Calder (2004) argues that there are many benefits that can be derived from the development of online relationships and online relationships that become sexual in cyberspace. Cyberspace can facilitate the formation of romantic relationships, improve the chances of finding an "optimal" partner, highlight that relationships can develop on attachments, and improve one's skills in interpersonal, yet virtual, communication.

14. *Dynamic social network*. The emergence of social network services has radically challenged our understanding of traditional, territorial social networks. An average Westerner's social network comprises about 150 individuals. Once a physical social network is established, this number of members tends to change little over time, and the members themselves do not change very much. In contrast, the Internet enables individuals to expand and reduce their social network and replace members in the network (CEOP, 2006). The Internet provides a social context for more and more people to meet more and more people where people are replaced by other people over time. There is a dynamic social network rather than a stable social network on the Internet. When both potential offenders and potential victims dynamically change their social networks, the likelihood of contact increases.

15. *Ubiquity*. In traditional grooming, a place for grooming is a physical place, such as schools, sporting events, shopping malls, children's clubs or public places. Online grooming is ubiquitous, meaning that it is possible just about everywhere, at all times. It makes it possible to groom from a laptop, at home, at work, or even from a car, using mobile technology. The result is called a grooming space – a grooming place extended beyond traditional boundaries and removed from a temporal and geographic location. From a groomers' point of view, ubiquity reduces transaction costs – the costs of grooming children. To transact with children online in the virtual world, it is no longer necessary that the potential sex offender spends time or money traveling to a grooming place, and much less mental effort is required to make an effort (Laudon and Laudon, 2010).

16. *Richness*. Information richness refers to the complexity and content of a message. Traditional communication channels have great richness. They are able to provide personal, face-to-face communication using aural and visual cues when making contact. The web makes it possible to deliver rich messages with text, audio, and video simultaneously to large numbers of people (Laudon and Laudon, 2010).

17. *Interactivity*. Systems used on the Internet are interactive, meaning they allow for two-way communication between adult and child. Interactivity allows an online groomer to engage a child in ways similar to face-to-face experience but on a massive, global scale (Laudon and Laudon, 2010). Interactivity gives both potential victim and potential offender the possibility of communicating messages without interruption.

This list of 17 characteristics was derived from the research literature. The list might be refined in terms of exhaustiveness; overlap and hierarchy in future research.

3.7 Virtual Offender Communities

Kierkegaard (2008) argues that the anonymity, availability of extremely sensitive personal information and ease of contacting people make social networking sites a useful tool for online child predators. The sites enable both potential offenders and potential victims to explore and exploit all 17 characteristics of the Internet listed above. While many of the sites have age restrictions, it is possible for potential offenders to misrepresent their age (how far the MySpace threat to remove those believed to be over 18 but posing as under 18 is carried out in practice for example is questionable). To hide their IP addresses and locations, they piggyback on Wi-Fi connections or use proxy servers. Decentralized peer-to-peer networks prevent material from being tracked to a specific server, and encryption lets them keep online chats private from those policing the web.

Social networking sites have been studied in different contexts. For example, Tufekci (2008) explored the rapid adoption of online social network sites by students on a US college campus. Using quantitative and qualitative data based on a diverse sample of college students, demographic and other characteristics of social networking site users and non-users were compared. A distinction was made between social grooming and presentation of self. In the study, non-users displayed an attitude towards social grooming (gossip, small-talk and generalized, non-functional people-curiosity) that ranged from incredulous to hostile. Contrary to expectations in the study, non-users did not report a smaller number of close friends compared with users, but they did keep in touch with fewer people. Users were also heavier users of the expressive Internet, which is the practice and performance of technologically mediated sociality.

Thus, while social grooming through language may well be an important human activity, there seems to be no reason to presuppose that everyone will be equally disposed to such activity. Interest in exchange and browsing social information about friends and acquaintances, and curiosity about people, is likely to be related to interest in how an application specifically facilitates such activity (Tufekci, 2008).

When we apply Tufekci's (2008) terminology to online grooming, online groomers are likely to be heavier users of the expressive Internet than pedophilic non-users of social networking sites. As users of the expressive Internet, online groomers use the Internet as an instrument to express opinions and communicate information. *Expressive Internet* is the practice and performance of technologically mediated sociality. It is the use of the Internet to perform and realize interactions, self-presentations, public performance, social capital management, social monitoring, and the production, maintenance and furthering of social ties. The expressive Internet might be recognized as a social ecology involving other people, values, norms and social contexts.

Instrumental Internet, on the other hand, refers to information seeking, knowledge gathering and commercial transactions on the Internet, and non-social communication involved in such transactions. This is typically the Internet of online banking, shopping and checking the weather. Tufekci (2008) found no difference in the use of instrumental Internet for users versus non-users of social networking sites.

The expressive Internet has been expanding rapidly, a process often described in the popular press as the rise of social computing. These tools have been assimilated as a means of social interaction and social integration for increasing numbers of people and communities. People are increasingly using the expressive Internet in ways that complement or further their offline sociality (Tufekci, 2008).

The distinction between the two groups of users is a point also raised by some of the probation officers interviewed by Davidson (2008) in the UK. The probation officers were working with groomers in treatment programs. They spoke about offenders for whom the Internet played a significant role in their lives and who had many online relationships. Using the Internet to offend was almost a natural progression for these offenders as it played such a big part in other areas of their lives.

The Internet has afforded potential sex offenders the opportunity to create their own virtual communities, by allowing instant access to other offenders worldwide, open discussion of their sexual desires, shared ideas about ways to lure victims, and mutual support of their adult-child sex philosophies. Computer technology and the Internet enable potential sex offenders to locate and interact with other offenders more readily than before. The organizational aspects of a common gathering place and the resultant support child predators are providing each other is probably their most significant advantage - and the most troublesome for a concerned public.

Child predators are forming online communities and bonds using the Internet. They are openly uniting against legal authorities and discussing ways to influence public thinking and legislation on child exploitation. While sex offender web sites are being tracked down and removed from Internet servers in countries all over the world, they are popping up again at a higher pace in most parts of the world, many sites are hosted in the United States and Russia.

An example of a web site representing a virtual community for sex offenders is "Boylove". One of the largest sex offender networks on the Internet. On the web site, The Boylove Manifesto could be found, which argued the case for intergenerational relationships (www.prevent-abuse-now.com):

> *As boy lovers we distance ourselves from the current discussion about "child sexual abuse". Human sexuality plays the same part in a boy love relationship as it undoubtedly does in any relationship between human beings. A boy lover desires a friendly and close relationship with a boy.*

Similar text can be found on Boylovers.net:

> *Over the years, paedophilia, or boy love as it is sometimes known, has come under heavy criticism from those who are opposed to it in the media, government and general society. Often, this can be very one-sided and extremely vitriolic in nature.*
>
> *Here at BoyLover.net, we believe that people deserve the chance to hear both sides of the argument. Doubtless, by now you will have read or heard many opinions against paedophilia. With this in mind, we have taken the opportunity to present different views so that people can make an informed decision regarding the subject.*

Boylover.net seems important to mention here, as sex offender research in countries such as Norway, Sweden and the UK tends to focus on girls more than boys. As listed in the Norwegian court sentence, almost all cases are concerned with victimization of girls. Lillywhite and Skidmore (2006) argue that the view that boys are not sexually exploited is very common among many professionals working with vulnerable young men. Do potential sex offenders interested in boys perform online grooming different from potential sex offenders that are interested in girls? Different grooming behaviors may be employed with different genders.

D'Ovidio et al. (2009) conducted a content analysis of 64 websites that promote, advocate, and convey information in support of sexual relationships between adults and children to determine whether these sites were structured as learning environments for crimes involving the sexual exploitation of children. Their findings indicate that the adult-child advocacy websites analyzed were criminal in that they contained a variety of communication tools (e.g., chat rooms, instant messengers, and message boards) to foster interaction among site users and expose users to rationalizations for offending and, in turn, definitions favorable to sexual violations against minors.

Given these research findings, D'Ovidio et al. (2009) recommend law enforcement to consider expanding restrictions for companies offering website hosting services to modify their terms of service agreements to ban content advocating sexual relationships between adults and children. Out of 64 websites studied, 40 websites were registered in the United States, 9 in the Netherlands, 5 in Canada, 4 in the United Kingdom, and 1 in each of the countries Brazil, Czech Republic, Finland, France, Liechtenstein, and Slovakia.

4. Crime Protection

When a business enterprise is the potential victim of computer crime, there are a number of measures that can be implemented to protect the business. In the survey by Hagen et al. (2008), they addressed both breath and depth in defense strategies. Depth is concerned with technological as well as organizational measures, while depth is concerned with dimensions of prevention, emergency preparedness and detection. The survey addressed the use of a broad range of technical security measures relating to access control and protection of data. Technical security measures include prevention (password, physical zones, biometric authentication, and software update), emergency (backup), and detection (intrusion detection and antivirus software). Organizational security measures include prevention (access rights and user guidelines), emergency (management plans), detection (log reviews), and incident response (management reports).

The survey showed that the use of personal passwords is widespread among all enterprises, even the smallest ones (Hagen et al., 2008: 364):

> The trend is that the use of a variety of access control mechanisms increases with enterprise size. There is also a clear tendency that large enterprises implement more and a wider range of emergency preparedness and detection measures. The findings show that small enterprises should strengthen their access control and data protection measures, in addition to security routines.

Hagen et al. (2008) found it surprising that large enterprises did not perform better than small enterprises when it comes to awareness raising and education of users as organizational security measures.

4.1 Criminal Profiling

Profiling of criminals is based on the idea that an individual committing crime in cyberspace using a computer can fit a certain outline or profile. A profile consists of offender characteristics that represent assumptions of the offender's personality and behavioral appearance. Characteristics can include physical build, offender sex, work ethic, mode of transportation, criminal history, skill level, race, marital status, passiveness/aggressiveness, medical history, and offender residence in relation to the crime (Nykodym et al., 2005).

Nykodym et al. (2005: 413) make distinctions between four main categories of cyber crime: espionage, theft, sabotage, and personal abuse of the organizational network:

> Unlike saboteurs and spies, the thief is guided only by mercantile motives for his own gain. The only goal in front of the cyber thief is to steal valuable information from an organization and use it or sell it afterwards for money.

In terms of criminal profiling, Nykodym et al. (2005) found that there is a strong pattern in the age of these cyber robbers. If the crime is for less than one hundred thousand dollars, then most likely the attacker is young 20-25 years old, male or female, still in the low hierarchy of the organization. If the crime involves more money, then the committer is probably an older male from a management level in the organization. His crime is not driven by hate or revenge but by greed and hunger for money.

4.2 White-Collar Criminals

Computer crime is defined as financial crime in this book. White-collar criminals commit financial crime. Characteristics of white-collar criminals include:

- Wealthy yet greedy person
- Highly educated yet practical person
- Socially connected yet anti-social person
- Talks ethics yet acts immoral
- Employed by and in a legitimate organization
- A person of respectability with high social status
- Member of the privileged socioeconomic class
- Commit crime within the occupation based on competence
- On the slippery slope from legitimate to illegitimate behavior
- Often charismatic, convincing and socially skilled
- So desperate to succeed that they are willing to use criminal means
- Sometimes excited about the thrill of not being uncovered
- Often in a position where the police is reluctant to start investigation
- Applies resources to hide tracks and crime outcome
- Behaves in court in a manner creating sympathy and understanding

These kinds of characteristics are organized according to criteria in criminal profiling. For example, some of them are individual factors that are grounded in psychology, while others are environmental factors grounded in sociology. In terms of psychological factors, criminal profiling may ask question such as:

- What kind of personality types become more easily white-collar criminals?
- What are their typical background, life style and development?
- What are their values, ideas and ambitions?

In terms of sociological factors, criminal profiling may ask questions such as:

- How do white-collar criminals look at society and their own role in society?
- How do they perceive laws, and what do they consider to be crime and criminals?
- How do they participate in networks, and what is associated with status and power?

Not all computer criminals are white-collar criminals, but most of them are committing crime for financial gain. Cyber offenders are likely to share a broader range of social characteristics, and the cases of hacking and other Internet-related offences that have been reported in the media would suggest they are likely to be young, clever and fairly lonely individuals who are of middle-class origin, often without prior criminal records, often processing expert knowledge and often motivated by a variety of financial and non-financial goals. Some degree of technical competence is required to commit many computer-related types of crime (Salifu, 2008).

4.3 Deterrence Theory

Some theorists believe that crime can be reduced through the use of deterrents. The goal of deterrence, crime prevention, is based on the assumption that criminals or potential criminals will think carefully before committing a crime if the likelihood of getting caught and/or the fear of swift and severe punishment are present. Based on such belief, general deterrence theory holds that crime can be thwarted by the threat of punishment, while special deterrence theory holds that penalties for criminal acts should be sufficiently severe that convicted criminals will never repeat their acts (Lyman and Potter, 2007). Threat is an external stimulus that exists whether or not an individual perceives it (Johnson and Warkentin, 2010). If an individual perceives the threat, then is has deterrent potential. Deterrence theory postulates that people commit such crimes on the basis of rational calculations about perceived personal benefits, and that the threat of legal sanctions will deter people for fear of punishment (Yusuf and Babalola, 2009).

In more recent years when executives have been seen arrested and handcuffed for the purposes of public humiliation, it sets in motion a deterrence model of crime prevention or at the very least, a shaming policy. The purpose of these public arrests are often symbolic and say more about the regulatory agencies need to appear to be legitimately prosecuting corporate wrongdoers. As such, with regulation so closely tied to the political climate, there has been no consistency in the prosecution of corporate criminals, as compared with drug war policies of the past couple of decades (Hansen, 2009).

The deterrence model of crime prevention rests on the assumption and potential offenders respond to the costs and benefits of crime. Individuals weigh costs and benefits when deciding whether or not to commit a crime, and they choose crime when it pays (Siponen and Vance, 2010). In the model, a criminal rationally maximizes his expected utility. Criminal act causes harm to third parties with certainty, and the offender faces an uncertain punishment. The decision to engage in criminal activity depends on the magnitude of the expected gain from committing the act relative to the expected punishment. If the expected utility exceeds the expected sanction, the individual commits the criminal act (Levitt and Miles, 2007).

The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) is a resource centre for the police and the prosecuting authorities in combating these types of crime. Økokrim was established in 1989, and is both a police specialist agency and a public prosecutor's office with national authority. Most of Økokrim's resources are devoted to working on specific criminal cases. The formal rules for Økokrim can be found in chapter 35 of the Prosecution Instructions. Økokrim's main objective is to combat economic crime, environmental crime and laundering of proceeds of crime. Økokrim has approximately 136 employees. Deterrence is one of their objectives (Økokrim, 2008). Though their work on specific criminal cases, they attempt to demonstrate to the public that anyone breaking the rules in the financial and computer area of jurisdiction will be liable to penalties.

Yusuf and Babalola (2009) applied deterrence theory to suggest control strategy for insurance fraud. Deterrence theory postulates that people commit financial crime on the basis of rational calculations about perceived personal benefits, and that the threat of legal sanctions (along with, as mentioned, severity and swiftness of offender punishment) will deter people for fear of punishment. The theoretical literature on insurance fraud has identified two strategic approaches of deterrence: contracting and auditing. Thus, a strategy should focus on these two elements:

- *Deterrence through contract design*. Firstly, a contract should be design in a way that makes it optimal for all actors to tell the truth. Since the premium paid by an individual is directly related to the features of a contract chosen, optimal insurance coverage involves balancing the effects of additional premium against the effect of additional coverage. Next, a contract should be designed in a way that minimizes audit costs. Third, a contract design should criminalizes fraudulent behaviors and entail penalty award against a fraudulent party. Finally, the moral hazard/crime approach proposes a contract design that entails penalty for engaging in fraudulent claiming against the opportunistic insured.

- *Deterrence through auditing*. Insurance claims that have observable characteristics that are associated with a potential for fraud, should be thoroughly audited. Then, those insurance claims that are found to be invalid, should be denied. Otherwise auditing may be ineffective as deterrence. Knowledge management should be introduced at this stage in terms of a hybrid knowledge- and statistics-based system, which uses knowledge discovery techniques. First, the system integrates expert knowledge with statistical information assessment to identify cases of unusual provider behavior. Next, the system uses machine learning to develop new rules and improve identification processes.

Employee information systems security violations and crime is a serious problem that has been studied by deterrence theory. It is assumed that detection and punishment of violators reduces computer abuse. It is expected that the use of information systems security deterrents result in a decreased incidence of computer crime by employees (Siponen and Vance, 2010).

4.4 Neutralization Theory

Potential criminals apply five techniques of neutralization: denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties. This is the original formulation of neutralization theory. Later, the metaphor of the ledger and the technique of necessary defense were added. The metaphor of the ledger uses the idea of compensating bad acts with good acts (Siponen and Vance, 2010).

According to Heath (2008), white-collar criminals tend to apply techniques of neutralization used by offenders to deny the criminality of their actions. Examples of neutralization techniques are (a) denial of responsibility, (b) denial of injury, (c) denial of the victim, (d) condemnation of the condemners, (e) appeal to higher loyalties, (f) everyone else is doing it, and (g) claim to entitlement. The offender may claim an entitlement to act as he did, either because he was subject to a moral obligation, or because of some misdeed perpetrated by the victim. These excuses are applied both for occupational crime and for corporate crime at both the rotten apple level and the rotten barrel level.

Siponen and Vance (2010) describe the five basic techniques as follows:

1. *Denial of responsibility* implies that a person committing a deviant act defines himself as lacking responsibility for his actions. The person rationalizes that the action in question is beyond his control. The deviant views himself as a ball helplessly kicked through different situations.

2. *Denial of injury* implies that the person is justifying an action by minimizing the harm it causes. Individuals who perpetrate computer crime may deny injury to victimized parties by claiming that attacking a computer does not do any harm to people.

3. *Defense of necessity* implies that rule breaking is viewed as necessary, and thus one should not feel guilty when committing the action. In this way, the offender can put aside feelings of guilt by believing that an act was necessary and there was no other choice. In computer crime, employees may claim that they do not have time to comply with the policies owing to tight deadlines.

4. *Condemnation of the condemners* implies that neutralization is achieved by blaming those who are the target of the action. For example, one may break the law because the law is unreasonable, or one may break information systems security policies that are unreasonable. Offenders engaged in computer crime can claim that the law is unjust.

5. *Appeal to higher loyalties* implies a dilemma that must be resolved at the cost of violating a law or policy. In an organizational context, an employee may appeal to organizational values or hierarchies. For example, an employee might argue that he must violate a policy in order to get his work done.

Computer crime protection is challenged by neutralization theory. There is a need for techniques that can inhibit neutralization. Siponen and Vance (2010) suggest that adequate explanation to justify the organizational policy through seminars, victim-offender mediation, and persuasive discussion can be useful means to change behavior. With respect to denial of injury, victim-offender mediations or persuasive discussion make offenders realize that there is an injury. With respect to denial of responsibility, supervisors in one-on-one interactions and speakers in company seminars need to stress that there is no excuse for computer crime. Regarding the defense of necessity, managers should emphasize to employees that even when they are under the pressure of a tight deadline there is no excuse to use a criminal shortcut. With respect to the appeal to higher loyalties, security managers at organizations need to ensure that team leaders and line managers do not support their subordinates in violating information systems security policies in order to get their job done.

Neutralization techniques can be found in all kinds of computer crimes including online child grooming. For example D'Ovidio et al. (2009) studied neutralization techniques that are used to promote, advocate, and convey information in support of sexual relationships between adults and children. Techniques of neutralization included appeal to higher loyalties, condemnation of the condemners, and denial of injury. Many of the adult-child websites studied appealed to higher loyalties to gain acceptance for their actions by linking to websites of social movements not tied to pedophilia activism or causes supporting sexual relationships between adults and children.

In a study of music piracy, Higgins et al. (2008) found a link between the extent of piracy and the extent of neutralization. The level and changes in neutralization by an individual was found to have a direct influence on the level and change in music piracy by that individual over time. Stronger neutralization caused more music piracy. In order to reduce instances of music piracy, the manner in which individuals perceive their own behavior is the key to reducing instances. If the illegality of this behavior is reinforced to youth before participation in this behavior, the likelihood that they will participate in music piracy, especially on a frequent and regular basis, should be diminished.

In a study by Moore and McMullan (2009), five more neutralization techniques were added:

6. *Ledger technique* is used when an individual argues that his or her inappropriate behavior is at times acceptable because the person has spent most of his or her time doing good and legal deeds. The person develops a reserve of good deeds that overshadow the one bad deed.

7. *Denial of necessity of law* argues that the law was the result of the larger society's attempts to regulate behavior that had nothing to do with the greater good of people. As a result, the law was deemed inappropriate and not worth obedience.

8. *Everybody else is doing it*, which implies that the individual feels that there is so much disrespect for a law that the general consensus is such that the law is nullified or deemed to be unimportant.

9. *Entitlement technique* is used by individuals who feel that they are entitled to engage in an activity because of some consideration in their life.

10. *Defense of necessity* is used when the individual finds the act necessary in order to prevent an even greater delinquent act from taking place.

An individual applies techniques of neutralization when there is doubt that there is something wrong with his or her behavior. If there is no guilt to neutralize then it stands to reason that there is no need for neutralization techniques (Moore and McMullan, 2009).

4.5 Regulation and Response

Computer crime is not as visible as conventional crime and detection is difficult. For instance, in a homicide case, there is generally a body and forensic evidence. In the case of financial crime, Hansen (2009) argues that accounting and computer forensics are currently the investigators best tools in detection and implemented in most white-collar investigations in recent years. Applications of science and technology to white-collar crime cases is increasing, and advances in technology have led to a greater dependence on expert testimony in white-collar crime cases, keeping in mind that expert opinion cannot be given with absolute certainty.

Perhaps, Hansen (2009) argues, due to the financial resources to defend their cases available to elite individuals and corporations who are brought to justice, plus aversion to negative publicity, plea bargaining prior to charges is more intense as compared to that in conventional crime cases. Formal charging is more likely to be viewed as a failure by prosecutors, because of the larger number of resources that prosecutors have to be diverted to prosecute white-collar crime cases. Also due to the greater stigma attached to jail or prison time for elites, they may be reluctant to negotiate a plea bargain if incarceration is included in the deal. On the other hand, it is not unusual for convicted defendants to suddenly decide to cooperate in investigations in order to receive leniency at sentencing.

4.6 Criminal Justice Response

When prosecuting corruption and organized criminal groups engaged in labour-management racketeering, the United States Department of Justice is searching new ways of thinking about old crimes. Toner (2009) describes how criminal prosecutors in the USA have expanded the reach of federal statutes punishing fraud and extortion to combat the influence of organized criminal groups in certain American labour unions and employee benefit plans. Prosecutors have used fraud and extortion offences in novel ways on a case-by-case basis to prosecute labour-management corruption in the USA. By diligently persuading trial judges, appellate courts, and the US Congress of the merit of looking at fraud and extortion in new ways, federal prosecutors have carried out the intent of the statutory laws, which Congress enacted to deal with corruption in government, business, and labour unions.

Financial crime such as tax fraud can be carried out by hiding income in low-tax countries. The US income tax law, however, is such that it has the audacity to tax US citizens and residents on their worldwide income. This has the effect of making the US income tax international in scope and presents a peculiar challenge for those charged with enforcing the law, in particular, how to get information on foreign bank accounts. Cihlar (2009) found that the courts of the USA in appropriate circumstances are not reluctant to order a foreign bank with a presence in the USA to produce account information and other records maintained abroad.

Similar issues as discussed by Cihlar (2009) in the USA have emerged in the UK. The issue is whether and how the prosecution of multi-jurisdictional financial crime in the electronic age should be handled. Historically, British courts strongly advocated the territoriality principle to strictly limit the assumption of criminal jurisdiction to crime that occurred entirely within the jurisdiction. With the rapid advance of information and communication technologies as well as transnational crime, such a narrow approach to jurisdiction became unworkable, as more and more of all financial crime have multi-jurisdictional aspects (Hodgson, 2008).

Hodgson (2008) argues that that unless consistent and rational manner of prioritizing the claims of competing jurisdictions over the same criminal conduct is adopted, there is a risk that the first jurisdiction to be in a position to make an arrest may not necessarily be the correct or most appropriate one. He argues that when dealing with transnational offences, law enforcement agencies should strive to coordinate effort amongst them selves to ensure that criminal proceedings in different jurisdictions are brought in the most beneficial sequence or order.

Criminal justice response to cyber crime includes cyber crime policing units. Hinduja (2009) quantified the number of such US units that are on the world wide web and described the manner in which they represent themselves. The findings suggest that though cyber crime units across the USA typically have similar missions (e.g., to respond to one or more forms of computer crime), they used their self-representing web site in different ways to communicate information to their constituency.

The first dedicated anti-fraud unit of the European Commission was established in 1988. Quirke (2007) examined how the more recent anti-fraud unit in the EU is cooperating with member states and how it accounted for its actions. The study found that the fight against fraud was fatally undermined by the high degree of fragmentation due to the multiplicity of national and EU agencies involved.

4.7 Regulation

Fletcher (2007) examined the challenges to regulating financial fraud in cyberspace. He studied those responsible for the fraud, the possibility of prosecution, and the position of cyberspace in the light of jurisdiction and control. Issues such as; who is responsible for online fraud, can enough evidence be gathered to prosecute those who commit financial fraud in cyberspace, is cyberspace its own jurisdiction and who controls it; these are important perspectives.

Fletcher (2007) found that the introduction of internet specific regulation will be useful in combating cyberspace fraud. What is needed is a specific transnational program to deal with cyber crime based on its characteristics and limited to the steps needed to address identified weaknesses.

Larsson (2006) studied developments in the regulation of economic crime in Norway. The methodology of his study was qualitative expert interviews and analysis of a wide range of publications on the work of these authorities. He found that there has been a substantial growth in the resources, laws and regulations that goes into the regulation of economic crime for the last two decades in Norway. There has been a shift in regulation from general agreements and incentives by the state towards a market-based regulation backed by the threat of penal and civil sanctions. Segments of the economy have gone from being conceived as a producer of value to being a crime scene.

Regulation and prevention of elite corporate crime tends to be reactive rather than prophylactic in nature. Additionally, opportunities for crime appear to rise as regulation declines. After the 1980s insider trading scandals, the Securities and Exchange Commission (SEC) adopted a rule prohibiting insiders of bidder and target companies from divulging information or trading based on mergers and acquisitions or arbitrage negotiations. Likewise, the Sarbanes-Oxley Law of 2002 came into being after the Enron and WorldCom debacles (Hansen, 2009).

In more recent years when executives have been seen arrested and handcuffed for the purposes of public humiliation, it sets in motion a deterrence model of crime prevention or at the very least, a shaming policy. The purpose of these public arrests are often symbolic and say more about the regulatory agencies need to appear to be legitimately prosecuting corporate wrongdoers. As such, with regulation so closely tied to the political climate, there has been no consistency in the prosecution of corporate criminals, as compared with drug war policies of the past couple of decades (Hansen, 2009).

The deterrence model of crime prevention rests on the assumption and potential offenders respond to the costs and benefits of crime. In the model, a criminal rationally maximizes his expected utility. A criminal act causes harm to third parties with certainty, and the offender faces an uncertain punishment. The decision to engage in criminal activity depends on the magnitude of the expected gain from committing the act relative to the expected punishment. If the expected utility exceeds the expected sanction, the individual commits the criminal act (Levitt and Miles, 2007).

Araujo (2009) developed a model to study an incentive-based approach to fraud prevention in companies. The theory of incentives was applied to design a mechanism that makes employees reveal their true type, that is, their willingness or ability to combat corruption. The mechanism design approach used in the study assumes that the manger or the principal is entrusted with the power of making the employees agents.

Regulation played a major role in the waves of white-collar crime that have struck many developed economies. During the 1980s, deregulation in many countries led to creative financial schemes, some legitimate, but others clearly criminal. Insider trading was rarely investigated or prosecuted by regulatory agencies, even though it was and is illegal. Deregulation is viewed as a culprit in allowing bad accounting practices, including the practice of hiding losses or debts, as in the case of Enron, as well as overstating profits and assets. By re-regulation in response to major corporate crimes, it is like closing the barn door after the sheep have all escaped. It is a difficult task to rein in malfeasance, particularly if the monetary reward continues to outweigh sanctions (Hansen, 2009).

According to Hansen (2009), self-regulation does not appear to be a solution either. Much of evaluation, either by external groups or internally, is ceremonial. For example, managers at a technology company may only have a rudimentary knowledge of chemistry, biology or computers, but employ technological experts to do the core work of the company. In other examples, there is a conflict of interest, as in the case of Arthur Andersen who served as both auditor and paid consultant to Enron. In addition, certifiable standards have not proven to be successful. One reason is the frequent disconnect between certification and consistent compliance.

Self-regulation in terms of private policing of economic crime does not appear to be a solution to Williams (2005) either. He identified five barriers to this kind of governance approach:

1. *Secrecy, low visibility and discretionary justice* lead to informal negotiations, easy termination, loose coupling between investigations and formal legal frameworks, and potential privileges for some individuals but not others.

2. *Multiple legal standards and forum shopping* lead to legal and procedural standards that tend to vary on a case-by-case basis depending on the specific legal avenue or forum that is selected.

3. *Multiple legal actors* with distinct credentials and qualifications apply a variety of different professional and quasi-professional codes, standards and obligations.

4. *Multiple stakeholders and interest groups* tend to have conflicts of interest. However, to speak of accountability and governance, one is inevitably required to adopt a particular point of view.

5. *Public-private dichotomy* leads to a liberal legal tradition, where the distinction between public and private remains an enduring feature of legal thought. It hinges on two related principles that bear directly on the activities of internal investigators. The first is that corporations enjoy the same legal rights as individuals and are thus defined as private legal actors. The second is that there are fundamental limits to the authority and jurisdiction of the state that preclude unnecessary interventions and incursions into the private realm.

Similar to both Hansen (2009) and Williams (2005), Schneider (2006) studied privatizing economic crime enforcement by exploring the role of private sector investigative agencies. A financial investigate agency refers to an accounting-based, private sector organization that provides investigative, risk management, consulting and litigation support services addressing economic crime.

A special kind of self-regulation is self-protection, where protection potentially is achieved by educating actors. An example is investor protection by weaknesses of initial public offerings (IPO). Solaiman (2009) argues that it is generally understood that investment knowledge empowers investors to protect them selves from the culpability of issuers, their professionals and intermediaries who are called gatekeepers. Investors' ability to make prudent investment judgments for allocation of resources is regarded as an important element in every market economy.

In addition to self-protection, Solaiman (2009) argues there is a need for regulators in protecting investors. Investor protection by securities regulators can be divided into two: indirect and direct protection. The former refers to empowering the investors to protect themselves, whilst the latter concerns protection by regulator through making, administering and enforcing

Private policing of financial crime will have to build on organizational justice as perceived by organizational members. Scott et al. (2009) find that a quarter century of research on organizational justice has revealed a great deal about how employees react to justice rule adherence and violation on the part of their managers. Employees evaluate justice along a number of dimensions: fairness of decision outcomes, fairness of decision-making processes, adequacy of explanations, and perceived sensitivity of interpersonal communication.

These dimensions are part of what Rodell and Colquitt (2009) call anticipatory justice: distributive justice, procedural justice, informational justice, and interpersonal justice. The effects of anticipatory justice have been explored in the context of organizational change. Change is a natural component of employees' working lives, and employees may experience a variety of changes during their organizational tenure, ranging from large-scale changes such as organizational relocations or mergers, to new policies such as fringe benefit bans.

As part of anticipatory justice, Zapata-Phelan et al. (2009) studied procedural justice and intrinsic motivation among employees. What stands out most from the results of their study is the significant relationship between procedural justice and intrinsic motivation. The relationship was supported using a self-report measure as well as reference motivation to both specific tasks and multifaceted tasks in terms of overall job duties. Such relationships will tend to influence the role and performance of financial investigative agencies.

Schneider (2006) recommends that public policies and programs be developed that nurture an increased and more formal role for financial investigative agencies within the context of a partnership with government agencies. In Norway, a public debate in the media indicated that the role of financial investigative agencies should be reduced and more resources should be made available to the police (DN, 2008).

Hansen (2009) argues that prevention of corporate crime should not be only the concern of regulatory and law enforcement agencies. Corporations stand to lose more than reputation when financial scandals occur. Even when white-collar crime does not reach Royal Bank of Scotland, Enron or WorldCom proportions, corporations are damaged. It is estimated that white-collar crime can cost companies on average six percent of annual sales.

There have been several attempts at preventing corporate crime by re-regulation, and the Sarbanes-Oxley Law of 2002 in the US has been one attempt to rectify some of the corporate governance issues that came to light with Enron. The law requires more stringent accounting to the SEC, as well as preventing top management (CEOs, presidents, etc.) to claim plausible deniability due to ignorance of accounting practices within their firms. Unfortunately, this does not prevent fraudulent reporting to the SEC or to shareholders, but holds managers directly responsible for the misdeeds of their accounting staff if caught (Hansen, 2009: 33):

> Additionally, the prevention of corporate and elite crime is doomed to fail if regulation is the only applied solution. Business practices do not happen in an environment of strict regulation. Rather they are largely messy and unregulated with less predictable outcomes. Yet industries complain of being over-regulated, with the government intervening (abet with limited resources and support) only when the financial well being and safety of workers, consumers, and the public are brought into question.

Also, when examining the deviance of organizations themselves, rather than individuals, there is often a fine line between what is criminal and what is not. Hansen (2009) finds that even with increased regulation and prosecution of corporate offences such as income tax evasion and false inventory values, as well as stiff penalties for the violation of employee rights and safety, it is no surprise that individuals within organizations find it difficult to discern between unethical and the illegal. Many individual and corporate offences take years to be discovered, as demonstrated by the insider trading scandals of Wall Street in the 1980s, as well as more recent Enron scandal. When whistle blowers do come forward, it is many times well after the fact, when they have left the organization and have established themselves in other corporations or careers.

Corporate crimes are difficult to detect, due to elaborate conspiracies in the form of social networks. Individuals within organizations do not necessarily operate solo in their commission of crime. Just as criminal activities such as drug trafficking, racketeering, prostitution, and gambling operate within crime networks, elite economic crime occurs within the confines of complex social relations. These elite networks are not restricted to members of the business community, but extend them selves to include politicians and law enforcement officials (Hansen, 2009).

Some businessmen who operate a presumably legitimate and wholly legal enterprise are involved either overtly or covertly in criminal activities. Some businessmen are the financiers behind criminal operations. Enforcement and sanction become problematic, when politicians and regulatory agencies are either actively co-conspiring or turning a blind eye to illegal activity (Hansen, 2009).

When corporations and individuals are "caught in the act" and must account for their criminal behaviour, they have greater financial means to fight charges of misconduct and criminality than the common criminal offender. Punishment does not follow a predictable pattern of retribution or rehabilitation. Even civil settlements fall far short of true reimbursement. This is, according to Hansen (2009), largely due to the inequalities that exist within society itself, where social regulation both reflects and reproduces inequalities in the political economy generally and in the social structure of business organizations especially. It suggests that business defendants generally experience advantages at law not available to conventional crime defendants. This is sometimes called the "dirty secret of crime": what worries the average citizen the most are violent street crimes that are products of poverty, unemployment, etc. while corporations with entourages of lawyers, accountants and public relations experts negotiate around regulations and law because law enforcement officials, investigators, judges and prosecutors are soft on crimes committed by the elite.

Three solutions for controlling corporate and white-collar crime (Hansen, 2009):

1. Voluntary change in both corporate attitudes and structure. Professionals should be held accountable to their various professional groups, such as doctors, lawyers, and other professions. Another deterrent to corporate crime is the social, rather than legal consequences of criminal activities. Because elite criminals are just that - elite - their social identity is institutionalized in the social strata they occupy and the impact of the prison term is intensified. In other words, the bigger they are, the harder they fall. There is some belief that informal sanctions (i.e. expulsion from professional community) in conjunction with fear of formal punishment prevents most individuals from committing crimes. However, unlike their street crime counterparts, white-collar criminals rarely receive long prison sentences.

2. Strong intervention of the political state to force changes in corporate structure

3. Legal measures to deter or to punish or consumer actions (hurting corporation in the pocketbook may be the only way to get their attention).

International organizations such as the IMF and the World Bank approach corruption and other economic crimes by paying attention to donors, nongovernmental organizations, and governments and citizens especially in developing countries, where corruption threatens to undermine grassroots support for foreign assistance. The approach has four aims (Ksenia, 2008): preventing fraud and corruption within bank-financed projects, helping countries that request bank support in their efforts to reduce corruption, taking corruption more explicitly into account in country assistance strategies, and supporting international efforts to reduce corruption.

Kayrak (2008) argues that corruption should be dealt with in an all-around approach involving all efforts to deter it owing to the fact that it is a multidimensional phenomenon. He presents the theoretical framework for involvement of supreme audit institutions (SAIs in anti-corruption struggle and their contributions in practice. SAIs are watchdog agencies that carry out external audit of expenditures, incomes and assets of all government institutions in general. SAIs are regarded as prominent figures to ensure public sector transparency and accountability.

Button and Brooks (2009) studied progress towards developing anti-fraud culture strategies in UK central government bodies. They found a number of central public bodies with limited anti-fraud culture strategies. The main elements for deterring and preventing fraud according to such a strategy is to: (i) create an anti-fraud culture, (ii) gain the support of the public, (iii) get the message to fraudsters that they will be caught, (iv) fraud proof new programs, (v) comply with existing controls, and (vi) strengthen controls in response to emerging threats.

Michel (2008) argues there is a constant challenge of seeking effective prevention solutions against financial crime. Similarly, Jayasuriya (2008) states that successes have been few and far between. Success in the fight against financial crimes must involve partnership, training, education, proper market design and public awareness.

To be successful in auditing, Dion (2009) suggests that an auditor must understand the organizational culture. If an auditor understands the culture, then the auditor can better understand where, when, how and why fraud or any other financial crime has been committed. The new auditing paradigm includes four steps:

1. The analysis of the organizational culture: competition versus cooperation, closed versus open, personnel turnover and its motives, management control or empowerment, etc.

2. The analysis of the industry: profitable or non-profitable enterprises, market growth or saturation, moral image of the industry, etc.

3. The expertise of consultant in organizational behaviour: weaknesses and threats in the organization that encourage fraud and other kinds of financial crime

4. The analysis of the risk control system: bureaucracy or knowledge organization.

Competitors as well as customers influence the firm's cost structure. Defining and responding to customers' needs, striving for profits, and reacting to competitors are ethical corporate decisions and actions insofar as we look at the enterprise as a moral agent (Dion, 2009).

4.8 Financial Regulation

Spalek (2004: 173) raised some important concerns about the nature of financial regulation in Britain and its impact on investors and the victims of financial crime:

> Essentially, an actuarial regime operates whereby the risks associated with financial crime and mismanagement are foisted onto the shoulders of individual consumers. The notion of 'free choice' and the myth of the victim as 'duped investor' are perpetuated by the Financial Services Authority.

This means that the regulatory framework views investors as being able to freely choose whether or not to invest in a particular product and institution, and that, moreover, individuals who become the victims of financial crime have been conned as a result of them having insufficient knowledge about the financial system and the risks that it carries.

Organized and Financial Crime Unit in the UK is responsible for developing the government's strategy against organized crime. This unit also oversees the recovery of criminal assets, and the detection and conviction of money launderers.

The unit's objectives include:

- improving the strategic picture on the threat from organized crime
- working with the Organized Crime Strategy Group develop a strategy to fight organized crime
- ensuring that agencies and forces are given a clear steer on the priorities for combating organized crime, and designing effective strategies
- ensuring that agencies and forces are able to generate, share and assess tactical intelligence effectively
- giving forces and agencies the tools they need to carry out successful operations against organized crime
- sponsorship of the Serious Organized Crime Agency (SOCA)

The Financial Crime Team is part of the government's effort to improve the criminal justice system's ability to trace and recover the proceeds of crime, and to prevent, detect and penalize money launderers. Its key tasks include:

- implementing the Proceeds of Crime Act 2002
- implementing the Asset Recovery Strategy and monitoring it through the Asset Recovery Committee
- operating the Recovered Assets Fund

In asset recovery investigations, the financially related, personal information is often the raw material. Therefore, Kennedy (2007) argues that collecting, sharing, and analyzing information in asset recovery investigations is all about winning the information wars. Criminals will utilize weaknesses by placing criminal assets where information in respect of those assets cannot easily be obtained by prosecutors. If asset recovery is to be successful, it is essential that investigators are able to collect critical information from unavailable sources rather than irrelevant information from accessible sources. This may be part of an anti-corruption strategy (Witten and Koffer, 2009).

The financial sector is critical for the effectiveness of the fight against organized crime, corruption and terrorism financing. Hardouin (2009) suggested principles of governance of the sector in terms of two channels. One is the general organization and regulation of the sector. Governance depends on a framework defined by the regulator. The other channel is corporate responsibility.

Also the legal sector is critical in the fight against financial crime. In Canada, lawyers are being imposed stringent anti-criminal finance regulatory obligations. However, Gallant (2009) argues that the tasking of Canadian lawyers with anti-money laundering and anti-terrorist finance obligations is a project fraught with uncertainty. This is because it is not clear that the strategy of pursuing criminal finance, the underlying reason for the conscripting of lawyers into the war on criminal finance, works to deter crime.

Sathye (2008) estimated the cost of compliance with anti-laundering legislation and found that the legislation brings substantial financial regulatory burden on the financial institutions in Australia.

The 2003 revised 40 recommendations of the Financial Action Task Force in the UK allows a region or nation to implement a risk-based approach in relation to key elements of their anti-money laundering and combating of financing terrorists. A risk-based approach involves the development of appropriate risk control measures based on a process of identification and categorization of risk (Koker, 2009).

Koker (2009) studied FATF's risk-based guidance to combat money laundering and terrorist financing to determine its approach to the identification and management of low-risk providers, products and transactions. He analysed the relevant FATF recommendations and its guidance notes and reflected on key questions for regulators and financial institutions. He concludes that it seems advisable for the FATF to provide a clearer and principled conceptual framework for the management of risk, but to refrain from identifying examples and indicators, especially of low-risk products and transactions, unless they are truly universal or correctly contextualized.

Risk-based regulation refers to the tailoring of rules to focus on instances of higher risk. Risk-based supervision is an approach where the supervisor focuses on risk as posed and managed by regulated entities and allocates supervisory resources on the basis of their risk profiles (Koker, 2009: 334):

> A risk-based approach generally leads supervisors to devote less attention to entities that pose a lower risk and rather focus their attention and resources on those posing a higher risk.

Regulated entities that follow a risk-based approach to anti-money laundering compliance tailor their control measures to fit the risk profiles of their different products and clients. The main benefit is an appropriate and efficient allocation of resources.

4.9 Cyber Security

Gallaher et al. (2008) define organizations' cyber security investment strategies in terms of two alternatives. One approach is to identify security needs and priorities, and is referred to as determining a targeted level of security. This implies deciding on the best or optimal level of security for an organization, given other spending priorities, regulations, and data sensitivity and privacy risks. Another approach is to determine the level or share of resources an organization should or might invest in cyber security. This implies that cyber security activities and purchases are determined, within a budget constraint, to maximize security.

4.10 Shari'ah Perspective

Personal, professional and business life is governed under Islam by a tradition of moral standards, ethics, values and norms of behaviour. Property is strongly protected in Islamic law (Al-Kashif, 2009: 86):

> Preserving property is one of the main five objectives, which Shari'ah has been revealed to preserve. The other four are the religion, life, intellect, and honour. These five basic and universal values presented as necessities or priorities on which the lives of people depend, and whose neglect leads to total disruption and chaos. It is unlawful for a person to abuse his own wealth, or abuse the wealth of others.

Islamic criminal law divides punishable acts into three categories: (i) crimes punishable according to the Qur'an, (ii) crimes involving wrongs against individuals, and (iii) crimes demanding restitution. Most financial crimes belong to the third category, such as fraud, bribery, and the forgery of documents. In the third category, Islamic judges enjoy flexibility to punish the offender in almost any fashion. An emphasis is placed on the societal and public interest when criminals in this category are convicted (Al-Kashif, 2009).

Islamic law emphasizes honest dealing among individuals and organizations. The Qu'ran is strict in making the point that traders and businesses that indulge in fraud are committing a sin in the eye of Allah. Allah says (Al-Kashif, 2009: 90):

1. "Woe to those that deal in fraud.
2. Those who, when they have to receive by measure from men, exact full measure.
3. But when they have to give by measure or weight to men, give less than due.
4. Do they not think that they will be called to account?
5. On a mighty day.
6. A day when all mankind will stand before the Lord of the Worlds?"

Similarly, Islamic law is strict upon bribery and corruption. Islam prohibits the Muslim to approach the officials of a government or their subordinates for the purpose of offering them a bribe; it has prohibited the latter to accept it; and it has prohibited that any third person should arrange matters between the givers and the takers of the bribe since Allah cursed the one who offers the bribe, the one who receives it and the one who arranges it, since Allah says (Al-Kashif, 2009: 90):

> And do not consume your property among yourself wrongfully, nor seek access to judges by means of it in order that you may sinfully consume a portion of peoples' wealth, while you know what you do.

4.11 Protecting Information Resources

Organizations have an array of tools and technologies for protecting their electronic information. They include methods for securing systems and data, ensuring system control and system quality (Laudon and Laudon, 2010: 348):

- *Access control* consists of the procedures an organization uses to prevent improper access to systems by unauthorized insiders and outsiders. To gain access a user must be authorized and authenticated. Authentication refers to the ability to know that a person is who he or she claims to be.

- *Firewall* is a combination of hardware and software that controls the flow of incoming and outgoing network traffic.

- *Intrusion detection system* features full-time monitoring tools placed at the most vulnerable points of organizational computing.

- *Antivirus software* is designed to check computer systems and drives for the presence of computer viruses.

- *Encryption* is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver.

- *Digital certificate* is a data file used to establish the identity of users and electronic assets for protection of online transactions.

- *System audit* examines the organization's overall security environment as well as controls governing individual information systems.

In addition to implementing effective security and controls both externally and internally, organizations can improve system reliability and prevent information theft by employing software metrics and rigorous software testing (Laudon and Laudon, 2010).

4.12 The Case of Chinese Securities Commission

China has criminalized insider trading via legislation and has a national regulation and enforcement regime performed by the Chinese Securities Regulatory Commission. The stock market in China has experienced tremendous growth and development in the last decade. A major finding of a study by Cheng (2008) is the paucity of insider trading cases and the lack of convictions for insider trading offences in China.

A primary challenge in the insider trading regulation in China comes from the fact that most insider trading cases involve high-ranking government and party officials. The regulatory commission lacks the power to directly administer discipline and penalties on government officials and party cadres for insider trading offences.

There are primarily three means by which the Chinese Securities Regulatory Commission detects and becomes aware of insider trading activities (Cheng, 2008):

- Commission staff that are on the front lines of enforcement, search for illegal behavior through regular inspections or by scanning the financial news for clues.

- Complaints are received by the Civil Complaint Office of the State Council, which deals with various kinds of complaints in the country.

- There are referrals of investigations conducted by the Shanghai Stock Exchange and The Shenzhen Stock Exchange.

The stock exchanges have the responsibility of monitoring the day-to-day trading activities on their exchanges for violations. Shanghai Stock Exchange reported one year that four cases of illegalities including insider trading had been discovered during a survey of over 600 top executives of 54 listed companies.

5. Corporate Reputation

Computer crime causes harm to corporate reputation. For example, when a bank is involved in money laundering or not reporting suspicion of illegal financial activities, the reputation of that bank is seriously damaged. Damage to reputation will result in tangible losses being incurred. This is because reputation damage is often linked to, or is the result of, a perceived impairment in the bank's financial soundness (Harvey and Lau, 2009: 59):

The immediate manifestation of this is likely to be through the actions of depositors as they move to withdraw their funds, as well as from bank counterparties who withdraw lines of credit. Such actions ultimately translate into a withdrawal of shareholder support and subsequent negative impact on the share price.

For a bank, cost associated with compliance with anti-money laundering legislation is justified by the belief that non-compliance will damage reputation with a consequent loss of business, even if the involvement of the institution is unintentional.

5.1 Reputation Defined

Corporate reputation is an important asset or liability bestowed upon a corporation by its stakeholders (Love and Kraatz, 2009). Walker (2010) defined corporate reputation by making distinctions between organizational identity, organizational image and corporate reputation. Organizational identity is the most central, enduring, and distinctive basic character of an organization. Organizational image is outsider judgment based on perception of corporate communication. Corporate reputation represents what is actually known by both internal and external stakeholders. For example, stakeholders perceive a corporation to be corrupt or involved in other forms of white-collar crime.

Corporate reputation is a soft concept. It is the overall estimation and judgment of an organization that is held by its internal and external stakeholders based on the corporation’s past actions and expected future actions and behavior. There may be differences in reputation among stakeholders according to their experiences and preferences in dealing with the organization as well as their information obtained from others. Reputation is judgment about vices and virtues, strengths and weaknesses, that stakeholders accumulate, process and reprocess about someone. The circulation of reputational information seems essential to all social interaction, whether conducting a business, achieving recognition or identifying reliable others (Bovenkerk et al., 2003).

Corporate reputation is the collective judgment of a corporation, it is a set of characteristics that are attributed to a firm by stakeholders, and it is visible in the particular type of feedback, received by the organization from its stakeholders, concerning the credibility of the organization's identity claims. However, reactions by stakeholders in relation to a firm are not part of the reputation (Einwiller et al., 2010).

Corporate reputation is a perceptual representation of a company's past actions and future prospects that describe the firm's overall appeal to all its key constituents when compared to other leading rivals. Reputation is a combination of reality such as economic and social performance and perception such as performance perceived by key stakeholders (Hemphill, 2006).

Corporate reputation is a global and general, temporally stable, evaluative judgment about a corporation that is shared by multiple stakeholders. It is the net reaction of customers, investors, employees, and other stakeholders to the company. It is a collective of individual impressions (Highhouse et al., 2009). Similarly, Friedman (2009) defines corporate reputation as a relatively stable, long-term intangible corporate asset that is important for organizational competitiveness. It is a perceptual representation of a company's past actions and future prospects that describe the company's overall appeal to all its key constituents when compared to its rivals.

Three key attributes are emphasized in the definition of reputation: (1) reputation is based on perceptions; (2) it is the aggregate perception of all stakeholders; and (3) it is comparative. Furthermore, (4) reputation can be positive or negative; and (5) it is stable and enduring (Walker, 2010).

Awareness of the link between corporate reputation and white-collar crime has risen substantially in the business world after the joint collapse of Enron and Arthur Andersen. As a consequence, companies have become more sensitive to the value of their reputation. Corporate audiences, including institutional and individual investors, customers and suppliers, public authorities and competitors, evaluate the reputation of firms when making choices and other decisions (Linthicum et al., 2010).

The two main sources of the corporate reputation are experience and information – a person's or a group's past dealings with the company and the extent and nature of their direct and indirect communication with the company. It is argued that a favorable reputation requires not only an effective communication effort on the part of the corporation. More importantly, it requires an admirable identity that can be molded through consistent performance, usually over many years and even decades.

5.2 Resource-Based Theory

According to the resource-based view of the firm, corporate reputation can be considered to be valuable strategic resource that contributes to or harms a corporation's sustainable position (Keh and Xie, 2009). The central tenet in resource-based theory is that unique organizational resources of both tangible and intangible nature are the real source of competitive advantage. With resource-based theory, organizations are viewed as a collection of resources that are heterogeneously distributed within and across industries. Accordingly, what makes the performance of an organization distinctive is the unique blend of the resources it possesses.

Corporate reputation is an intangible resource that influences stakeholder behavior, including employees, management, customers and investors (Friedman, 2009). The resource-based view of the firm places specific emphasis on corporate intangibles that is difficult to imitate. Reputation is one corporate intangible thought to enhance customer satisfaction and loyalty, employee attraction and retention, firm equity, and investor awareness. It is also argued that reputation as a resource enhances bargaining power in trade channels, helps raise capital on the equity market, provides a second chance in the event of a crisis, provides access to the best professional service providers, facilitates new product introduction, and adds value such as trust to goods and services (Highhouse et al., 2009).

Corporate reputation as an intangible resource is both influenced by the extent of white-collar crime as well as influencing the extent of white-collar crime. Competitors that are involved in given value networks contribute to define how each enterprise in an industry can strive for profit. Dion (2009) argues that the capacity to convert corporate intangibles, such as corporate reputation, in a negotiable value could contribute to prevent corporate crime.

From a resource-based perspective, reputation is a valuable and rare resource that can lead to a sustained advantage or a temporary or permanent collapse. A good reputation is difficult to imitate and highly causally ambiguous. Walker (2010) argues that the greater the ambiguity experienced by constituents, the greater the importance of reputation as a resource as it reduces uncertainty by signaling, for example, service quality.

Although reputation is an intangible resource, it is argued that a good reputation consistently increases or sustains corporate worth and provides sustained competitive advantage. A business can achieve it objectives more easily if it has a good and consistent reputation among its stakeholders, especially key stakeholders such as its largest customers, opinion leaders in the business community, suppliers and current and potential employees.

5.3 Determinants of Corporate Reputation

In addition to white-collar crime, there are a number of other determinants of corporate reputation. For example, Highhouse et al. (2009: 1481) applied an organizational impression management perspective on the formation of corporate reputation by asking how reputation judgments are formed:

> What factors are considered? How can reputation judgments be influenced? These are questions that are appropriately addressed by behavioral science. Working from a view of reputation as a social construction - one that indicates the general, shared regard in which relevant constituents hold a company - we review literature that is relevant to the formation and foundation of corporate reputation.

Highhouse et al. (2009) applied a working definition of reputation as a collective of individual impression that necessitated a micro view of impression formation as a foundation for understanding corporate reputation. In their search for determinants of corporate reputation, the researchers distinguished between internal and external factors, where internal factors were separated into substantive and symbolic attributes. Substantive attributes that may harm reputation similar to white-collar crime are lack of social capital, lack of knowledge, lack of product development, and diversification with little substance. Symbolic attributes that may harm reputation similar to white-collar crime are failed advertising, misleading public relations and negative corporate social responsibility policy. External factors that may harm reputation similar to white-collar crime are negative word of mouth and negative media exposure.

In a different study, Friedman (2009) searched for determinants of corporate reputation within human resource management. He found that organizational value is lost when employee competencies and motivation deteriorate since this in turn negatively influence corporate reputation. He argues that effective implementation of the strategic partner, the change agent, the administrative expert and the employee champion human resources management roles can indirectly enhance corporate reputation.

Love and Kraatz (2009) focused only on downsizing as determinant of corporate reputation. The aim of their study was to illuminate reputational change processes and identify the underlying theoretical mechanisms. They found that downsizing exerted a strong, negative effect on reputation, consistently with the character explanation.

Resource-base theory can be applied to understand the role of news media as an influence on corporate reputation. Corporate reputation is influenced by news media when stakeholders are dependent on news media to learn about reputation dimensions of the company. If stakeholders learn directly from experience and observation, then news media are less important. This is in line with media system dependency theory, which proposes an integral relationship among audiences, the news media and the larger social and economic system. Dependency is defined as a relationship in which the satisfaction of needs or the attainment of goals by one party is contingent upon the resources of another party (Einwiller et al., 2010).

5.4 Effects of Corporate Reputation

According to Friedman (2009), corporate reputation is an intangible resource that influences stakeholder behavior, including employees, management, customers and investors. According to Highhouse et al. (2009), reputation is thought to enhance customer satisfaction and loyalty, employee attraction and retention, firm equity, and investor awareness. It is also argued that reputation as a resource enhances possibilities in a number of other aspects. According to Dion (2009), reputation can even prevent white-collar crime.

Keh and Xie (2009) studied how corporate reputation influences customer behavioral intentions. They proposed a model with customer trust, customer identification and customer commitment as the key intervening factors between corporate reputation and customer purchase intention and willingness to pay a price premium. They tested the model empirically and found that corporate reputation has positive influence on both customer trust and customer identification. Furthermore, customer commitment mediates the relationships between the two relational constructs (customer trust and customer identification) and behavioral intentions.

5.5 Theories of Corporate Reputation

In addition to resource-based theory, a number of other theories can be applied to examine corporate reputation. Examples include institutional theory, signaling theory, stakeholder theory, social identity theory, game theory, social cognition theory, economic theory, mass communication theory, impression management theory, and transaction cost theory (Walker, 2010).

To understand how the three most prominently used theoretical perspectives have been applied, Walker (2010) presented them as moving from pre-action, to action, and finally to post-action. With a focus on context and building reputation, institutional theory is often applied in a pre-action stage. The theory is used to examine how corporations gain legitimacy and cultural support within their institutional contexts to build their reputation.

At the action stage, signaling theory includes building images (signals), maintaining, and defending a reputation based on projected organizational images. The theory is applied to corporate reputation to explain how the strategic choices of firms represent signals, which are then used by stakeholders to form impressions of the firms. At the post-action stage, resource-based theory is applied to understand the outcome of a strong reputation. The theory examines how reputation is a valuable and rare resource that leads to a sustained competitive advantage (Walker, 2010).

The self-presentation theory suggests that corporations, like individuals, are concerned with the impression they create among stakeholders. According to Highhouse et al. (2009), there are two self-presentation motives of corporations: (a) desire for approval and (b) desire for status. Like individuals, corporations develop reputation based on their success at getting along with others and getting ahead of others. This socio-analytical perspective of personality focuses on external perceptions where the structure of organizational personality is found in the structure of perceptions.

5.6 Measurement of Corporate Reputation

A construct such as corporate reputation must have an empirical definition closely tied to construct definition. Therefore, measurement of corporate reputation should examine perceived reputation in terms of stakeholders' perceptions, not factual representation. The perceptual nature of the construct reputation is important to measure correctly. Furthermore, as argued by Weber (2010), corporate reputation is an issue-specific and aggregate perception. Reputation is an aggregate perception of all stakeholders. Thus, there are three important considerations for measuring corporate reputation, i.e. reputation for-what, reputation for-whom, and reputation to-whom.

Reputation is a relative construct that can be relative to reputation in the past, relative to competitors at present, or relative to a desired or acceptable reputation level. Measurement of corporate reputation should therefore permit the construct to be both positive and negative.

Since reputation is defined as a relative stable and enduring phenomenon, measurement must be applied accordingly. Weber (2010: 374) finds that this point provides some interesting implications for the measurement of corporate reputation:

> Although it is generally accepted that longitudinal research is more valuable than cross-sectional in the study of corporate reputation because research has demonstrated that it is stable, cross-sectional studies have relatively greater value as compared to similar studies examining other concepts. For example, given that organizational images are relatively short lived, generalized conclusions from cross-sectional studies examining this concept would be questionable. So, while longitudinal studies are preferred, more credence can be placed in the conclusions of cross-sectional studies examining corporate reputation than most other concepts.

A central theme in the reputation literature is the reasoning that stakeholders assign positive reputation to corporations that appear to possess desirable character traits. In this theme, stakeholders views organizations as coherent and purposive social entities rather than mere social aggregates or collectivities. Furthermore, constituencies are especially concerned with organizations' sustainability as partners. Therefore, stakeholders tend to admire corporations that appear to possess character traits such as trustworthiness and reliability (Love and Kraatz, 2009).

5.7 Rebuilding Corporate Reputation

Rebuilding corporate reputation involves both transparency and action. As argued by Bonini et al. (2009), reputation is built on a foundation not only of communications but also of deeds. Sharing information about critical business issues is important, and reputation-oriented actions such as willingness to tackle white-collar crime have to be convincing to stakeholders.

When a company responds to serious reputation threats from white-collar crime, the company must use many other means in addition to formal marketing and public relations. Such means of spreading positive messages about its activities quickly include people with high standing reinforce key strategic messages, interactive web sites, and credible third parties speaking for the company (Bonini et al., 2009).

Dowling (2006: 98) argues that corporate reputation is best communicated through stories, where good corporate stories and reputation are built on a solid platform of valued mission and good morality and behavior:

> This information should be crafted into a corporate reputation story sustainable for both internal and external stakeholders. Corporate reputation storytelling in its long forms (such as books, shareholder briefings, advertorials, web sites, and annual reports) and short forms (in corporate advertising) is art underpinned by science. The art of storytelling involves creating enough mystery and intimacy to result in a more favorable evaluation of the company.

Brønn and Vidaver-Cohen (2009) studied corporate motives for social initiative. They studied motives such as legitimacy, sustainability and bottom line for engaging in social initiatives. Of the four motives in the legitimacy factor applied, they found that the motives to improve image and to be recognized for moral leadership dominated the list. Furthermore, sustainability motives for social initiative were driven by personal managerial values, while profitability motives were driven by the belief that engaging in social initiatives can yield direct financial benefits for the firm, either by generating new revenues or by protecting existing profit levels.

5.8 Social Responsibility

In the three stage model of corporate social responsibility developed by Castello and Lozano (2009), corporate reputation is important as a fundamental requirement at the first stage. Stage 1 labeled risk management is a base stage where corporate social responsibility is seen as a tool to protect reputation value. Within risk management, firms start to develop systems to measure and control environmental and social issues and threats. These control systems involve the planning and social forecasting, preparing for social response and development of the first set of corporate social policies.

Corporate social responsibility is tightly linked to acceptable ethical behavior, since it represents the continuing commitment by business to behave ethically and contribute to economic development while improving the quality of life of the workforce as well as the community at large (Linthicum et al., 2010).

Linthicum et al. (2010) examined the influence of social responsibility on firm reputation during a period of crises. Specifically, they studied the influence of social responsibility ratings on market returns to Arthur Andersen clients following the Enron audit failure. Proponents of social responsibility argue that social responsibility can improve the reputation of the firm, while detractors argue that social responsibility expenditures are a poor use of shareholder money. Results from the study were inconsistent with claims that social responsibility can burnish a firm's reputation in a time of crises and with prior research indicating a positive relationship between social responsibility and market value. This is because the researchers found no evidence that social responsibility mitigated the negative returns to Arthur Andersen clients following the Enron audit failure. The researchers used a matched sample of Arthur Andersen and non-Arthur Andersen firms.

5.9 Corporate Governance Ratings

An influential factor on corporate reputation in a white-collar perspective is corporate governance rating. Corporate governance ratings can be based on categories such as board, audit, charter, executive compensation, and director education. Governance ratings can be generated from reviews of public and private corporate information as well as from interviews with top executives and independent trustees. Such ratings can be influential, for example, with investors on matters related to election of directors and executive compensation. Corporate governance scores also can influence credit rating services, and thereby directly impacting cost of capital (Abdolmohammadi and Read, 2010).

Abdolmohammadi and Read (2010) studied the relationship between corporate governance ratings and the incidence of financial restatement. They selected a sample of 150 US firms that restated their financial statements for 2003 to bring them into conformity with general accounting principles. The researchers found that the sample of restatements had significantly lower governance ratings than the control sample during the restated year of 2003. They also found that the sample of restatement firms improved their governance ratings in the year following the restated year, suggesting that financial restatement leads to improvements in governance mechanisms.

6. Knowledge Management

Prevention of computer crime and protection of corporate reputation require knowledge management. Knowledge management is a systematic and integrative process of coordinating organization-wide knowledge sharing and knowledge development to reach organizational goals such as improved corporate reputation. Knowledge management encompasses the managerial efforts in facilitating activities of acquiring, creating, storing, sharing, diffusing, developing, and deploying knowledge by individuals and groups. Knowledge management practices need to fit with organizational context in order to make a difference. Practices of knowledge management are context-specific, and they can influence organizational effectiveness (Zheng et al., 2010).

Zheng et al. (2010) studied the possible mediating role of knowledge management in the relationship between organizational culture, structure, strategy, and organizational effectiveness. Their results suggest that knowledge management fully mediates the impact of organizational culture on organizational effectiveness, and partially mediates the impact of organizational structure and strategy on organizational effectiveness.

Hinduja (2007) suggests that leveraging knowledge from the past to address the future will improve computer crime investigations. Cyber crime is requiring law enforcement departments in general and criminal investigators in particular to tailor a significant amount of their efforts toward successfully identifying, apprehending, and assisting in the successful investigation and prosecution of perpetrators.

6.1 Knowledge Organization

Knowledge is considered an important resource in most firms. The resource-based view of the firm posits that firm competitiveness comes from unique bundles of tangible and intangible assets that are valuable, rare, imperfectly imitable, non-substitutable, combinable and sustainable (Zheng et al., 2010).

Knowledge organization has emerged as the dominant structure of both public and private organizations in the transition from an industrial to a knowledge society (Lassen et al., 2006). Knowledge organization in the management sciences is concerned with structures within which knowledge workers solve knowledge problems (Bennet, 2005a, 2005b; Bergström et al., 2009; Lassen et al., 2006; Smith, 2003; Uretsky, 2001).

There are many definitions of knowledge. Nonaka et al. (2000) describe it as justified true belief. Definitions of organizational knowledge range from a complex, accumulated expertise that resides in individuals and is partly or largely inexpressible to a much more structured and explicit content. There are also several classifications of knowledge, e.g. far, explicit, embodied, encoded, embedded, event, procedural, and common. Knowledge has long been recognized as a valuable resource for the organizational growth and sustained competitive advantage, especially for organizations competing in uncertain environments. Recently, some researchers have argued that knowledge is an organization's most valuable resource because it represents intangible assets, operational routines, and creative processes that are hard to imitate (Wasko and Faraj, 2005). However, the effective management of knowledge is fundamental to the organization’s ability to create and sustain competitive advantage.

Knowledge management research has described organizational knowledge flows in terms of the knowledge circulation process, consisting of five components: knowledge creation, accumulation, sharing, utilization and internalization. Of these five parts, the knowledge sharing process is what this book focuses on. Knowledge sharing within and between organizations is not a one-way activity, but a process of trial and error, feedback, and mutual adjustment of both the source and the recipient of knowledge. This mutuality in the knowledge sharing suggests that the process can be constructed as a sequence of collective actions in which the source and the recipient are involved. There are many different knowledge-sharing mechanisms: it can be informal and personal as well as formal and impersonal. Informal mechanisms include talk, unscheduled meetings, electronic bulletin boards, and discussion databases. More formal knowledge sharing channels include video conferencing, training sessions, organizational intranets, and databases.

Bennet and Bennet (2005a) define knowledge organizations as complex adaptive systems composed of a large number of self-organizing components that seek to maximize their own goals but operate according to rules in the context of relationships with other components. In an intelligent complex adaptive system the agents are people. The systems (organizations) are frequently composed of hierarchical levels of self-organizing agents (or knowledge workers), which can take the forms of teams, divisions or other structures that have common bonds. Thus while the components (knowledge workers) are self-organizing, they are not independent from the system they comprise (the professional organization).

Knowledge is often referred to as information combined with interpretation, reflection, and context. In cybernetics, knowledge is defined as a reducer of complexity or as a relation to predict and to select those actions that are necessary in establishing a competitive advantage for organizational survival. That is, knowledge is the capability to draw distinctions, within a domain of actions (Laise et al., 2005). According to the knowledge-based view of the organization, the uniqueness of an organization's knowledge plays a fundamental role in its sustained ability to perform and succeed (Turner and Makhija, 2006).

According to the knowledge-based theory of the firm, knowledge is the main resource for a firm's competitive advantage. Knowledge is the primary driver of a firm's value. Performance differences across firms can be attributed to the variance in the firms' strategic knowledge. Strategic knowledge is characterized by being valuable, unique, rare, non-imitable, non-substitutable, non-transferable, combinable, and exploitable. Unlike other inert organizational resources, the application of existing knowledge has the potential to generate new knowledge (Garud and Kumaraswamy, 2005).

Inherently, however, knowledge resides within individuals and, more specifically in the employees who create, recognize, archive, access, and apply knowledge in carrying out their tasks (Liu and Chen, 2005). Consequently, the movement of knowledge across individual and organizational boundaries is dependent on employees' knowledge-sharing behaviors (Liebowitz, 2004). Bock et al. (2005) found that extensive knowledge sharing within organizations still appears to be the exception rather than the rule.

The knowledge organization is very different from the bureaucratic organization. For example, the knowledge organization's focus on flexibility and customer response is very different from the bureaucracy's focus on organizational stability and the accuracy and repetitiveness of internal processes. In the knowledge organization, current practices emphasize using the ideas and capabilities of employees to improve decision-making and organizational effectiveness. In contrast, bureaucracies utilize autocratic decision-making by senior leadership with unquestioned execution by the workforce (Bennet and Bennet, 2005b).

In knowledge organizations, transformational and charismatic leadership is an influential mode of leadership that is associated with high levels of individual and organizational performance. Leadership effectiveness is critically contingent on, and often defined in terms of, leaders' ability to motivate followers toward collective goals or a collective mission or vision. (Kark and Dijk, 2007).

In the knowledge society, knowledge organizations are expected to play a vital role in local economic development. For example, knowledge institutions such as universities are expected to stimulate regional and local economic development. Knowledge transfer units in universities such as Oxford in the UK and Grenoble in France are responsible for local and regional innovations (Smith, 2003).

Uretsky (2001) argues that the real knowledge organization is the learning organization. A learning organization is one that changes as a result of its experiences. Under the best of circumstances, these changes result in performance improvements. The phrases knowledge organization and learning organization are usually (but not necessarily) used to describe service organizations. This is because most, if not all, of the value of these organizations comes from how well their professionals learn from the environment, diagnose problems, and then work with clients or customers to improve their situations. The problems with which they work are frequently ambiguous and unstructured. The information, skills, and experience needed to address these problems vary with work cases. A typical example is detectives in police investigations of white-collar crime.

Similarly, Bennet and Bennet (2005b) argue that learning and knowledge will have become two of the three most important emergent characteristics of the future world-class organization. Learning will be continuous and widespread, utilizing mentoring, classroom, and distance learning and will likely be self-managed with strong infrastructure support. The creation, storage, transfer, and application of knowledge will have been refined and developed such that it becomes a major resource of the organization as it satisfies customers and adapts to environmental competitive forces and opportunities.

The third characteristic of future knowledge organizations will be that of organizational intelligence. Organizational intelligence is the ability of an organization to perceive, interpret and respond to its environment in a manner that meets its goals while satisfying multiple stakeholders. Intelligent behavior may be defined as being well prepared, providing excellent outcome oriented thinking, choosing appropriate postures, and making outstanding decisions. Intelligent behavior includes acquiring knowledge continuously from all available resources and building it into an integrated picture, bringing together seemingly unrelated information to create new and unusual perspectives and to understand the surrounding world (Bennet and Bennet, 2005b).

In the context of policing and law enforcement, 'intelligence' has another meaning as well. Brown (2007: 340) define intelligence in this context as follows:

> Intelligence is information, which is significant or potentially significant for an enquiry or potential enquiry.

What establishes information as intelligence is that it is a subset of information defined by the special quality of being significant and relevant. If information is significant, it has value and it has relevance. Analysis does not create intelligence; it merely discovers, attributes and refines it.

According to Bennet and Bennet (2005a), designing the knowledge organization of the future implies development of an intelligent complex adaptive system. In response to an environment of rapid change, increasing complexity and great uncertainty, the organization of the future must become an adaptive organic business. The intelligent complex adaptive system will enter into a symbiotic relationship with its cooperative enterprise, virtual alliances and external environment, while simultaneously retaining unity of purpose and effective identification and selection of incoming threats and opportunities.

In the knowledge organization, innovation and creativity are of critical importance. The literature on creativity provides a view of organizing for innovation by focusing on how individuals and teams come to shape knowledge in unique ways. Innovation consists of the creative generation of a new idea and the implementation of the idea into a valuable product, and thus creativity feeds innovation and is particularly critical in complex and interdependent work. Taylor and Greve (2006) argue that creativity can be viewed as the first stage of the overall innovation process.

Innovative solutions in the knowledge organization arise from diverse knowledge, processes that allow for creativity, and tasks directed toward creative solutions. Creativity requires application of deep knowledge because knowledge workers must understand the knowledge domain to push its boundaries. Team creativity likewise relies on tapping into the diverse knowledge of a team’s members (Taylor and Greve, 2006).

Within knowledge organizations, we often find communities of practice. Brown and Duguid (2001) argue that for a variety of reasons, communities of practice seem a useful organizational subset for examining organizational knowledge as well as identity. First, such communities are privileged sites for a tight, effective loop of insight, problem identification, learning, and knowledge production. Second, they are significant repositories for the development, maintenance, and reproduction of knowledge. Third, community knowledge is more than the sum of its parts. Fourth, organizational ability to adapt to environmental change is often determined by communities of practice.

6.2 Business Intelligence

While data are numbers and letters without meaning, information is data in a context that makes sense. Information combined with interpretation, reflection and context is knowledge, while knowledge accumulated over time as learning is wisdom. In this hierarchical structure we find intelligence as more than information, while less than knowledge. Intelligence is analyzed information. In police work, intelligence can provide the basis for opening a new criminal case, it can be applied to the investigation of existing criminal cases, it can be used to reallocate investigative resources based on new crime patterns and actors, and it can be used for preventive measures.

In the private sector, a term called “business intelligence” has received substantial attention in recent years. Although different from police intelligence, business intelligence has some interesting perspectives for police intelligence as well (Laudon and Laudon, 2010; Williams and Williams, 2003).

Business intelligence is a process of taking large amounts of data, analyzing that data, and presenting a high-level set of reports that condense the essence of that data into the basis of business actions, enabling management to gain new insights and thereby contributing to their business decisions. Business intelligence is an interactive process that starts by assembling the data into a format conducive to analysis. Once the data are organized in a database, they must be checked and cleaned to correct errors and flaws. Once the information is retrieved to establish patterns or make predictions, models and hypotheses are tested and validated.

A series of tools enables users to analyze data to see new patterns, relationships, and structures that are useful for guiding investigations and decision-making. Such tools for consolidating, analyzing, and providing access to vast amounts of data to help users improve business performance are referred to as business intelligence.

Business intelligence (BI) is an application of information technology (IT) that is used to extract critical business information for a growing number of functions. IT is used to process and analyze large amounts of data. IT is used for collection, treatment and diffusion of information that serves a purpose. Principle tools for business intelligence include software for database query and reporting, tools for multidimensional data analysis, and data mining.

Data have to be captured and organized before they are available for analysis. Data redundancy in terms of the presence of duplicate data should be avoided. Data inconsistency, where the same attribute may have different values, should be avoided as well. Rather than having traditional files where data are stored, it is much better to have data in databases, data warehouses, and data marts. Database technology cuts through many of the problems of traditional file organization. A database is a collection of data organized to serve many applications efficiently by centralizing the data and controlling redundant data (Laudon and Laudon, 2010: 240):

> Rather than storing data in separate files for each application, data are stored so as to appear to users as being stored in only one location. A single database services multiple applications.

A data warehouse is a database that stores current and historical data of potential interest to decision makers throughout the organization. The data originate in many core operational transaction systems, such as systems for sales, customer accounts, and manufacturing, and may include data from web site transactions. The data warehouse consolidates and standardizes information from different operational databases so that the information can be used across the enterprise for management analysis and decision making (Laudon and Laudon, 2010).

A data mart is a subset of a data warehouse in which a summarized or highly focused portion of the organization's data is placed in a separate database for a specific population of users. A data mart typically focuses on a single subject area or line of business, so it usually can be constructed more rapidly and at lower cost than an enterprise-wide data warehouse (Laudon and Laudon, 2010).

The following components constitute IT for BI:

- OLAP – On Line Analytical Processing. It refers to IT tools that allow for navigation in databases for hierarchies, relationships, developments and other perspectives. OLAP provides multidimensional and summarized views of business data and is used for modeling, analysis, reporting and planning of business activities. OLAP enables users to obtain online answers to ad hoc questions.

- Data Mining. This component takes advantage of statistical analysis techniques such as correlation analysis and regression analysis. Data mining is more discovery-driven than OLAP.

- Performance Management. For example, a balanced score card collects and exhibits performance in key areas such as finance, personnel, production, and market.

Similar to police intelligence, business intelligence is concerned with the identification of critical information for business performance. Business intelligence applications and their underlying critical information concepts support the needs of the business provided they are tightly integrated to both business environment and information technology infrastructure (Williams and Williams, 2003).

In the hierarchical structure of data-information-knowledge-wisdom we find intelligence as more than information and as less than knowledge. Intelligence is analyzed information, as illustrated in Figure 1. Here we use police investigation as an example.

Information and to a similar extent intelligence then consists of facts and other data which is organized to characterize or profile a particular situation, incident, or crime and the individual or group of individuals presumed to be involved. This organizing of the data to meaningful information of necessity involves some level of interpretation of the facts as presented. However, the role of interpretation here in information is relatively minor in comparison to its role in terms of knowledge construction. In this regard, the role of interpretation in intelligence is greater and more explicit than in information, but not as full blown as in the making of knowledge.

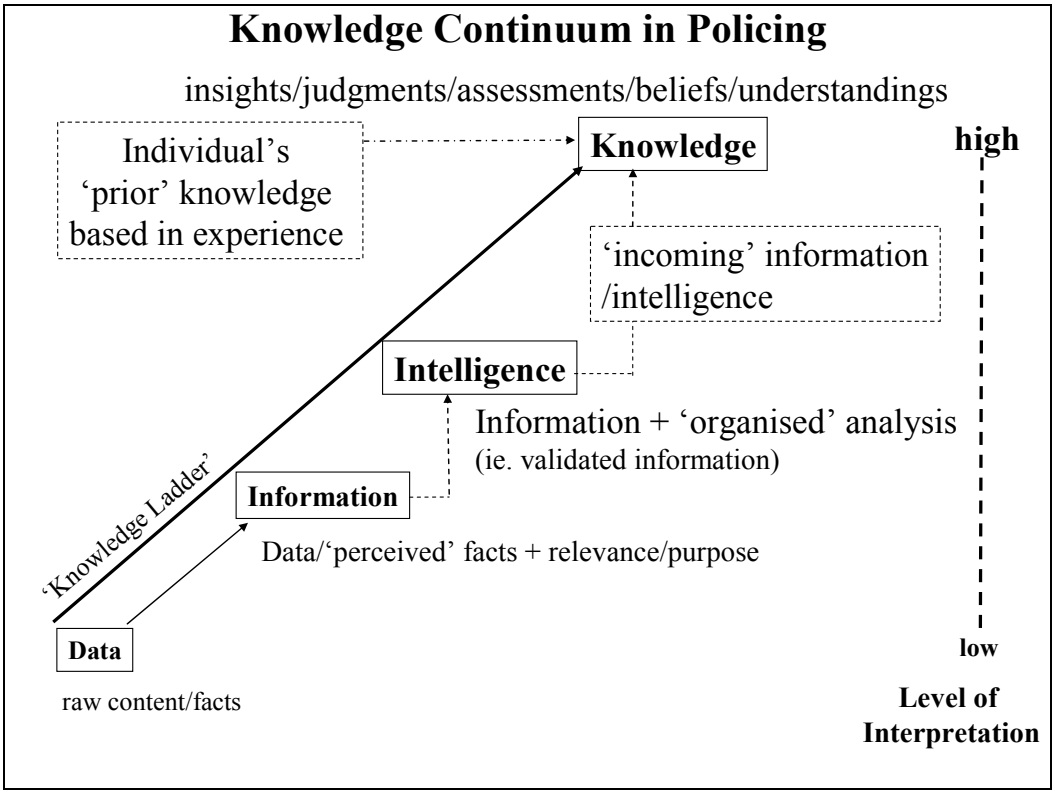


Figure 1. Hierarchy of police investigation insight expressed as a continuum

Knowledge helps develop relevant meaning to information in intelligence work (Innes and Sheptycki, 2004: 6):

> The distinction between information and intelligence is well established, but can be difficult to grasp. Information consists of bits of data that, when combined and viewed together with relevant background knowledge, may be used to produce intelligence, which informs the actions and decisions of policing organizations.

Knowledge as implied operates at a higher level of abstraction and consists of judgments and assessments based in personal beliefs, truths, and expectations about the information received and how it is should be analyzed, evaluated and synthesized - in short interpreted - so that it can be used and implemented into some form of action.

6.3 Stages of Growth

A knowledge organization is defined as an organization where the end product of work processes in the organization is knowledge or a service. If the end product of an organization is not a knowledge-based service while most or all work processes require advanced knowledge, such an organization is defined as a knowledge-intensive organization. While a knowledge-intensive organization might deliver goods such as food and transportation, a knowledge organization delivers a service, which is an intangible product.

A typical example of a knowledge organization is a law firm. A law firm is an organizational specialized in the application of legal knowledge to client problems. The client may want to prevent a problem or solve a problem. In law firm work of prevention and solution, lawyers in the firm apply a variety of knowledge categories such as declarative knowledge and procedural knowledge. Many law firms have transformed themselves from a professional model to a corporate business model. Knowledge is perceived as the resource on which the business is based. Unique, non-imitable, combinable and exploitable knowledge provides competitive advantage. Thus, their primary resources stem for the human capital and social capital of the individuals employed within them.

'Business model' is an expression that has gained ground considerably in the last decade. This concept is applied both in private business and in public administration. For a service firm, the process of developing a business model to improve performance will typically involve three steps (Sheehan and Stabell, 2007):

- *Step 1. Identifying the type of knowledge organization*: Key value creating activities as a problem-solving organization; reputation capital that attracts cases to the organization; and governance of independence from police as well as interoperability with the police.

- *Step 2. Mapping the organization*: Opportunities and threats to police oversight; and strengths and weaknesses of the police oversight agency.

- *Step 3. Generating new business model*: New value creating activities; new assets; and new governance structure.

Stages of growth models have been used widely in both organizational research and information technology management research. According to King and Teo (1997), these models describe a wide variety of phenomena – the organizational life cycle, product life cycle, biological growth, and so forth. These models assume that predictable patterns (conceptualized in terms of stages) exist in the growth of organizations, the sales levels of products, the diffusion of information technology, and the growth of living organisms. These stages are (1) sequential in nature, (2) occur as a hierarchical progression that is not easily reversed, and (3) involve a broad range of organizational activities and structures. This is the core idea of the concept of growth models.

Figure 2 illustrates a potential stage model for knowledge organizations:

- Stage 1. *Activity Organization*. Tasks are performed and completed in workflows according to specifications, rules and regulations. It is important to avoid mistakes and delays in the workflows. Activity repetition and completion is measured and monitored. Management is concerned with resource allocation and utilization according to tasks to be completed. The organization structure is broken down into work groups according to division of labor.

- Stage 2. *Problem Organization*. Each new assignment is perceived more as a problem to be solved than as a task to be completed. Problems are interpreted and solved by application of relevant knowledge. The quality of problem solution is more important than workflow performance or resource utilization. Management is concerned with quality control so that the solution really solves the problem. Interoperability is important at this stage in terms of technical as well as semantic interoperability, where technical interoperability among knowledge workers ensures access to each other and semantic interoperability ensures shared understanding.

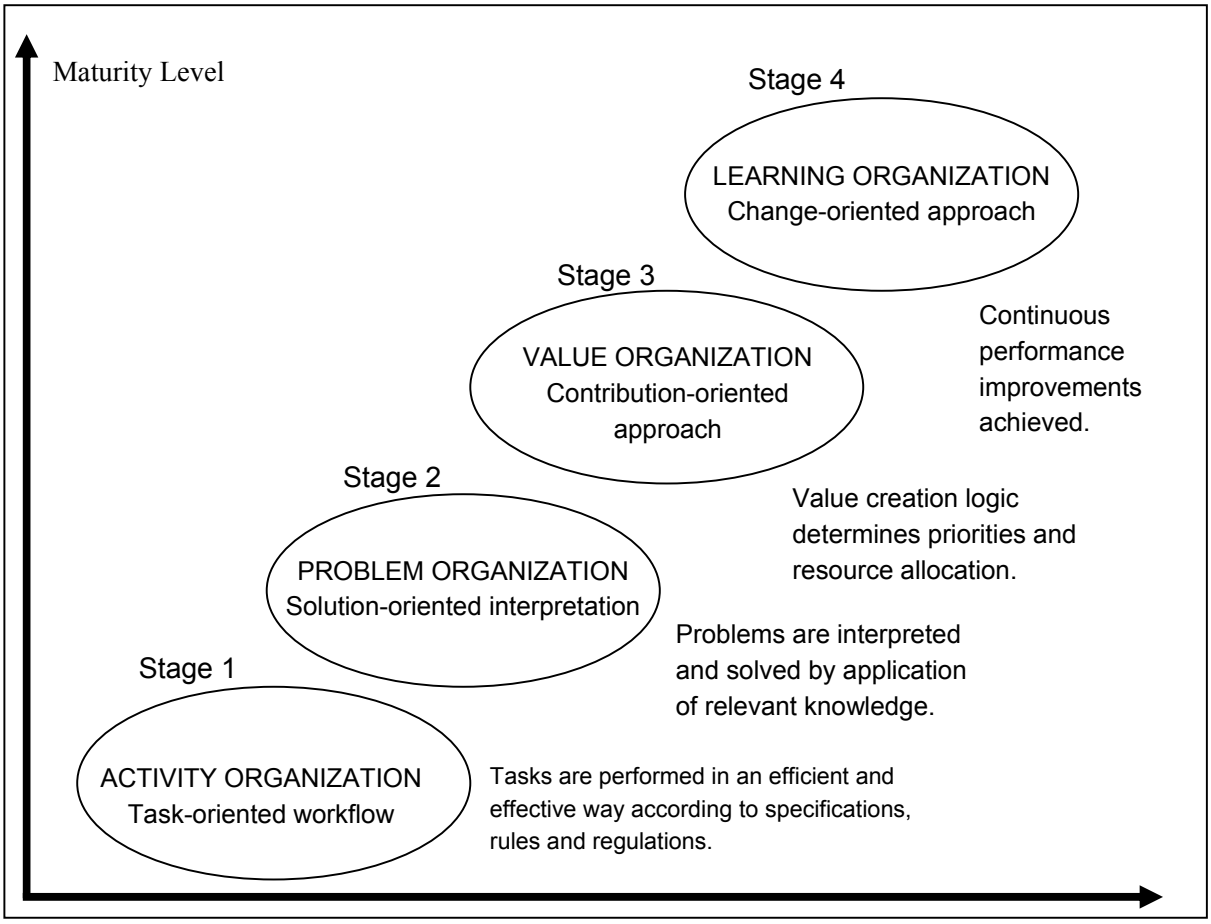


Figure 2. Stages of growth in knowledge organizations

- Stage 3. *Value Organization*. Value creation logic determines priorities and resource allocation. The value that might be created by working on and solving a problem determines how each problem is perceived and understood. A value organization makes strategic decisions about the role of the organization as it relates to the specter of problems with which is confronted. Performance goals are important at this stage, where goal setting is part of the strategy process, while goal achievement is part of the management process.

- Stage 4. *Learning Organization*. Continuous improvements are to be achieved based on experience. Change in resources, activities and approaches occur in the organization on a continuous basis. Communication channels are expanded internally (intra-organization) as well as externally (inter-organization). An organizational culture of sharing, transparency and contribution is stimulated. At this stage, supply-side knowledge management is replaced by demand-side knowledge management. Here knowledge sources are familiar to everyone and knowledge sharing occurs on demand for that knowledge.

In knowledge organizations at Stage 4, transformational and charismatic leadership is an influential mode of leadership that is associated with high levels of individual and organizational performance. Leadership effectiveness is critically contingent on, and often defined in terms of, leaders' ability to motivate followers toward collective goals or a collective mission or vision (Kark and Dijk, 2007).

6.4 Knowledge Resources

Knowledge is a renewable, reusable and accumulating resource of value to the organization when applied in the production of products and services. Knowledge cannot as such be stored in computers; it can only be stored in the human brain. Knowledge is what a knower knows; there is no knowledge without someone knowing it.

The need for a knower in knowledge existence raises the question as to how knowledge can exist outside the heads of individuals. Although knowledge cannot originate outside the heads of individuals, it can be argued that knowledge can be represented in and often embedded in organizational processes, routines, and networks, and sometimes in document repositories. However, knowledge is seldom complete outside of an individual.

In this book, knowledge is defined as information combined with experience, context, interpretation, reflection, intuition and creativity. Information becomes knowledge once it is processed in the mind of an individual. This knowledge then becomes information again once it is articulated or communicated to others in the form of text, computer output, spoken, or written words or other means. Six characteristics of knowledge can distinguish it from information: knowledge is a human act, knowledge is the residue of thinking, knowledge is created in the present moment, knowledge belongs to communities, knowledge circulates through communities in many ways, and new knowledge is created at the boundaries of old. This definition and these characteristics of knowledge are based on current research (e.g., Poston and Speier, 2005, Wasko and Faraj, 2005).

Today, any discussion of knowledge quickly leads to the issue of how knowledge is defined. A pragmatic definition defines the topic as the most valuable form of content in a continuum starting at data, encompassing information, and ending at knowledge.

Typically, data is classified, summarized, transferred or corrected in order to add value, and become information within a certain context. This conversion is relatively mechanical and has long been facilitated by storage, processing, and communication technologies. These technologies add place, time, and form utility to the data. In doing so, the information serves to inform or reduce uncertainty within the problem domain. Therefore, information is united with the context, that is, it only has utility within the context.

Knowledge has the highest value, the most human contribution, the greatest relevance to decisions and actions, and the greatest dependence on a specific situation or context. It is also the most difficult of content types to manage, because it originates and is applied in the minds of human beings. People who are knowledgeable not only have information, but also have the ability to integrate and frame the information within the context of their experience, expertise, and judgment. In doing so, they can create new information that expands the state of possibilities, and in turn allows for further interaction with experience, expertise and judgment. Therefore, in an organizational context, all new knowledge stems from people. Some knowledge is incorporated in organizational artifacts like processes, structures, and technology. However, institutionalized knowledge often inhibits competition in a dynamic context, unless adaptability of people and processes (higher order learning) is built into the institutional mechanisms themselves.

Our concern with distinctions between information and knowledge is based on real differences as well as technology implications. Real differences between information and knowledge do exist, although for most practical purposes these differences are of no interest at all. Information technology implications are concerned with the argument that computers can only manipulate electronic information, not electronic knowledge. Business systems are loaded with information, but without knowledge.

Some have defined knowledge as a fluid mix of framed experience, values, contextual information, and expert insights that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the mind of a knower. In organizations, it often becomes embedded not only in documents or repositories but also in organizational routines, processes, practices, and norms. Distinctions are often made between data, information, knowledge and wisdom:

Data are letters and numbers without meaning. Data are independent, isolated measurements, characters, numerical characters and symbols.

Information is data that are included in a context that makes sense. For example, 40 degrees can have different meaning depending on the context. There can be a medical, geographical or technical context. If a person has 40 degrees Celsius in fever, that is quite serious. If a city is located 40 degrees north, we know that it is far south of Norway. If an angle is 40 degrees, we know what it looks like. Information is data that make sense, because it can be understood correctly. People turn data into information by organizing it into some unit of analysis, e.g., dollars, dates, or customers. Information is data endowed with relevance and purpose.

Knowledge is information combined with experience, context, interpretation and reflection. Knowledge is a renewable resource that can be used over and over, and that accumulates in an organization through use and combination with employees' experience. Humans have knowledge; knowledge cannot exist outside the heads of individuals in the company. Information becomes knowledge when it enters the human brain. This knowledge transforms into information again when it is articulated and communicated to others. Information is an explicit representation of knowledge; it is in itself no knowledge. Knowledge can both be truths and lies, perspectives and concepts, judgments and expectations. Knowledge is used to receive information by analyzing, understanding and evaluating; by combining, prioritizing and decision making; and by planning, implementing and controlling.

Wisdom is knowledge combined with learning, insights and judgmental abilities. Wisdom is more difficult to explain than knowledge, since the levels of context become even more personal, and thus the higher-level nature of wisdom renders it more obscure than knowledge. While knowledge is mainly sufficiently generalized solutions, wisdom is best thought of as sufficiently generalized approaches and values that can be applied in numerous and varied situations. Wisdom cannot be created like data and information, and it cannot be shared with others like knowledge. Because the context is so personal, it becomes almost exclusive to our own minds and incompatible with the minds of others without extensive transaction. This transaction requires not only a base of knowledge and opportunities for experiences that help create wisdom, but also the processes of introspection, retrospection, interpretation and contemplation. We can value wisdom in others, but we can only create it ourselves.

It has been argued that expert systems using artificial intelligence are able to do knowledge work. The chess-playing computer called Deep Blue by IBM is frequently cited as an example. Deep Blue can compete with the best human players because chess, though complex, is a closed system of unchanging and rules that are codified. The size of the board never varies, the rules are unambiguous, the moves of the pieces are clearly defined, and there is absolute agreement about what it means to win or lose. Deep Blue is no knowledge worker; the computer does only perform a series of computations at extremely high speed.

While knowledge workers develop knowledge, organizations learn. Therefore, the learning organization has become a term frequently used. The learning organization is similar to knowledge development. While knowledge development is taking place at the individual level, organizational learning is taking place at the firm level. Organizational learning occurs when the firm is able to exploit individual competence in new and innovative ways. Organizational learning also occurs when the collective memory - including local language, common history and routines - expands. Organizational learning causes growth in the intellectual capital. Learning is a continuous, never-ending process of knowledge creation. A learning organization is a place where people are constantly driven to discover what has caused the current situation, and how they can change the present. To maintain competitive advantage, an organization's investment decisions related to knowledge creation are likely to be strategic in nature.

Our perspective of knowledge applied in this chapter is derived from the resource-based theory of the firm, as introduced in Chapter 1. According to the resource-based theory of the firm, performance differences across firms can be attributed to the variance in the firms' resources and capabilities. In this chapter, we focus on knowledge. Knowledge that is valuable, unique, difficult to imitate, combinable, difficult to substitute and exploitable can provide the basis for firms' competitive advantages. The essence of the resource-based theory of the firm lies n its emphasis on the internal resources - here knowledge - available to the firm, rather than on the external opportunities and threats dictated by industry conditions and market change.

6.5 Core Competence

According to Prahalad and Hamel (1990), core competencies are the collective learning in the organization, especially how to coordinate diverse service skills and integrate multiple streams of technologies. Since core competence is about harmonizing streams of technology, it is also about the organization of work and the delivery of value. Core competence does not diminish with use. Unlike physical assets, which do deteriorate over time, competencies are enhanced as they are applied and shared.

But competencies still need to be nurtured and protected; knowledge fades if it is not used. Competencies are the glue that binds existing business and coordinate service innovation. They are also the engines for new business development. At least three tests can be applied to identify core competencies in a company. First, a core competence provides potential access to a wide variety of markets. Second, a core competence should make a significant contribution to the perceived customer benefits of the end product. Finally, a core competence should be difficult for competitors to imitate.

The tangible link between identified core competencies and end products is what Prahalad and Hamel (1990) call core products - the embodiments of one or more core competencies. Core products are the components or subassemblies that actually contribute to the value of the end products. Core competencies are sometimes called firm-specific competencies, resource deployments, invisible assets, and distinctive competencies.

Quinn (1999) argues that core competencies are not products or "those things we do relatively well". They are those activities, usually intellectually based service activities or systems that the company performs better than any other enterprise. They are the sets of skills and systems that a company does at best-in-the-world levels and through which a company creates uniquely high value for customers. Developing best-in-the-world capabilities is crucial in designing a core competency strategy. Unless the company is best in the world at an activity it is someone else's core competency. The company gives up competitive edge by not buying that skill from a best-in-the-world source.

Competence and capability are terms often used interchangeably (Madhavaram and Hunt, 2008). However, competence represents implicit and invisible assets, while capability represents an explicit knowledge set. Leonard-Barton (1992) adopted a knowledge-based view of the firm and defined core capability as the knowledge set that distinguishes and provides competitive advantage. There are four dimensions to this knowledge set. Its content is embodied in (1) employee knowledge and skills and embedded in (2) technical systems. The processes of knowledge creation and control are guided by (3) managerial systems. The fourth dimension is (4) the values and norms associated with the various types of embodied and embedded knowledge and with the processes of knowledge creation and control.

Harreld et al. (2007) suggest that capabilities build on the notion of competencies but focuses on the role of management in building and adapting these competencies to address rapidly changing environments. Dynamic capabilities help enterprises to identify opportunities and mobilize competencies by reallocating resources. The ability to adapt and extend existing competencies is a key characteristic of dynamic capabilities. This ability places responsibility for entrepreneurship on executive management, as they must be able to accurately sense changes and opportunities. They must also act on these opportunities to be able to seize them by reconfiguring both tangible and intangible assets to meet new challenges.

Similar to core competencies, capabilities are considered core if they differentiate a company strategically. The concept is not new. Their strategic significance has been discussed for decades, stimulated by research discovery that of nine diversification strategies, the two that were built on an existing skill or resource base in the firm were associated with the highest performance. The observation that industry-specific capabilities increased the likelihood a firm could exploit a new technology within that industry, has confirmed the early work.

Therefore some authors suggest that effective competition is based less on strategic leaps than on incremental innovation that exploits carefully developed capabilities. On the other hand, institutionalized capabilities may lead to incumbent inertia in the face of environmental changes. Technological discontinuities can enhance or destroy existing competencies within an industry. Such shifts in the external environment resonate within the organization, so that even seemingly minor innovations can undermine the usefulness of deeply embedded knowledge. All innovation necessarily requires some degree of creative destruction.

A capability is defined as dynamic if, in a rapidly changing environment, it enables the firm to modify itself so as to continue to produce, efficiently and/or effectively, market offerings for some market segments (Madhavaram and Hunt, 2008).

6.6 Entrepreneurship Capabilities

Corporate entrepreneurship is crucial in the acquisition of dynamic organizational capabilities (Zahra et al., 1999). Scholars have identified entrepreneurship as the core process by which companies have attempted to redefine, renew, and remake themselves.

An entrepreneurship perspective on the nature of the firm rests on two fundamental assumptions about the nature of business activity: profit-seeking individuals and asymmetrically dispersed knowledge across economic actors. The quest for profit, wealth and power plays an important motivational role in the entrepreneur's pursuit of new business opportunities. Asymmetrically dispersed knowledge implies differentiated sets of knowledge held by decision makers, which in the business context causes variation in the ability to identify and assimilate new information and events. Individual decision makers tend to notice new information that relates to and can be combined with knowledge they already have (Zander, 2007).

An entrepreneur is a person who operates a new enterprise or venture or revitalizes an existing enterprise and assumes some accountability for the inherent risk. The newly and modern view on the entrepreneurial talent is a person who takes the risks involved to undertake a business venture. Entrepreneurship is often difficult and tricky, as many new ventures fail. In the context of the creation of for-profit enterprises, entrepreneur is often synonymous with founder. Most commonly, the term entrepreneur applies to someone who creates value by offering a product or service in order to obtain certain profit.

Entrepreneurship is thus the practice of starting new organizations or revitalizing mature organizations, particularly new businesses generally in response to identified opportunities. Entrepreneurship is sometimes labeled entrepreneurialism. Entrepreneurship is often a difficult undertaking, as a vast majority of new businesses fail. Entrepreneurial activity is substantially different from operational activity as it is mainly concerned with creativity and innovation. Entrepreneurship ranges from small individual initiatives to major undertakings creating many job opportunities.

The majority of recent theories in the business and managerial economic literature assume that the economic performance of small and medium-sized firms depends largely on the entrepreneurs' (or team's) capacities. Even so, economists still do not fully understand the relationship between entrepreneurs and firm performance. The entrepreneurial process is the result of a complex interaction between individual, social and environmental factors. Taken separately, neither the personality of the entrepreneur nor the structural characteristics of the environment can, on its own, determine an organization's performance (Thomas and Mancino, 2007).

In order to provide an example of the relationship between entrepreneurs' subjective characteristics/traits and organizational performance, Thomas and Mancino (2007) carried out an empirical study. The study aimed to explain how the presence of entrepreneurs' specific subjective characteristics can influence an organization's strategic orientation and, as a consequence, local development. By analyzing several subjective characteristics taken from a sample of 101 successful entrepreneurs from southern Italy, certain issues emerged regarding the link between the economic performance of the ventures launched in this area and the weak level of growth. Successful entrepreneurs' behavior and decisions seemed heavily influenced by family support. The entrepreneurial culture of the family also tends to substitute the protective role played by public institutions. The entrepreneurial decisions of local entrepreneurs are triggered both by their need to rid themselves of poverty and their feeling that they are destined to continue the family business, the majority of them being the children of entrepreneurs. Most of the interviewees were classified as necessity rather than opportunity entrepreneurs.

An entrepreneur might be driven by a compulsive need to find new ways of allocating resources. He or she might be searching for profit-making opportunities and engineer incremental changes in products and processes. While strongly innovative entrepreneurs tend to champion radical changes in resource allocation by making new service markets and pioneering new processes, weakly innovative entrepreneurs tend to seek small changes in resource allocation to explore profit-making opportunities between already established activities (Markovski and Hall, 2007).

Founders of new legal firms tend to be experienced professionals who pursue opportunities closely related to their previous employment. Entrepreneurs often have several years of work experience in the same industry as their own start-up enterprises. This suggests that entrepreneurs do not come from out of the blue, but build their human intellectual capital through work experience in established firms. Similarly, criminal entrepreneurs might be experienced professionals before establishing their own criminal business enterprise.

Jacobides and Winter (2007) phrased the question: How do entrepreneurs choose their boundaries of their own ventures? To answer this question, they started from the premise that while entrepreneurs believe themselves to have superior ideas in one or multiple parts of value creation arenas, they are characteristically short of cash, and of the ability to convince others to provide it. This premise motivates a simple model in which the entrepreneur has a value-adding set of ideas for parts of a value creation arena. Assuming that the entrepreneur's objective is to maximize wealth, it might be observed that initial scope depends on available cash, but also on how much value the entrepreneur's ideas add to each participant in the enterprise. Entrepreneurs will focus on the areas that provide the maximum profit and minimum risk per available cash in service innovation.

6.7 A Case of Dynamic Capabilities

So far in this chapter, we have explained the definitions and relationships of knowledge, skills, capabilities, organizational capabilities and core competencies as they relate to the resource-based and knowledge-based theory of the firm. Next, we will exemplify the concepts of dynamic capabilities exhibited by agile organizations, as they relate to dynamic knowledge management and the practice of excellent strategy execution.

Harreld et al. (2007) present the case of dynamic capabilities at IBM. They argue that dynamic capabilities are driving strategy into action in the firm. They studied the rise, fall, and transformation of IBM during a 20-year period. IBM's dynamic capabilities transformed IBM from a set of conventional silos (e.g., hardware, software, and services) to an integrated structure oriented to provide solutions for customer needs. To make this new approach work, the entire role of the corporate strategy group at IBM needed to change.

Dynamic capabilities enable the sensing of changes in competitive environment as well as the seizure of opportunities. To ensure that the strategy process at IBM provides the insight necessary to sense opportunities and the execution required to seize them, a set of complementary mechanisms have evolved. Strategic leadership forums and other initiatives help explore into new spaces, while metrics and structure help exploit existing capabilities and processes.

Sensing new opportunities to gain strategic insight is conducted in a number of processes at IBM (Harreld et al., 2007):

- The Technology Team meets monthly and assesses the market readiness and the potential of emerging technologies.
- The Strategy Team meets monthly to examine the market results of existing unit strategies as well as to explore new growth areas.
- The Integration and Value Team meets quarterly to support company-wide initiatives.
- Deep Dive processes are initiated when confronting a performance or opportunity gap to scrutinize a topic in great detail.

Each of these processes help ensure steady surveillance and intelligence of the competitive environment. Intelligence is the systematic approach to collecting information with the purpose of tracking and predicting change to improve business performance. Intelligence analysts investigate who are the actors, how, when, where and why. They provide recommendations on how to react to market changes and opportunities. As part of this, analysts may produce profiles of market problems and targets, and produce both strategic (overall, long-term) and tactical (specific, short-term) assessments within the confines set by the business and the industry.

Seizing new opportunities for strategic execution is conducted in a number of processes at IBM (Harreld et al., 2007):

- Emerging Business Opportunities are an integrated set of processes, incentives, and structures designed explicitly to enable IBM to address new business opportunities and drive revenue growth.

- Strategic Leadership Forums are several days of team-based workshops built around specific performance or opportunity gaps that bring extended teams together for intensive work on problems or opportunities.

- Corporate Investment Funds are a way of providing funding for new initiatives identified by the Integration and Value Teams.

Harreld et al. (2007) argue that unlike other piecemeal approaches to strategy, the IBM process is one driven by line management based on the realities of the marketplace as seen in performance or opportunities gaps, not a staff exercise or slide deck. This has moved the strategy-making process from an annual ritual to a continual process, from an emphasis on planning to one on action, from a staff function to one that line managers own, and from a concern with strategy only to a focus on both strategy and execution.

6.8 Knowledge Driven Innovation

Knowledge resources, core competences and dynamic capabilities are key drivers of service innovation in firms. Based on such drivers, a variety of modes of innovation emerge in knowledge-intensive business services. For example, Corrocher et al. (2009) identified the interactive innovation mode, the techno-organizational mode, the conservative mode, and the product innovation mode for knowledge-intensive business services:

- The interactive innovation mode occurs in the interaction with other firms and customers.

- The techno-organizational mode occurs when technology adoption is not an isolated and passive strategy, but is closely intertwined with changes associated with the way in which services are provided and organized.

- The conservative mode occurs when a firm does not carry out any relevant innovation activity.

- The product innovation mode occurs when innovative ideas are linked to manufacturing.

Corrocher et al. (2009) found that the attention paid to the innovative activities of service sectors has significantly increased over the last decade. Simultaneity of production and consumption and the intangible nature of the service make long distance trade more difficult than for goods and give a local flavor to competition, even when considering the more sophisticated services. This is particularly evident in advanced regions, where competitiveness depends on knowledge content, provided by highly specialized experts.

Therefore, knowledge production is increasingly directed at business services. The emphasis is laid in the role of business services in innovative networks as carriers of knowledge and intermediates between science (knowledge creator) and their customers (knowledge users). An empirical analysis by Hipp (1999) shows that knowledge-intensive business services are able to make existing knowledge useful for their customers, improving the customer's performance and productivity and contributing to technological and structural change.

In this context, knowledge-intensive business services are defined in terms of service characteristics and knowledge characteristics. Among service characteristics we find close interaction between service provider and customer and highly intangible content of service products and processes. Among knowledge characteristics we find ability to receive information from outside the firm and to transform this information together with firm-specific knowledge into useful services for their customers (Hipp, 1999).

Madhavaram and Hunt (2008) argue there is a service-dominant logic in resource management. They apply resource-advantage theory to suggest marketing's evolution toward a new dominant logic that requires the focus of marketing to be on the intangible, dynamic, operant resources that are the heart of competitive advantage and performance.

Drawing from the resources, competences, resource-advantage theory, capabilities, and dynamic capabilities literature, Madhavaram and Hunt (2008) extend and elaborate on the service-dominant logic's notion of operant resources by proposing a hierarchy of operant resources. Starting from the seven basic resource categories (financial, physical, legal, human, organizational, informational, and relational), they propose basic, composite, and interconnected operant resources as the hierarchy.

Innovation in services very often includes creative application of information technology found in the technological dimension of innovation. However, as pointed out by Gallouj and Savona (2009), innovation in services is becoming an increasingly complex issue, in which the adoption of information and communication technology is just one of many possible facilitators.

A number of important concepts have been introduced in this chapter, including knowledge, knowledge management, core competencies, and dynamic capabilities. These concepts represent perspectives to gain insights into barriers and enablers of service innovation. At the center of these concepts we find knowledge as a resource to be explored and exploited for the benefit of innovation in services.

7. Intelligence Strategy

An intelligence strategy is needed for business intelligence. Business intelligence is a process of taking large amounts of data, analyzing that data, and presenting a high-level set of reports that condense the essence of that data into the basis of business actions. Business intelligence can enable management to gain new insights and thereby contributing to their business decisions to prevent computer crime and to strengthen corporate reputation.

7.1 Strategy Characteristics

Traditionally, intelligence was understood to mean information from criminals about criminal activity by a covert source. Today, intelligence is a systematic approach to collecting information with the purpose, for example, of tracking and predicting crime to improve law enforcement (Brown et al., 2004). Intelligence analysts investigate who is committing crimes, how, when, where and why. They then provide recommendations on how to stop or curb the offences. As part of this, analysts produce profiles of crime problems and individual targets, and produce both strategic (overall, long-term) and tactical (specific, short-term) assessments within the confines set by the policing unit.

The aim of intelligence strategy is to continue to develop intelligence led policing in all parts of an organization, a nation or in all regions of the world. An intelligence strategy provides a framework for a structured problem solving and partnership enhanced approach, based around a common model. For example, the National Intelligence Model in the UK is a structured approach to improve intelligence led policing both centrally and locally in policing districts such as the South Yorkshire Police (SYPIS, 2007).

Intelligence-led policing is carried out in many law enforcement areas. For example, intelligence-led vehicle crime reduction was carried out in the West Surrey police area in the UK. Analysis of vehicle crime included identifying (Brown et al., 2004):

- Locations (hotspots, streets, car parks, postcodes, wards, etc.) of vehicle crime,
- Sites where vehicles were dumped,
- Times of offences,
- Prolific vehicle crime offenders,
- Areas where prolific offenders were identified as offending,
- Models of vehicles targeted for vehicle crime,
- Type of property stolen in theft from vehicle offences.

The analysis resulted in problem profiles, which identified emerging patterns of crime. These patterns included vehicle crime occurring in beauty spot car parks and the theft of badges from cars. Such information was disseminated to local officers to act on.

Intelligence-led policing is defined as a business model and a management philosophy according to Ratcliffe (2008: 89):

> Intelligence-led policing is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders.

An interesting case of intelligence-led policing in the UK was the project called "Operation Gallant" that lead to a reduction of 17% in car thefts. Operation Gallant involved all Basic Command Unit (BCU) in the collection and analysis of information (Brown et al., 2004: 2):

> In the case of Operation Gallant, the intelligence-led vehicle crime reduction approach involved the activity of officers from across a BCU. A crime analyst, dedicated solely to examine vehicle crime patterns and trends, developed a detailed picture of vehicle crime in the area, including analysis of time, location, vehicle type and known offenders. As a result of this strategic analysis, a number of interventions were planned, drawing heavily upon the Operation Igneous tactical menu. The most significant, in terms of resources devoted to the operation, involved a program of prolific offender targeting and crime prevention advice targeted towards the owners of high-risk vehicles.

The substantial decline in car crimes were explained by the increased attention paid to this crime sector (Brown et al., 2004: 16):

> Given the fact that the first reduction coincides with the commencement of the planning process for Operation Gallant, this may also reflect an anticipatory effect in which the very act of planning and talking about an operation leads to a decline.

7.2 Information Sources

In intelligence work for investigating and preventing white-collar crime, a variety of information sources are available. Sheptycki (2007) list the following information sources in policing for general corporate social responsibility work: victim reports, witness reports, police reports, crime scene examinations, historical data held by police agencies (such as criminal records), prisoner debriefings, technical or human surveillance products, suspicious financial transactions reporting, and reports emanating from undercover police operations. Similarly, internal investigation units in business organizations can apply intelligence sources. Intelligence analysis may also refer to governmental records of other governmental departments and agencies, and other more open sources of information may be used in elaborate intelligence assessment. Most of the information used to prevent and investigate financial crime is sensitive, complex, and the result of time consuming tasks (Wilhelmsen, 2009).

However, Sheptycki (2007) found that most crime analysis is organized around existing investigation and prevention sector data. Intelligence analysis is typically framed by already existing institutional ways of thinking. He argues that organized crime notification, classification and measurement schemes tend to reify pre-existing notions of traditional policing practice.

In this perspective, it is important for strategic criminal analysts to be aware of the variety of information sources available. We choose to classify information sources into the following categories in this book:

1. *Interview*. By means of *interrogation* of witnesses, suspects, reference persons and experts, information is collected on crimes, criminals, times and places, organizations, criminal projects, activities, roles, etc.

2. *Network*. By means of *informants* in the criminal underworld as well as in legal businesses, information is collected on actors, plans, competitors, markets, customers, etc. Informants often have connections with persons that are an investigating colleague would not be able to approach formally.

3. *Location*. By analyzing potential and actual *crime scenes* and potential criminal scenes, information are collected on criminal procedures, preferences, crime evolution, etc. Hot spots and traces are found. Secret ransacking of suspicious places is part of this information source. Pictures in terms of crime scene photographs are important information elements.

4. *Documents*. By studying documents from *confiscations* may provide information on ownership, transactions, accounts, etc. An example is forensic accounting, which is the application of accounting tasks for an evidentiary purpose. Forensic accounting is the action of identifying, recording, settling, extracting, sorting, reporting and verifying past financial data or other accounting activities for settling current or prospective legal disputes or using such past financial data for projecting future financial data to settle legal disputes. Forensic accountants are essential to the legal system, providing expert services such as fake invoicing valuations, suspicious bankruptcy valuations, and analysis of financial documents in fraud schemes (Curtis, 2008).

5. *Observation*. By means of *anonymous personal presence* both individuals and activities can be observed. Both in the physical and the virtual world, observation is important in financial crime intelligence. An example is digital forensics, where successful cyber crime intelligence requires computer skills and modern systems in policing. Digital forensics is the art and science of applying computer science to aid the legal process. It is more than the technological, systematic inspection of electronic systems and their contents for evidence or supportive evidence of a criminal act. Digital forensics requires specialized expertise and tools when applied to intelligence in important areas such as online victimization of children.

6. *Action*. For example, *provocation* is and action by the investigating unit to cause reactions that represents intelligence information. In the case of online victimization of children, online grooming offenders in a pedophile ring are identified and their reaction to provocations leads intelligence officers into new nodes (persons, computers) and new actual and potential victims. While the individual pedophile is mainly concerned with combining indecent image impression and personal fantasy to achieve personal satisfaction, online organizers of sexual abuse of children are doing it for profit. By claiming on the Internet to be a boy or girl of 9 years, police provoke contact with criminal business enterprises making money on pedophile customers. Undercover operations by police officers do as well belong to the action category of information sources.

7. *Surveillance*. Surveillance of places by means of *video cameras* as well as microphones for viewing and listening belong to this information source. Many business organizations have surveillance cameras on their premises to control entrants and other critical areas. It is possible for the police to be listening in on what is discussed in a room without the participants knowing. For example, police in a country identified which room was used by local Hells Angels members in their resort for crime planning and installed listening devices in that room. Harfield (2008: 64) argues that when surveillance is employed to produce evidence, such product is often considered incontrovertible (hence defense lawyers' focus on process rather than product when cross-examining surveillance officers): "An essentially covert activity, by definition surveillance lacks transparency and is therefore vulnerable to abuse by over-zealous investigators".

8. *Communication control*. Wire tapping in terms of *interception* belongs to this information source. Police is listening in on what is discussed on a telephone or data line without the participants knowing. In the UK, the interception of communications (telephone calls, emails, letters, etc.), whilst generating intelligence to identify more conventional evidential opportunities, is excluded from trial evidence by law, to the evident incredulity of foreign law enforcement colleagues (Harfield, 2008).

9. *Physical material*. Investigation of material to identify for example *fingerprints* on doors or bags, or material to identify blood type from blood splatters. Another example is legal visitation, which is an approach to identify illegal material. DNA is emerging as an important information source, where DNA is derived from physical material such as hair or spit from a person. Police search is one approach to physical material collection.

10. *Internet*. As an *open source*, the Internet is as important for general information and specific happenings to corporate crime intelligence as to everyone else. It is important to note that use of open sources is not at all a new activity and not a new phenomenon of the Internet, which is not in itself a source, but a tool at finding sources. Also, there are risks of using open sources such as self-corroboration.

11. *Policing systems*. Readily available in most police agencies are *police records*. For example, DNA records may prove helpful when having DNA material from new suspects. Similarly, corporate social responsibility units may develop records that do not violate privacy rights.

12. *Employees*. Information from the *local community* is often supplied as tips to local police using law enforcement tip lines. Similarly, a corporate social responsibility unit is receiving tips from employees in various departments.

13. *Accusations*. Victimized persons and goods file a *claim* with the corporate investigation unit or the unit for corporate social responsibility.

14. *Exchange*. International *policing cooperation* includes exchange of intelligence information. International partners for national police include national police in other countries as well as multinational organizations such as Europol and Interpol. Similarly, trade organizations and other entities for business organizations create exchanges for financial crime intelligence.

15. *Media*. By reading newspapers and watching TV, intelligence officers get access to *news*.

16. *Control authorities*. Cartel agencies, stock exchanges, tax authorities and other control authorities are *suppliers of information* to the corporate executives in case of suspicious transactions.

17. *External data storage*. A number of business and government organizations store information that may be useful in financial crime intelligence. For example, telecom firms store data about traffic, where both sender and receiver are registered with date and time of communication.

All these information sources have different characteristics. For example, information sources can be distinguished in terms of the extent of trustworthiness and the extent of accessibility.

Prisons and other correctional environments are potential places for several information sources and production of intelligence useful to law enforcement. The total prison environment, including the physical plant, the schedule regimens of both staff and inmates, and all points of ingress and egress can be legitimately tapped for intelligence purposes in countries such as the US (Maghan, 1994). Since organized criminals often are sophisticated in using the correction environment to their advantage, police and correction personnel need immersion in the intelligence operations and strategies of their respective agencies. Legal visitation and escape attempts are sources of information. Prisoners are reluctant to testify, and their credibility is easily attacked. Communication control is derived from inmate use of phones, visits, mail, and other contacts.

The 17 information sources can be classified into two main categories. The first category includes all person-oriented information sources, where the challenge in corporate intelligence is to communicate with individuals. The second category includes all media-oriented information sources, where the challenge in corporate intelligence is to manage and use different technological and other media. This distinction into two main categories leads to the following classification of 17 information sources:

A. *Person-oriented information sources*
   1 Interrogation in interview
   2 Informants in network
   5 Anonymous, individual presence undercover for observation
   6 Provocation through action
   12 Tips from citizens in local community
   13 Claims in accusations
   14 Information exchange in inter-organizational cooperation

B. *Media-oriented information sources*
   3 Crime scenes at location
   4 Confiscated documents
   7 Video cameras for surveillance
   8 Interception for communication control
   9 Physical materials such as fingerprints
   10 Open sources such as Internet
   11 Internal records in policing systems
   15 News in the media
   16 Supply of information from control authorities
   17 External data storage

Combinations of information sources are selected in investigation and intelligence depending on the subject of white-collar crime. When forensic accounting is applied as document study, it is typically combined with interviews and observations, thereby integrating behavioral aspects into forensic accounting (Ramamoorti, 2008).

7.3 Knowledge Categories

Information sources provide the raw material for knowledge work to prevent white-collar crime and strengthen corporate reputation. Knowledge has to be identified in terms of categories and levels. One identification approach suggested here is the knowledge matrix approach. A knowledge matrix is a table that lists knowledge needs. The matrix shows knowledge categories and knowledge levels.

Here we make distinctions between the following knowledge categories for investigating and preventing financial crime:

1. *Administrative knowledge* is knowledge about the role of management and executive leadership. It is knowledge about procedures, rules and regulations.

2. *Organization knowledge* is knowledge about how the business is organized and management as a law enforcement role. This is knowledge at the organizational level.

3. *Employee knowledge* is knowledge about where employees spend their working hours, what they do, and why they do it. This is knowledge at the individual level.

4. *Process knowledge* is knowledge about work processes and practices in business work when committing financial crime. Process knowledge is based on police science, which includes all aspects of policing internally as well as externally (Jaschke et al., 2007). It includes external factors that influence the role and behavior of policing in society.

5. *Investigative knowledge* is knowledge based on case specific and case oriented collection of information to confirm or disconfirm whether an act or no-act is criminal. Included here are case documents and evidence in such a form that they prove useful in a court case.

6. *Intelligence knowledge* is knowledge based on a systematic collection of information concerned with a certain topic, a certain domain, certain persons or any other focused scope. Collected information is transformed and processed according to a transparent methodology to discover criminal capacity, dispositions and goals. Transformation and processing generate new insights into criminality that guide the effectiveness and efficiency of prevention and investigation. Included in intelligence knowledge is phenomenological knowledge, which is defined as knowledge about a phenomenon, in terms of what it is about (know-what), how it works (know-how), and why it works (know-why). Phenomenological knowledge enables intelligence workers to "see" what "something" is about, by understanding and not missing when information emerges.

7. *Legal knowledge* is knowledge of the law, regulations and legal procedures. It is based on access to a variety of legal sources both nationally and internationally, including court decisions. Legal knowledge is composed of declarative, procedural and analytical knowledge. Declarative knowledge is law and other regulations. Procedural knowledge is the practice of law. Analytical knowledge is the link between case information and laws.

8. *Technological knowledge* is knowledge about the development, use, exploitation and exploration of information and communication technology. It is knowledge about applications, systems, networks and databases.

9. *Analytical knowledge* is knowledge about the strategies, tactics and actions that executive managers and investigators can implement to reach desired goals.

An example of investigative knowledge in financial crime investigations is forensic accounting. Forensic accounting is concerned with identifying, recording, settling, extracting, sorting, reporting, and verifying past financial data. The focus of forensic accounting is on evidence revealed by the examination of financial documents. Financial crime such as fraud can be subject to forensic accounting, since fraud encompasses the acquisition of property or economic advantage by means of deception, through either a misrepresentation or concealment. Forensic examinations include consideration of digital evidence, including communications (Curtis, 2008).

To develop investigative knowledge in the area of forensic accounting, Kranacher et al. (2008) suggest a model curriculum consisting of several concepts such as basic accounting, basic auditing, transaction processing, business law, business communication and computer skills. The purpose of such a curriculum is to build knowledge, skills and abilities in forensic accounting to combat white-collar crime.

In addition to the above classification into knowledge categories, we also make distinctions between knowledge levels:

1. *Basic knowledge* is knowledge necessary to get work done. Basic knowledge is required for an intelligence officer and investigator as a knowledge worker to understand and interpret information, and basic knowledge is required for an intelligence and investigation unit as a knowledge organization to receive input and produce output. However, basic knowledge alone produces only elementary and basic results of little value and low quality.

2. *Advanced knowledge* is knowledge necessary to get good work done. Advanced knowledge is required for an intelligence officer and investigator as a knowledge worker to achieve satisfactory work performance, and advanced knowledge is required for an intelligence and investigation unit as a knowledge organization to produce intelligence reports and crime analysis as well as charges that are useful in investigation and prevention of financial crime. When advanced knowledge is combined with basic knowledge, then we find professional knowledge workers and professional knowledge organizations in law enforcement.

3. *Innovative knowledge* is knowledge that makes a real difference. When intelligence officers and investigators apply innovative knowledge in intelligence and analysis of incoming and available information, then new insights are generated in terms of crime patterns, criminal profiles and prevention and investigation strategies. When intelligence units apply innovative knowledge, then new methodologies in intelligence and analysis are introduced, that corporate management can learn.

#	Category	Basic Knowledge	Advanced Knowledge	Innovative Knowledge
1	Administrative knowledge	*The role of a complaints and whistle-blowing investigator*	*Sources of information*	*Best practice in complaints and crime investigations*
2	Organization knowledge	*How the business is organized and managed*	*How internal misconduct and crime is solved*	*Power structures in the organization and links to the criminal world*
3	Employee knowledge	*Where employees spend their working hours*	*What employees do in their working hours*	*Why employees do what they do in their working hours*
4	Process knowledge	*Information sources in investigation and prevention*	*Analyses techniques in investigation and prevention*	*Behavior in investigative and preventive work*
5	Investigative Knowledge	*Investigative procedures*	*Contingent approaches to investigations*	*Hypothesis and causality in crime*
6	Intelligence knowledge	*Intelligence procedures*	*Contingent approaches to intelligence*	*Hypotheses and causality in potential crime*
7	Legal knowledge	*What investigators can do*	*What investigators cannot do*	*Expected outcome of court procedure*
8	Technological knowledge	*Equipment in investigative work*	*Equipment in analysis work*	*Artificial intelligence and expert systems*
9	Analytical knowledge	*Analytical methods*	*Analytical procedures*	*Analytical creativity*

Table 1. Knowledge management matrix for knowledge needs in investigation and prevention of financial crime in organizations.

Based on these categories and levels, our knowledge matrix consists of 9 knowledge categories and 3 knowledge levels as illustrated in Table 1. The purpose of the table is to illustrate that there are a total of twenty-seven knowledge-needs in investigating and preventing financial crime. Based on the table, each intelligence unit and investigation unit has to identify and fill in the table for knowledge needs.

#	Category	Know-What	Know-How	Know-Why
1	Administrative knowledge	*What investigating colleagues is all about*	*How investigating colleagues is done*	*Why investigation and prevention of financial crime is carried out*
2	Organization knowledge	*What employees do*	*How employees do the things they do*	*Why employees do the things they do*
3	Employee knowledge	*What colleagues do during their working hours*	*How colleagues do their work*	*Why colleagues do what they do*
4	Process knowledge	*What kinds of financial crime do occur*	*How financial crime does occur*	*Why financial crime does occur*
5	Investigative knowledge	*What investigative procedures are available*	*How investigative procedures work*	*Why investigative procedures work the way they do*
6	Intelligence knowledge	*What intelligence procedures are available*	*How intelligence procedures work*	*Why investigative procedures work the way they do*
7	Legal knowledge	*What laws and regulations are relevant for financial crime*	*How these laws and regulations are relevant for financial crime*	*Why these laws and regulations are relevant for financial crime*
8	Technological knowledge	*What technological means are available to enforce law on criminal employees*	*How these technological means enable law enforcement*	*Why these technological means enable law enforcement*
9	Analytical knowledge	*What approaches are successful in enforcing law on criminal employees*	*How are these approaches successful*	*Why are these approaches successful*

Table 2. Alternative knowledge management matrix for knowledge needs in investigation and prevention of financial crime in organizations.

Knowledge levels were here defined at basic knowledge, advanced knowledge and innovative knowledge. An alternative approach is to define knowledge levels in terms of knowledge depth: know-what, know-how and know-why. These knowledge depth levels represent the extent of insight and understanding about a phenomenon. While know-what is simple perception of what is going on, know-why is complicated insight into cause-and-effect relationships in terms of why it is going on:

1. *Know-what* is knowledge about what is happening and what is going on. An executive perceives that something is going on, that might need his or her attention. The executive's insight is limited to perception of something happening. The executive does neither understand how it is happening nor why it is happening.

2. *Know-how* is knowledge about how financial crime develops, how a criminal behaves or how a criminal activity is organized. The executive's or investigator's insight is not limited to a perception of something is happening; he or she also understands how it is happening or how it is.

3. *Know-why* is the knowledge representing the deepest form of understanding and insight into a phenomenon. The executive or investigator does not only know that it occurs and how it occurs. He or she also has developed an understanding of why it occurs or why it is like this. Developing hypotheses about cause-and-effect relationships and empirically validating causality are important characteristics of know-why knowledge.

One part of the knowledge work is to investigate a crime were a colleague is a suspect. That type of internal policing is described above. It seems easy to forget another part of internal policing as well. Not just executives, but also other colleagues do themselves have a responsibility to prevent that colleagues get involved in illegal actions during the business work. To succeed with that executives and colleagues need knowledge mentioned above, and it is also important that internal police officers have an interest and dare to take action to prevent or react on illegal actions when taken by colleagues during work processes.

8. Crime Investigations

Cyber crime investigations have both similarities and differences when compared to traditional crime such as burglary and robbery. Traditional crime generally concern personal or property offences that law enforcement has continued to combat for centuries. Cyber crime is characterized by being technologically advanced, it can occur almost instantaneously, and it is extremely difficult to observe, detect, or track. These problems are compounded by the relative anonymity afforded by the Internet as well as the transcendence of geographical and physical limitations in cyberspace. Criminals are able to take advantage of a virtually limitless pool of potential victims (Hinduja, 2007).

Policing financial crime generally – according to Pickett and Pickett (2002) – is concerned with whistle blowing and detection, roles of shareholders and main board and chief executive officer and senior executives, investigations, forensics. Policing financial crime – according to Levi (2007) – is concerned with the organization of policing deception, the contexts of police undercover work, covert investigations of white-collar crime, prosecution and relationship to policing fraud. Covert activity is restricted mainly to the informal obtaining of financial information or the official obtaining of information about suspected bank accounts without the knowledge of the account-holder. Policing cyber crime is concerned with all these issues as well as a tight surveillance of relevant activities on the Internet.

Within crime investigations, IT forensics and cyber crime investigations are an extremely complicated field (Callanan and Jones, 2009). Kao and Wang (2009) suggest an approach to improving cyber crime investigation consisting of three stages: independent verification of digital clues, corresponding information from different sources, and preparation of a valid argument. Furthermore, covert investigations in the workplace represent a debated practice when investigating financial crime (Tackett, 2008).

8.1 Value Shop Configuration

Investigation and prevention of cyber crime and building corporate reputation have the value configuration of a value shop. As can be seen in Figure 1, the five activities of a value shop are interlocking and while they follow a logical sequence, much like the management of any project, the difference from a knowledge management perspective is the way in which knowledge is used as a resource to create value in terms of results for the organization. Hence, the logic of the five interlocking value shop activities in this example is of a policing unit and how it engages in its core business of conducting reactive and proactive investigations.

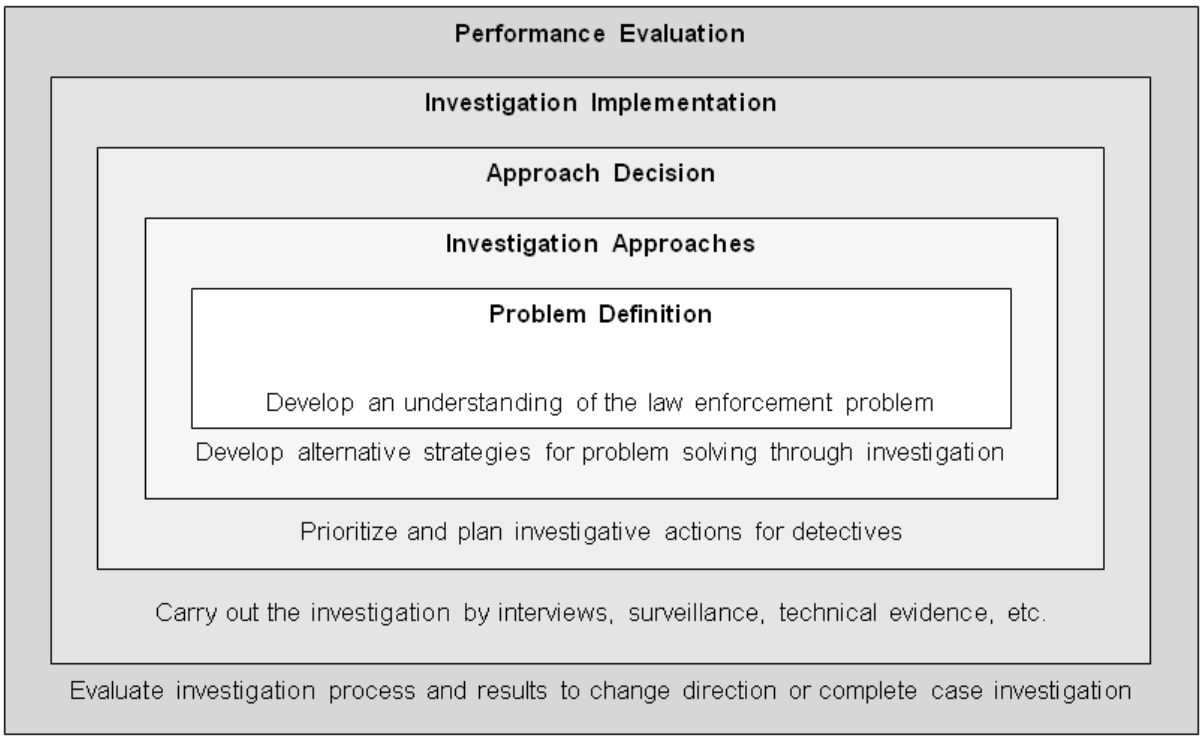


Figure 1. The knowledge organization of investigation and prevention units as value shop activities

The sequence of activities starts with problem understanding, moves into alternative investigation approaches, investigation decision, and investigation implementation, and ends up with criminal investigation evaluation (Sheehan and Stabell, 2007). However, these five sequential activities tend to overlap and link back to earlier activities, especially in relation to activity 5 (control and evaluation) in policing units when the need for control and command structures are a daily necessity because of the legal obligations that policing unit authority entails. Hence, the diagram is meant to illustrate the reiterative and cyclical nature of these five primary activities for managing the knowledge collected during and applied to a specific investigation in a value shop manner.

Furthermore, Figure 1 illustrates the expanding domain of the knowledge work performed in financial crime investigations, starting in the centre with problem understanding and ending at the edge with evaluation of all parts of the investigation process.

These five primary activities of the value shop in relation to a financial crime investigation and prevention unit can be outlined as (Sheehan and Stabell, 2007):

1. *Problem Definition*. This involves working with parties to determine the exact nature of the crime and hence how it will be defined. For example, a physical assault in a domestic violence situation depending on how the responding officers choose and/or perceive to define it can be either upgraded to the status of grievous bodily harm to the female spouse victim or it may be downgraded to a less serious common, garden variety assault where a bit of rough handing took place towards the spouse. This concept of making crime, a term used on how detectives choose to make incidents into a crime or not, is highly relevant here and is why this first activity has been changed from the original problem finding term used in the business management realm to a problem definition process here in relation to policing work. Moreover, this first investigative activity involves deciding on the overall investigative approach for the case not only in terms of information acquisition but also as indicated on Figure 1 in undertaking the key task, usually by a senior investigative officer in a serious or major incident, of forming an appropriate investigative team to handle the case.

2. *Investigation Approaches.* This second activity of identifying problem solving approaches involves the actual generation of ideas and action plans for the investigation. As such it is a key process for it sets the direction and tone of the investigation and is very much influenced by the composition of the members of the investigative team. For example, the experience level of investigators and their preferred investigative thinking style might be a critical success factor in this second primary activity of the value shop.

3. *Approach Decision.* This solution choice activity represents the decision of choosing between alternatives generated in the second activity. While the least important primary activity of the value shop in terms of time and effort, it might be the most important in terms of value. In this case, trying to ensure as far as is possible that what is decided on to do is the best option to follow to get an effective investigative result. A successful solution choice is dependent on two requirements. First, alternative investigation steps were identified in the problem solving approaches activity. It is important to think in terms of alternatives. Otherwise, no choices can be made. Next, criteria for decision-making have to be known and applied to the specific investigation.

4. *Investigation Implementation.* As the name implies, solution execution represents communicating, organizing, investigating, and implementing decisions. This is an equally important process or phase in an investigation as it involves sorting out from the mass of information coming into the incident room about a case and directing the lines of enquiry as well as establishing the criteria used to eliminate a possible suspect from further scrutiny in the investigation. A miscalculation here can stall or even ruin the whole investigation. Most of the resources spent on an investigation are used here in this fourth activity of the value shop.

5. *Performance Evaluation.* Control and evaluation involves monitoring activities and the measurement of how well the solution solved the original problem or met the original need. This is where the command and control chain of authority comes into play for investigation and prevention units and where the determination of the quality and quantity of the evidence is made as to whether or not to charge and prosecute an identified offender in a court of law.

Application of an intelligence strategy in the company should strengthen its core competencies. According to Prahalad and Hamel (1990), core competencies are the collective learning in the organization, especially how to coordinate diverse service skills and integrate multiple streams of technologies. Since core competence is about harmonizing streams of technology, it is also about the organization of work and the delivery of value. Core competence does not diminish with use. Unlike physical assets, which do deteriorate over time, competencies are enhanced as they are applied and shared.

8.2 Investigation Issues

Hinduja (2007) developed a number of issues that are of particular relevance to computer crime investigations. He argues that the following points will result in greater investigative efficacy when addressing high-tech wrongdoing:

- *Role of first-responding officer*. This role in computer crime cases is of critical importance because the evidence associated with cyber crime is often intangible in nature. Certain precautions must be taken to ensure that data stored on a system or on removable media is not modified or deleted - either intentionally or accidentally. Even the simple shutting-down of a computer can change the last-modified or last-accessed timestamp of certain system files, which introduces questions associated with the integrity of the data. To preclude vulnerabilities in the prosecutor's case and to adequately defend against any related challenges, responders should exercise grave care during the search and seizure of computer equipment.

- *Role of investigator*. In traditional crime, a significant amount of information is provided to the responding officer by the victim(s). In computer crime, much effort will be expended in order to identify evidentiary facts, interpret clues, follow leads, and gather data to make a compelling case against the suspect(s). Due to the veiled nature of the techniques associated with computer crime, a victim may have none of little valuable and relevant information for the police investigation.

- *Information, instrumentation, and interviewing*. Information refers to the fact that criminal investigation is centered in the gathering, organizing, and interpreting of data directly or tangentially related to the case. Instrumentation refers to forensic science and specific techniques afforded to crime-solving investigators. Interviewing refers to the process of soliciting and lawfully extracting information from individuals who are knowledgeable about the circumstances of a crime in some capacity. Instrumentation in investigating financially related and profit-oriented crime involving computer systems primarily revolves around the tracking and analysis of records and logs to determine discrepancies or irregularities in the normal order. For example, money laundering with the use of computers concerns the process of concealing the source of illegally obtained money and often involves the creation, fabrication, or alteration of documents to create a legitimate paper trail and history. Interviewing appears to be less salient as a direct method to investigate computer crime, largely because the victim is often unaware (either immediately or even for a great length of time) that a crime has occurred and that harm has resulted. However, interviews can be extremely useful in terms of expert interviews and stakeholder interviews that can provide new insights and new perspectives for the investigation.

- *Evidence collection and processing*. In terms of evidentiary issues, the preliminary strategies associated with computer crime will normally be executed as any other type of crime. Police departments have procedural requirements for evidence collection that is followed, but certain subtleties endemic to computer crime can be noted. The complexity associated with the lack of tangible evidence and an actual crime scene can cause the investigator to concentrate on evidence collection related to individual-level variables as predictors of this form of criminality. The detailed analyses of logs, records, and documents associated with the unlawful transaction or action has to be organized in a structure that is retrievable and combinable as evidence.

Once evidence associated with a computer crime is lawfully discovered, Hinduja (2007) stresses the importance of multiple safeguards to preserve evidence continuity and integrity. Physical and removable media have to be protected because of their sensitive nature. Magnetic fields and even static electricity have the potential to render unusable and unreadable certain electronic equipment such as data storage devices and disks. The suspect should be restricted from the computing environment because of the possibility that digital evidence might be altered or deleted.

8.3 Senior Investigating Officer

The performance of the financial crime investigation and prevention unit should be continually under scrutiny by the executive leadership of the business or public organization. There is widespread recognition within the policing service that there is a need to improve the professionalism of the investigative response. In the UK, the professionalizing investigation program was introduced in 2005 for police units. The purpose is to significantly improve the personal, functional and organizational ability of the service to investigate crime of any category. In performance terms the aim of the program is to deliver (Home Office, 2005b):

- Improved rates of crime detection
- Improvement in the quality of case files
- A reduction in the number of failed trails
- Improved levels of judicial disposal
- Increased public confidence in the police service

The long-term outcomes of the program shall deliver the professional development of staff against robust national occupational standards by developing police staff that is better-qualified and thereby better skilled in investigation, more focused training for investigation, and minimal accreditation bureaucracy.

In all complex or serious cases, on which a team of investigators is deployed, the senior investigating officer sets out what the main lines of enquiry are, and record his or her decisions on those lines of enquiry as the investigation progresses. For example, the SIO directs which policy decisions are recorded in the HOLMES system in the UK. The Major Incident Policy Document is maintained whenever a Major Incident Room using HOLMES system is in operation (Home Office, 2005a).

The SIO plays a pivotal role within all serious crime investigations. Concerns have been expressed, however, that there is a shortage of investigators with the appropriate qualities to perform this role effectively. The consequences of such a shortage could be severe. Not only might it threaten the effective workings of the judicial process, it can also waste resources, undermine integrity and reduce public confidence in the police service. The principal aim of the research conducted by Smith and Flanagan (2000) was to establish what skills, abilities and personal characteristics an SIO ought to possess to be effective in the investigation of low-volume serious crimes (stranger rape, murder and abduction).

Interviews were conducted with 40 officers from ten forces in the UK. These were selected to reflect a range of roles and experience with Criminal Investigation Departments (CID). Ten of these officers were nominated by their peers as examples of particularly effective SIOs.

Although the debate around SIO competencies has often polarized into arguments for and against specialist or generalist skills, the research highlighted the fact that the role of an SIO is extremely complex and the skills required wide-ranging. By applying a variety of analytical techniques, a total of 22 core skills were identified for an SIO to perform effectively in the role. The 22 skills were organized into three clusters:

- *Investigative ability*. This includes the skills associated with the assimilation and assessment of incoming information into an enquiry and the process by which lines of enquiry are generated and prioritized.

- *Knowledge levels*. This relates to the different types of underpinning knowledge an SIO should possess.

- *Management skills*. These encompass a broad range of skill types that were further sub-divided between people management, general management and investigative management.

The research revealed that the effective SIO is dependent upon a combination of management skill, investigative ability and relevant knowledge across the entire investigative process, from initial crime scene assessment through to post-charge case management.

Ideally, an SIO should possess a high level of competency across each of the three clusters. In reality this is not always possible and, when this happens, there is an increased risk that the investigation will be inefficient or, in the worst case, will fail.

For example, an SIO from a predominantly non-CID background will have little experience within an investigative context. Hence there is an increased risk that an investigation will fail due to sub-optimal investigative decisions being made. Similarly, an SIO from a predominantly CID background may have less general management experience. Hence there may be an increased risk of failure from sub-optimal management decisions.

The research suggested that some - but not all - deficiencies in an SIO's skill portfolio can be compensated for by drawing on the skills and abilities of more junior officers within his/her investigative team. However, it was recognized that this was still a high-risk and short-term strategy.

In police investigations the manager of an investigative unit is generally referred to as a SIO. This is a middle management type position in the command and control hierarchy of a police organization. Such a middle ranking position carries much responsibility for making sure an investigation stays on track, within budget and produces good results in terms of evidence and prosecution. Such responsibility places strong leadership demands on an SIO. Hence, Mintzberg's (1994) research on management roles is relevant and provides a firm basis on which to appreciate and understand the inter-related activities of a manager.

A manager's job consists of several parallel roles. At a certain point in time, the manager may perceive one role as more important than the others. Mintzberg (1994) found that it is a peculiarity of the management literature that its best-known writers all seem to emphasize one particular part of the manager's job to the exclusion of the others. Together they cover all the parts, but even that may not describe the whole task of managing.

Mintzberg's role typology is frequently used in studies of managerial work. When such role terminology is applied to a financial crime investigation and prevention context, some modification is required as an SIO will not necessarily be responsible for all aspects of each role. Furthermore, business management terminology does not fit so well in a policing and law enforcement domain. Hence, some of the role labels have been changed to provide a more accurate fit with police terminology.

These six policing manager roles for corporate social responsibility are briefly described below along with the police-specific role label noted in brackets.

- ***Personnel leader*** **(Motivating Role)**. As a leader, the manager is responsible for supervising, hiring, training, organizing, coordinating, and motivating a cadre of personnel to achieve the goals of the organization. This role is mainly internal to the investigation and prevention unit. As stated previously, an SIO would not be generally be responsible for hiring a particular individual in a business sense, but would have a say in which particular investigator might join his team for a particular investigation. However, the main thrust of this role for an SIO is that of motivating his/her staff and keeping such motivation up especially in a difficult and protracted investigation.

- ***Resource allocator*** **(Resourcing Role)**. The manager must decide how to allocate human, financial and information resources to the different tasks of the investigation. This role emphasizes planning, organizing, coordinating and controlling tasks, and is mainly internal to the financial crime investigation and prevention unit. Often, an SIO has to be an advocate in this regard to get the necessary resources for his team to be able to conduct the investigation efficiently and effectively.

- ***Spokesperson*** **(Networking Role)**. As a spokesperson, the manager extends organizational contacts to areas outside his or her own jurisdiction. This role emphasizes promoting acceptance of the unit and the unit's work within the organization of which they are part. For the manager it means contact with the rest of the organization. Frequently, he or she must move across traditional departmental boundaries and become involved in personnel, organizational and financial matters. Hence, with regard to an SIO this key role is one of networking within the business organization.

We distinguish between the following roles as illustrated in Figure 2:

- ***Entrepreneur*** **(Problem-solving Role)**. The manager identifies the policing needs and develops solutions that change situations. A major responsibility of the manager is to ensure that rapidly evolving investigation methods are understood, planned, implemented, and strategically exploited in the organization. Such a role is more akin to being a problem-solver than an entrepreneur in a policing setting.

- ***Liaison*** **(Liaising Role)**. In this role, the manager communicates with the external environment, and it includes exchanging information with government agencies, private businesses, and the media. This is an active, external role. This is a very similar role description for an SIO who has to liaise with a wide range of people throughout an investigation who are external to the investigation and prevention unit like executive management but which are part of the overall criminal justice system in the organization.

- ***Monitor* (Gatekeeping Role)**. This role emphasizes scanning of the external environment to keep up with relevant changes, such as politics and economics. The manager identifies new ideas from sources outside his or her organization. To accomplish this task, the manager uses many resources, including vendor contacts, professional relationships, and a network of personal contacts. While an SIO clearly monitors the progress or otherwise of an investigation, the role description here is more like a gatekeeping role. In that it is not so much external politics or economics, which an SIO has to contend with but rather making sure the media and other outside forces do not disrupt the progress on an investigation. Hence, in that sense this is a gatekeeping role to protect the investigative team and undue external pressure.

These investigation and prevention manager roles are illustrated in the figure. As can be seen the motivating and resourcing roles are internal to the investigation team for the SIO. The networking and problem-solving roles are directed towards the policing organization, and the liaising and gatekeeping roles are linked to the external environment for the SIO.

We would expect that these roles are not equally important for a SIO in relation to creating investigative success. Moreover, some roles may be more influential in terms of stimulating knowledge sharing. For example, adopting a motivating role may be more important for an SIO to engage in within the investigative team, but not as important in relation to the wider policing organization. There is some research that suggests that the networking role (or spokesperson) is the most important for dealing with the larger organization when knowledge is communicated to stakeholders (Lahneman, 2004).

A survey instrument was applied in this research, where respondents filled in a space. In the open electronic space, respondents could write five characteristics in their own wording. To classify these responses, content analysis was needed. According to Riffe and Freitag (1997), seven features of content analysis distinguish poor studies from excellent studies. First, an explicit theoretical framework is needed. In this research, the theoretical framework of management roles as developed by Mintzberg (1994) is applied. Second, hypotheses or research questions are needed. In this research, the research question 'what' is concerned with descriptions of characteristics. Third, other research methods should also be applied. In this research, a survey is supplemented with content analysis. Forth, extra-media data should be incorporated. In this research, results from another investigation survey were incorporated. Fifth, inter-coder reliability should be reported. In this research, the characteristics content construct was coded by two researchers independently. Sixth, reliability based on random sample of coded content was not relevant in this research, as there is a complete set of responses. Finally, presentations of only descriptive statistics should be avoided.

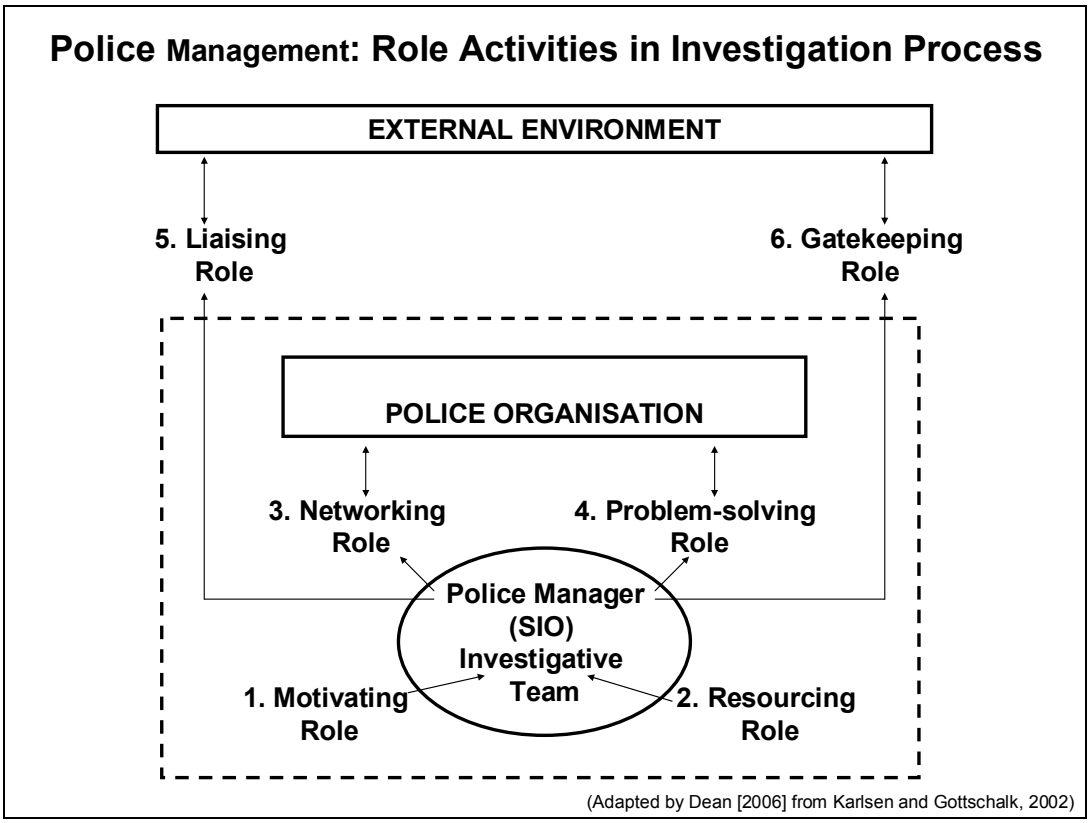


Figure 2. Manager roles in financial crime investigation and prevention

The questionnaire was sent to 325 detectives by email. With 110 responses returned, this gave a response rate of 34%. However, only 71 detectives filled in the open space for characteristics of effective detectives, thereby reducing the response rate to 22%. Since each detective wrote five characteristics each, a total of 355 characteristics were collected, as listed in Table 1.

Two raters were involved in the classification of responses. There was no need to develop key words in this research, as respondents provided responses in terms of key words. Acceptable inter-rater judgment reliability (IJR) of 0.94 was achieved. Reliability is an assessment of the degree of consistency between multiple raters of a variable (Hair et al., 2006).

Objectivity	Cooperative skills	Authority when needed	Keeping overview	Organizational skills
Creative	Investigative knowledge	Cooperative skills	Organizational skills	Motivational skills
Creative	Motivational skills	Listening skills	Participating in work	Managing the case
Curious	Detailed	Knowledge of law	Not giving up	Human knowledge
Motivational skills	Inspirational	Professional	Patient	
Open mind	Communicative skills	Empowering skills	Exploring personnel	Analytic skills
Communicative skills	Feedback skills	Identifying connections	Investigative knowledge	Resisting pressure
Experience	Broad competence	Action oriented	Understanding the case	
Communicator	Good listener	Ability to motivate	Avoiding details	Creating ideas
Investigative insights	Integrity	Ability to listen	Judgment	Decision maker
Analytic skills	Creative	Systematic	Showing empathy	Good leader
Objective	Sensitive	Analytic	Structured	Creative
Listening to others	Experienced in the field	Motivational	Good mood	Make decisions
Ability to lead	Find good solutions	Value employees	Cooperation	Good mood every day
Clever at organizing	Clear speech	Cooperative	Creative	Lots of experience
Good organized	Speed	Knowledgeable	Good memory	Divide work
Good overview	Delegation skills	Analytic ability	Team leadership	Motivational skills
Stimulate officers	Delegate	Humor	Structured	
Ability to communicate	Positive attitude	Flexibility	Investigative knowledge	Involvement
Structure	Goal oriented	Self confidence	Engaged	Creative
Motivational	Engaged	Analytic	Professional skills	Systematic
Seeing the whole picture	Motivator	Good at delegating	Good feedback	Does care
Ability to supervise	Knowledge of the cases	Ability to delegate	Investigative knowledge	Open minded
Openness	Organized	Motivating	Results oriented	Fair
Systematic	Thorough	Honest	Calm	Empathetic
Objectivity	Good at listening	Good mood	Ability to prioritize	Having good overview
Motivational	Systematic	Good communication	Human	Balanced
Concrete	Caring	Thorough	Open to proposals	Experience
Patient	Seeking options	Listening	Motivational	Giving feedback
Results oriented	Not afraid	Communicative skills	Stimulate employees	Action oriented
Leadership skills	Offensive	Active	Curious	Fair
Cooperative skills	Structured	Creative	Listening	Engaged
Investigative insights	Ability to receive	Ability to systematize	Ability to delegate	Ability to motivate
Structured	Investigative knowledge	Fair	Positive attitude	Ability to have oversight
Understanding	Honesty	Offensive	High moral	Objective

people				
Creative	Encouraging	Open	Knowledgeable	Overview
Cooperative skills	Sees person potential	Ability to listen	Tactical	Open to new ideas
Knowledgeable of law	Delegating	Being creative	Make decisions	Motivate officers
Ability to see all	Ability to inspire	Ability to listen	Ability to implement	Ability to correct
Professional	Decision oriented	Engaged	Motivational	Team leader
Human	Professional	Openness	Honesty	Energy
Investigative insights	Motivational	Including	Ability to delegate	Goal oriented
Broad experience	Ability to cooperate	Listen to others' opinions	Being explicit	Ability to delegate
Open mind	Good at communicating	Decision minded	Investigative knowledge	Present
Distribute tasks	Thinking creatively	Good monitoring	Good consulting	Thinking new
Having good overview	Give credit and criticism	Good at encouraging	Suggesting solutions	Ability to cut the crap
Mature soul	Investigative level	Good organizer	Communicative skills	Contribute to openness
Communication	Humility	Authority	Self insight	Humor and good mood
Open to proposals	Let others lead	Give feedback	Push progress	Make decisions
Systematic	Analytic	Creative	Determined	Knowledgeable
Good team leader	Stimulating creativity	Having overview	Open minded	Patient
Motivator	Keeping calm	Decision power	Creative	Listening
Objectivity	Listen	Leading	Think new	Cooperation
Professional skills	Thorough	Create team feeling	Ability to motivate	Analytic ability
Motivational	Ability to stimulate	Communicative skills	Including personnel	Systematic
Leadership skills	Investigative skills	Organizational skills	Creative	Supervising skills
Stimulating team	Full of initiatives	Knowledgeable	Involving officers	Clear messages
Listening	Relevant attitude	Objective	Humble	Person oriented
Open	Creative	Innovative	Inspirational	Integrity
Knowing how to motivate	Able to cooperate	Thinking creatively	Being structured	Being effective
Creative	Motivational	Listening	Social	Investigative competent
Integrity	Objective	Cooperative skills	Reliable	Experience
Objective	Motivational	Structured	Competent	Thinking systematically
Investigative strengths	Ability to lead	Having good overview	Being creative	Good to communicate
Knowledge	Experience	Attitude	Patience	Overview
Ability to motivate	Ability to listen	Investigative competence	Identifying limitations	Creativity
Good to communicate	Ability to delegate	Ability to prioritize	Decision power	Ability to cooperate
Ability to motivate	Ability to be critical	Decision making ability	Ability to delegate	Ability to evaluate
Ability to motivate	Having patience	Relevant experience	Being team oriented	Listen to others

Motivator	Listening	Supervising	Create good environment	Let all in the team act
Focus	Cooperative skills	Knowledge	Creativity	Humility

Table 1. *Characteristics of effective SIOs according to respondents (5 characteristics by 71 respondents)*

As can be seen in the table, most respondents provided 5 characteristics of effective SIOs as requested. Only three respondents provided 4 characteristics. A total of 352 characteristics represent our data in this research. Respondents were not asked to prioritize their five characteristics. Therefore, all 352 characteristics are treated as equally important in this research.

Our first analysis was simply to look for words, which were mentioned by several respondents. We find words such as 'creativity', 'communication', and 'cooperation', indicating that the manager of the investigation should contribute with new ideas (creativity), should talk to people (communication) and should work with people (cooperation).

Our second analysis was concerned with person focus versus task focus. It was assumed that SIOs tend to be task focused, while investigators would like them to be more person focused. When classifying all responses in Table 7.1 along these two categories, we found that 54% of the statements are person focused, while 46% are task focused.

Our third analysis was classification of items in the table according to management areas.

We make distinctions between four management areas:

- *Task management*. Managing the tasks of the investigation.
- *Person management*. Managing the officers involved in the investigation.
- *Administration management*. Managing the systems supporting the investigation.
- *Strategy management*. Managing the direction of the investigation.

When independent raters applied this classification scheme to the 352 items in Table 7.1, the following distribution emerged:

- 40 percent of the characteristics were assigned to *person management*.
- 30 percent of the characteristics were assigned to *task management*.
- 18 percent of the characteristics were assigned to *strategic management*.
- 12 percent of the characteristics were assigned to *administrative management*.

The fourth analysis was concerned with our adoption of Mintzberg's (1994) management roles into motivating role, resourcing role, networking role, problem-solving role, liaising role, and gatekeeping role. Although not explicitly asked for, characteristics of effective detectives can be interpreted in terms of their importance to the management roles. Each characteristic might be assigned to one of the roles according to importance of the characteristic in that specific role. This was done in the research, which resulted in the following distribution:

- 38 percent of the characteristics were assigned to the motivating role of *personnel leader*.
- 23 percent of the characteristics were assigned to the resourcing role of *resource allocator*.
- 11 percent of the characteristics were assigned to the networking role of *spokesperson*.
- 19 percent of the characteristics were assigned to the problem-solving role of *entrepreneur*.
- 5 percent of the characteristics were assigned to the liaising role of *liaison*.
- 4 percent of the characteristics were assigned to the gatekeeping role of *monitor*.

The fifth and final analysis was concerned with the distinction between investigative ability, knowledge levels, and management skills, as suggested by Smith and Flanagan (2000). When these three categories were applied to Table 1, we found 38% investigative ability, 9% knowledge, and 53% management skills as characteristics of effective SIOs as defined by investigators.

Survey results indicate that the most important leadership role for SIOs is the motivating role of the personnel leader. In this role, the SIO is responsible for the supervising, hiring, training, organizing, coordinating, and motivating a cadre of personnel to achieve the goals of the organization. This role is mainly internal to the police investigation unit. As stated previously, an SIO would not be generally be responsible for hiring a particular individual in a business sense, but would have a say in which particular police investigator might join his team for a particular investigation. However, the main thrust of this role for an SIO is that of motivating his/her staff and keeping such motivation up especially in a difficult and protracted investigation.

In different study, we asked SIOs how they would rate the importance of each leadership role. Their results are listed in Table 2. SIOs themselves find the problem-solving role most important (5.0), followed by the resourcing role (4.8).

Management roles in police investigations	**Mean**
Motivating role - responsible for guiding and follow-up personnel who participate in the investigation	4.7
Resourcing role - making decisions about allocation of resources in the investigation	4.8
Networking role - informing other involved units in the Police about the investigation	4.4
Problem-solving role - identifying opportunities and initiatives in the investigation	5.0
Liaising role - managing information & knowledge about external matters that might be relevant for the investigation	4.6
Gatekeeping role - communicating with the external environment about the progress in the investigation	4.4

(Scale: 1=not important to 7=very important)

Table 2. Measurement of management roles

When compared to the current responses from detectives, we find some interesting results. While the SIOs do not find the motivating role particularly important, detectives that are supervised by SIOs find this role most important. Opposite, while SIOs find the problem-solving role most important, detectives do not find this role particularly important.

When combining the results from all five analyses, we find than an effective detective is characterized by being person focused in person management as a personnel leader with management skills.

Two important limitations in the current study have to be addressed. First, the response rate of 22 percent is low. As there were no follow-ups in the survey administration, and responding to each open-ended question was voluntary, the response rate as such is as expected. However, a bias in responses is not unlikely, limiting the possibility of generalized findings. For example, only detectives with strong opinions about leadership and management may have articulated their views in the survey. Future research designs should strive for higher response rates and include contacting some random non-respondents.

Second, the construct 'effective' SIOs is problematic. Implicitly, we argue that there is a significant, positive relationship between detectives' opinions and actual effectiveness, since we only measured what detectives consider to be effective. Also, since effectiveness was not defined in the questionnaire, responding detectives might have emphasized very different interpretations of this construct. Future questionnaire designs should strive to solve such research design problems.

Effective SIOs as evaluated by their subordinates are characterized by being person oriented rather than case oriented. Important skills are motivational skills, communicative skills, listening skills, and organizational skills. According to this study, the least important for SIOs is investigation knowledge, when compared to investigative ability and management skills.

8.4 Electronic Evidence

Electronic evidence and computer forensics have become essential for responding to legal actions against financial crime. More and more of the evidence for crimes such as fraud, theft, corruption and embezzlement is in digital form. Legal cases today increasingly rely on evidence represented as digital data stored on computers and storage media. In legal actions, organizations are obligated to respond to a discovery request for access to information that may be used as evidence in court, and the organization is required by law to produce those data. Courts all over the world now impose severe financial and also criminal penalties for improper destruction of electronic documents that should have been stored safely and retrievably (Laudon and Laudon, 2010).

Laudon and Laudon (2010) argue that all organizations should have an effective electronic retention policy that ensures that electronic documents, e-mail, and other records are well organized, accessible, and neither retained too long nor discarded too soon. It also reflects an awareness of how to preserve potential evidence for computer forensics.

Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. Computer forensics or digital forensics is the art and science of applying computer science to aid the legal process. It is more than the technological, systematic inspection of electronic systems and their contents for evidence or supportive evidence of a criminal act. Digital forensics requires specialized expertise and tools when applied to intelligence in important areas such as financial crime. As a term, digital forensics refers to the study of technology, the way criminals use it, and the way to extract and examine digital evidence (Ferraro and Casey, 2005).

Digital forensics is an approach to identifying evidence from computers that can be used in trials. A typical forensics investigation consists of two main phases, exploration and evidence respectively. During the exploration phase, investigators attempt to identify the nature of the problem and what exactly happened or is expected to happen at the crime scene. The evidence phase takes place after the exploration has been concluded. It consists of accumulating all documentation, which will work in court.

From a data viewpoint, this two-phase procedure can be broken down into six stages: preparation, incident response, data collection, data analysis, presentation of findings, and incident closure. Some of these stages may be so complex in certain circumstances that they are divided into sub-stages. The most time consuming tasks in digital forensics investigation are searching, extracting, and analyzing. Therefore, there is a need for a forensics model that allows formalization of the digital forensics process, innovative data mining techniques for the forensics process, and a dedicated infrastructure for digital forensics.

Computer forensics deals with the following problems (Laudon and Laudon, 2010: 338):

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

Laudon and Laudon (2010) argue that an awareness of computer forensics should be incorporated into an organization’s contingency planning process. The CIO, security specialists, information systems staff, and corporate legal counsel should all work together to have a plan in place that can be executed if a legal need arises.

8.5 How Detectives Work

According to Tong (2007), the secretive nature of the detective world has attracted little attention from researchers. However, competing perspectives about detective work can be discerned from available literature. Detective work has been characterized as an art, a craft, a science, and a combination of all three. The old regime of the seasoned detective highlighted the notion of detective work as a craft. An alternative perspective highlights the scientific nature of detective work, which focuses on the skills needed for crime scene management, the use of physical evidence, investigative interviewing, informant handling, offender profiling, management of the investigative process, and knowledge management.

It is important for detectives to be effective in their work, as new public management is focusing closely on the effective use of resources. However, measuring effectiveness is no easy task. Measurement, in an investigative context, has focused upon the outcome of cases, often at the expense of evaluating the process of the investigation and quality of its outputs. Tong (2007) argues that not only have the police been subject to inadequate measurement criteria such as clear-up rates, there has also been a lack of recognition of good quality police work. The task of recognizing good detective work involves more than providing an appropriate method of measurement; it also implies an awareness of the impact of practice as well as an awareness of the knowledge accumulation, sharing and reuse.

It follows that the most useful approach to measuring detective effectiveness will not necessarily be the measurement of specific outcomes, although such measures will be useful for resource management. Tong (2007) argues that effectiveness in the context of detective work is best measured by focusing on the key processes and decisions in which detectives engage to encourage a professional working culture based on how detectives come to decisions. In the context of the value shop for knowledge work, decisions are made in all five primary activities: understanding the problem, identifying problem solutions, prioritizing actions, implementing investigation, and evaluating and controlling detective work.

Tong (2007) constructed the following profile of an effective detective after analyzing the academic literature relating to detective skills and abilities:

1. *Personal Qualities.* Intelligence, common sense, initiative, inquisitiveness, independence of thought, commitment, persistence, ability to talk to people, flexibility, ability to learn, reflexivity, lateral thinking, creative thinking, patience, empathy, tolerance and interpreting uncertain and conflicting information, ability to work away from family and home, interpreting feelings, ideas and facts, honesty and integrity.

2. *Legal knowledge.* Knowledge of the law referring to police powers, procedure, criminal justice process, a good grounding in criminal law, awareness of changes to legislation, courtroom protocol, rules of disclosure, use of evidence, format of case file and awareness of defence arguments.

3. *Practical knowledge.* Technology available to detectives and used by criminals, understanding the context in which crime is committed and awareness of investigative roles of different functions of the police organization and specialist advisors. Recognition that crime changes with time and place and may require police responses that are tailored to specific context. Forensic awareness and practical expertise (e.g. crime scene preservation and packaging of evidence).

4. *Generic knowledge.* Recognition that knowledge changes, awareness of developments in practice will allow the detective to remain up to date.

5. *Theoretical knowledge.* Understanding of theoretical approaches to investigative reasoning and theories of crime.

6. *Management skills.* The management and control of case information, implementing investigative action, formulating investigative strategies, verify expert advice, prioritize lines of enquiry, formulate media strategies, awareness of resource availability and knowledge of roles of personnel available to the investigation. Manage knowledge and learning through the use of research skills to enable the detective to remain up to date.

7. *Investigative skills.* Interview technique, presenting evidence, cultivating informants, extracting core information (from files, reports, victims and witnesses), file construction, appraising and evaluating information, ability to absorb and manage large volumes of information, statement taking, problem-solving, formulating lines of enquiry, create slow time, assimilate information from crime scene, continually review lines of enquiry, question and challenge legal parties.

8. *Interpersonal skills.* Ability to communicate and establish a rapport with a range of people, remain open minded, awareness of consequences of actions and avoid speculation.

Stelfox and Pease (2005) argue that there has been surprisingly little empirical research into the way in which individual officers approach the task of investigating crime. In their own research they found that investigators are practical people. Assuming that the cognitive abilities of the average investigator are no more nor less than the population as a whole, it can be anticipated that he or she will remain liable to make the same cognitive errors as the rest of us. Assuming also that the decision-making environment the detective works in is unlikely to change much, it can be anticipated that errors will recur.

Intelligence has emerged as an important component of contemporary policing strategies. However, Innes et al. (2005) argue that crime intelligence analysis is used in line with traditional modes of policing; is a way of claiming 'scientific objectivity' for police actions; and is largely shaped by police perspectives on data. They argue that the sense of enhanced objectivity often attributed to the products of 'intelligence work' is frequently overstated. Therefore, the products of crime analysis might better be understood as an artifact of the data and methods used in their construction, rather than providing an accurate representation of any crime problems.

Added to which, Innes et al. (2005) found that there has been increasing frustration within certain sections of the police organization, with the perceived failure of community-policing programs to facilitate the routine supply of high-quality information to the police from members of the community. Any such concerns with low policing have been reinforced and amplified by recent developments at the 'high policing' level, where there is a well documented shift towards trying to effect enhanced national security from threats posed by terrorist groups, drug cartels and organized-crime networks.

The presence of criminal markets and networks implies a degree of organization to the conduct of crime. In turn, this serves to recursively justify the investment in technologies of analysis. It signals to the police themselves that simply arresting isolated individuals will have only a temporary effect on crime levels, before the adaptive qualities and replacement mechanisms of the surrounding networks and markets cause them to reform. Therefore, they need to conduct analysis so as to improve their awareness of the shape and make-up of the supporting networks and markets in which motivated criminals are located, so that any interventions taken against them are made to have more impact (Innes et al., 2005).

One of the bottlenecks in international police cooperation is the targeting of the proceeds of crime. International agencies such as Interpol and Europol are sometimes involved in the interaction between the authorities and enforcement organizations of the countries concerned. Borgers and Moors (2007) studied bottlenecks in international cooperation for the Netherlands in targeting the proceeds of crime. While no bottlenecks were found in cooperation with countries such as Belgium and the United Kingdom, bottlenecks were found in relation with countries such as Spain and Turkey. In relation to Turkey, the Netherlands acts mainly as the requesting state and not the requested state (Borgers and Moors, 2007: 8):

> Regarding the cooperative relations with Turkey, Turkish respondents state that the framing of Dutch mutual assistance requests is inadequate. On the part of the Netherlands, there are different opinions on the depth of the investigation conducted at the request of the Netherlands. As far as the way in which people address one another is concerned, it is striking that the Turkish respondents sometimes consider the Dutch manner of operation as haughty and impatient. According to Dutch respondents, communication difficulties also occur if Dutch police officials directly contact the Turkish judges involved.

To fight organized crime, law enforcement in the UK reorganized. The United Kingdom's Serious Organized Crime Agency (SOCA) commenced operations in 2006 with an annual budget of £400 million. SOCA amalgamates the National Crime Squad, the National Criminal Intelligence Service (NCIS), and investigators from Customs and the Home Office's Immigration Service (Segell, 2007).

8.6 Detective Thinking Styles

In criminal investigations, detectives apply different thinking styles, such as method style, challenge style, skill style, and risk style. In a survey in Norway, detectives were asked to list the five most important characteristics of effective investigators. This was done in a free format, requiring content analysis to categorize responses. Responses were categorized according to thinking styles. While creativity was the most frequently mentioned characteristic, content analysis shows that the skill style of detectives is the most effective thinking style. To be effective, detectives need to practice good empathic communication, open-minded curiosity, logical reasoning, creative thinking, and dogged determination.

Creativity is often mentioned as a characteristic of effective detectives. Detectives can be creative in their job by generating new ways to perform their work, by coming up with novel procedures and innovative ideas, and by reconfiguring known approaches into new alternatives (Perry-Smith and Shalley, 2003). Yet, detectives are often told to work by the book, forgetting the importance of creative thinking and the importance of creative persons.

We distinguish between four thinking styles in police investigations. The method style is driven by procedural steps and conceptual processes for gathering information. The challenge style is driven by intensity of the job, the victim, the criminal and the crime. The skill style is driven by personal qualities and abilities of relating to people at different levels. The risk style is driven by creativity in discovering and developing information into evidence.

These four investigative thinking styles as illustrated in Figure 7.3, were introduced in this book to classify characteristics of effective detectives into relevant thinking styles. Such classification enables identification of important thinking styles and learning forms (Garcia-Morales et al., 2006).

Our study was concerned with how police detectives experience, understand, and think about the process of doing serious and complex criminal investigations. In police investigations, the experience of investigation begins for detectives when they are given a crime to solve. When handed a case detectives apply the basics of the procedural method they were trained in.

There are a variety of procedural steps within the criminal investigation training literature for various types of crimes but in essence all such steps follow a logical sequence that can be subsumed under a set of basic steps, referred to as the ’5 C’s’ of the police procedural method of investigation. The 5 C’s are the procedural steps of - collecting, checking, considering, connecting, and constructing – information into evidence.

Conceptually, this ‘procedural method’ presents a problem for detectives in that since their formal investigative training only equips them with this one way of ‘thinking’ investigation, the question becomes how do they learn to think in any other way or do they when investigating?

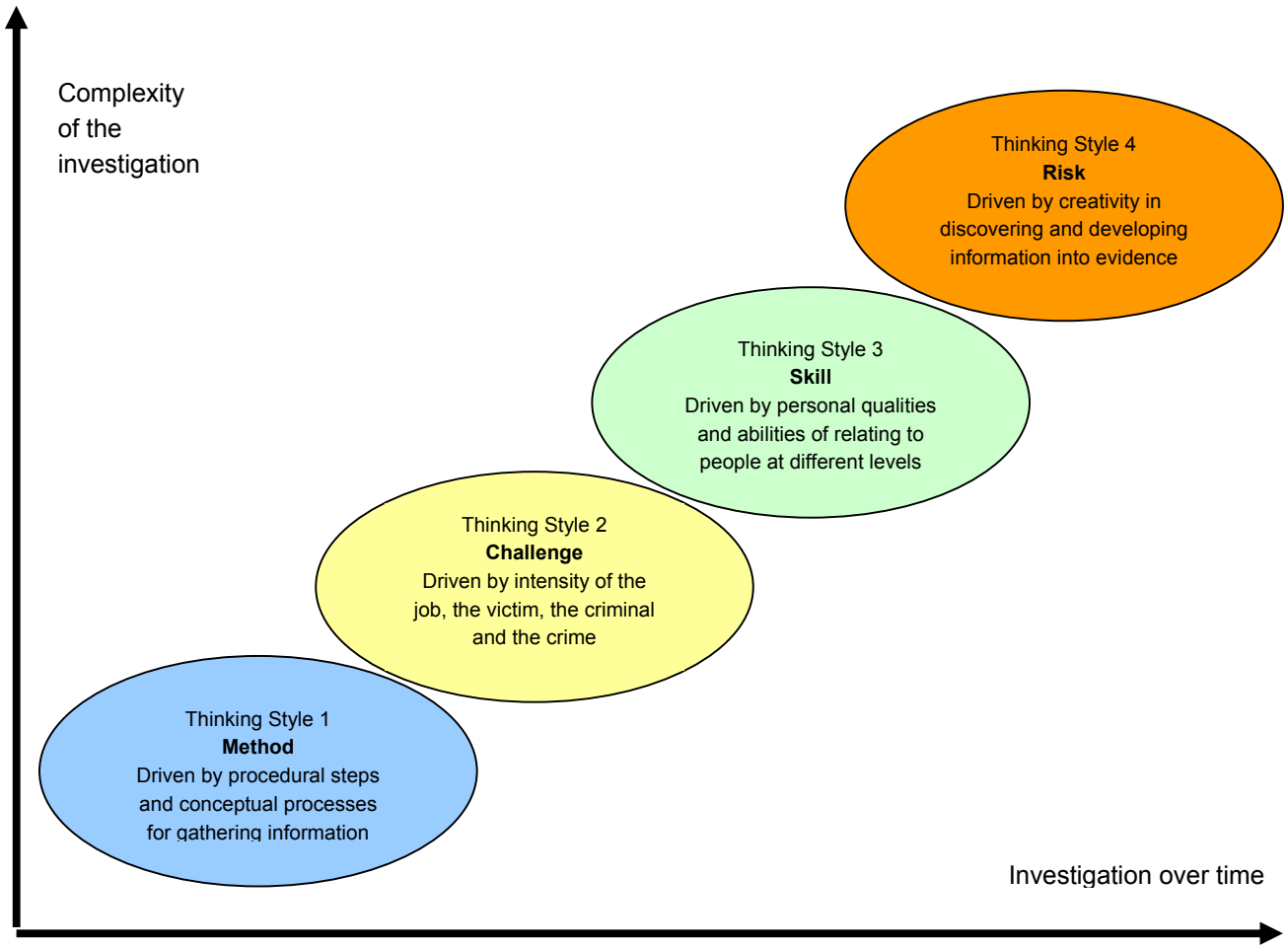


Figure 3. Ways of thinking about the investigation process

Previous empirical research has identified that apart from the above mentioned 'method' style of investigative thinking there are three other qualitatively different ways or styles of thinking that potentially can come into play when detectives investigate a crime. The three other styles or preferred ways of thinking about the investigative process that experienced detectives use with serious and complex crimes are the challenge style, the skill style, and the risk style of investigative thinking. How each of these other three investigative thinking styles works in conjunction with the basic method style is briefly outlined.

As detectives conduct a serious and/or complex investigation, they become driven by the intensity of the challenge, which motivates them to do the best job they can for the victim(s) by catching the criminal(s) and solving the crime through the application of the 'basic 5C's' of the investigative method style of thinking they were trained in. This challenge style of thinking is all about what motivates that drive detectives to do the best they can do in a particular investigation (Home detectives. At this level detectives think about the job, the victim, the crime, and the criminal. These four elements (job-victim-crime-criminal) are the key sources of intensity (Home Office, 2005b).

In meeting this investigative challenge detectives require skill to relate and communicate effectively to a variety of people to obtain information so as to establish a workable investigative focus (Kiely and Peek, 2002). Such skill also requires detectives to be flexible in the how they approach people and the case, while maintaining an appropriate level of emotional involvement towards victims, witnesses, informants, and suspects. With this skill style of investigative thinking, detectives are concerned with how they relate to people. Detectives must think about how they are going to relate to the victim, witnesses, possible suspects, the local community, and the wider general public in order to get the information they need to make the case.

When exercising their investigative skill detectives seek to maximize the possibilities of a good result by taking legally sanctioned and logically justifiable risks across wide latitude of influence. Such justifiable risk-taking requires detectives to be proactive in applying creativity to how they seek to discover new information and, if necessary, how they develop such information into evidence. This risk style revolves around how detectives think through being proactively creative enough to discover new information and if necessary develop it into evidence that will stand up to testing in a court of law.

Although experienced detectives and investigators intuitively use these four levels of thinking in an investigation, it is rare that any one detective will give equal weight to all four styles of investigative thinking in a particular case, because detectives like everyone else, have a preference for maybe one or two particular styles or ways of thinking.

This phenomenon is about the cognitive psychology of police investigators. At its core, investigation is a mind game. When it comes to solving a crime, a detective's ability to think as an investigator is everything. Four distinctively different ways of thinking are investigation as method, investigation as challenge, investigation as skill, and investigation as risk. All four ways of describing a criminal investigation can be seen as more or less partial understandings of the whole phenomenon of investigation.

The four distinctively different ways of thinking (styles) about the investigation process by detectives is illustrated in the figure. As can be seen in the figure, there is a hierarchical structure to how investigators think. Not all cases will require the use of all four investigation-thinking styles to solve them. However, as time matches on in an investigative without a result then other styles of investigative thinking will need to come into play to increase the likelihood of a successful outcome. In essence, the more complex the crime the higher the investigative thinking style required solving it.

8.7 The Case of Økokrim in Norway

The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) is tasked with combating economic crime, environmental crime and the laundering of proceeds of crime. The work entails mainly investigating and prosecuting specific criminal cases. Økokrim (NAIPEE) is a national centre in the Norwegian police in combating financial crime. Økokrim is both a police specialist agency and a public prosecutor office with national authority (Økokrim, 2008).

Investigation work is carried out by permanent and interdisciplinary teams at Økokrim (2008). There were 12 such teams in 2007. Each individual team has primary responsibility for specific areas, and most teams are primarily tasked with investigating and prosecuting their own criminal cases. The teams were: (i) tax and duties team, (ii) fraud team, (iii) corruption team, (iv) securities team, (v) criminal assets team, (vi) financial intelligence unit, (vii) tax and competition team, (viii) bankruptcy team, (ix) subsidies fraud team, (x) stolen goods and money laundering team, (xi) assistance team, and (xii) environmental team.

The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) is a resource centre for the police and the prosecuting authorities in combating these types of crime. Økokrim was established in 1989, and is both a police specialist agency and a public prosecutor´s office with national authority. The formal rules for Økokrim can be found in chapter 35 of the Prosecution Instructions. Økokrim´s main objective is to combat economic crime, environmental crime and laundering of proceeds of crime. Økokrim has approximately 136 employees.

Økokrim´s tasks are to:

- Uncover, investigate, prosecute and bring to trial its own cases
- Assist the national and international police and prosecuting authorities
- Boost the expertise of the police and the prosecuting authorities and to provide information
- Engage in criminal intelligence work, dealing in particular with reports of suspicious transactions
- Act as an advisory body to the central authorities
- Participate in international cooperation

Deterrence is one of our main objectives. Though our work on specific criminal cases, we demonstrate to the public that anyone breaking the rules in our area of jurisdiction will be liable to penalties. Most of Økokrim´s resources are devoted to working on specific criminal cases.

Økokrim engages in extensive external training and information work in the form of talks, lectures and presentations at meeting, conferences and seminars. Such training and information measures also have a preventive effect. Økokrim actively uses its website to provide information about court sentences and other news, and to inform and provide warnings about different forms of crime (e.g., Nigerian scams, investment scams and various Internet and e-mail scams).

Økokrim has been heavily critized in the media for public exposure of suspects and long investigation periods. In terms of public exposure, Økokrim tends to carry out razzias in the beginning of an investigation, thereby attracting media attention. A short while after the razzia in offices or homes, media is able to identify suspects and publish pictures of the suspects, their homes and families. In terms of long investigation period, it is not uncommon that it takes more than a year for Økokrim before they decide to prosecute or to dismiss the case. In the meantime, suspected white-collar criminals have been exposed in the media, and everyone remembers them as criminals, even though they were never convicted (DN, 2009).

References

Abbasi, A., Zhang, Z., Zimbra, D. and Chen, H. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory, *MIS Quarterly*, 34 (3), 435-461.

Abdolmohammadi, M.J. and Read, W.J. (2010). Corporate Governance Ratings and Financial Restatements: Pre and Post Sarbanes-Oxley Act, *Journal of Forensic & Investigative Accounting*, 2 (1), 1-44, www.buis.lsu.edu/accounting/faculty/lcrumbley/jfia/Articles.htm.

Abramova, I. (2007). The funding of traditional organized crime in Russia. *Economic Affairs*, Institute of Economic Affairs, March, 18-21.

Afuah, A. and Tucci, C.L. (2003). *Internet business models and strategies*, 2nd edition, New York: McGraw-Hill.

Al-Kashif, M. (2009). Shari'ah's normative framework as to financial crime and abuse, *Journal of Financial Crime*, 16 (1), 86-96.

Alalehto, T. (2010). The wealthy white-collar criminals: corporations as offenders, *Journal of Financial Crime*, 17 (3), 308-320.

Ampratwum, E.F. (2009). Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA), *Journal of Financial Crime*, 16 (1), 67-79.

Araujo, R.A. (2009). Are labour contracts efficient to combat fraud? *Journal of Financial Crime*, 16 (3), 255-261.

Australian (2008). Online child grooming laws, *Australian Institute of Criminology*, Project 0074a, Australian Government, www.aic.gov.au.

Bachmann, M. (2007). Lesson Spurned? Reactions of Online Music Pirates to Legal Prosecutions by the RIAA, *International Journal of Cyber Criminology*, 1 (2), 213-227.

BBC '*MySpace Bars 29,000 Sex Offenders'* 25th July 2007
http://news.bbc.co.uk/2/hi/technology/6914870.stm

Bennet, A. and Bennet, D. (2005a). Designing the Knowledge Organization of the Future: The Intelligent Complex Adaptive System, In: Holsapple, C.W. (editor), *Handbook of Knowledge Management*, Springer Science & Business Media, Netherlands, Volume 2, 623-638.

Bennet, D. and Bennet, A. (2005b). The Rise of the Knowledge Organization. In: Holsapple, C.W. (editor), *Handbook of Knowledge Management*, Springer Science & Business Media, Netherlands, Volume 1, 5-20.

Benson, M.L. and Simpson, S.S. (2009). *White-Collar Crime: An Opportunity Perspective, Criminology and Justice Series*, Routledge, NY: New York.

Bergström, O., Hasselbladh, H. and Kärreman, D. (2009). Organizing disciplinary power in knowledge organization, *Scandinavian Journal of Management*, 25, 178-190.

Bock, G.W., Zmud, R.W. and Kim, Y.G. (2005). Behavioral intention formation in knowledge sharing: examining the roles of extrinsic motivators, social-psychological forces, and organizational climate, *MIS Quarterly*, 29 (1), 87-111.

Bonini, S., Court, D. and Marchi, A. (2009). Rebuilding corporate reputations, *McKinsey Quarterly*, 3, 75-83.

Borgers, M.J. and Moors, J.A. (2007). Targeting the Proceeds of Crime: Bottlenecks in International Cooperation, *European Journal of Crime, Criminal Law and Criminal Justice*, 1-22.

Bossler, A.M. and Holt, T.J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, *International Journal of Cyber Criminology*, 3 (1), 400-420.

Bovenkerk, F., Siegel, D. and Zaitch, D. (2003). Organized crime and ethnic reputation manipulation, *Crime, Law and Social Change*, 39, 23-38.

Brightman, H.J. (2009). *Today's White-Collar Crime: Legal, Investigative, and Theoretical Perspectives*, Routledge, Taylor & Francis Group, NY: New York.

Brown, S.D. (2007). The meaning of criminal intelligence. *International Journal of Police Science & Management*, 9 (4), 336-340.

Brown, J.S. and Duguid, P. (2001). Knowledge and Organization: A Social-Practice Perspective, *Organization Science*, 12 (2), 198-213.

Brown, R., Cannings, A. and Sherriff, J. (2004). *Intelligence-led vehicle crime reduction: an evaluation of Operation Gallant*, Home Office Online Report 47/04, http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr4704.pdf.

Brønn, P.S. and Vidaver-Cohen, D. (2009). Corporate Motives for Social Initiative: Legitimacy, Sustainability, or the Bottom Line? *Journal of Business Ethics*, 87, 91-109.

Button, M. and Brooks, G. (2009). "Mind the gap", progress towards developing anti-fraud culture strategies in UK central government bodies, *Journal of Financial Crime*, 16 (3), 119-144.

Calder, M.C. (2004). The Internet: Potential, Problems and Pathways to Hands-on Sexual Offending, in: Calder, M.C. (editor), *Child sexual abuse and the Internet: Tackling the new frontier*, Russell House Publishing, Dorset, UK, 1-23.

Callanan, C. and Jones, N. (2009). *Project on Cybercrime*, University College Dublin, Ireland.

Castello, I. and Lozano, J. (2009). From risk management to citizenship corporate social responsibility: analysis of strategic drivers of change, *Corporate Governance*, 9 (4), 373-385.

CEOP (2006). *Understanding Online Social Network Services and Risks to Youth*, Child Exploitation and Online Protection Centre, London, UK, www.ceop.gov.uk.

Chang, J.J.S. (2008). An analysis of advance fee fraud on the internet, *Journal of Financial Crime*, 15 (1), 71-81.

Cheng, H. (2008). Insider trading in China: the case for the Chinese Securities Regulatory Commission, *Journal of Financial Crime*, 15 (2), 165-178.

Cheng, H. and Ma, L. (2009). White collar crime and the criminal justice system – Government response to bank fraud and corruption in China, *Journal of Financial Crime*, 16 (2), 166-179.

Cihlar, F.P. (2009). Coming to America: the extraterritorial reach of US judicial process, *Journal of Financial Crime*, 16 (2), 115-124.

Cook, N. (2008). *Enterprise 2.0: How Social Software Will Change the Future of Work*, Gower Publishing Limited, Aldershot, UK.

Corrocher, N., Cusmano, L. and Morrison, A. (2009). Modes of innovation in knowledge-intensive business services evidence from Lombardy, *Journal of Evolutionary Economics*, 19, 173-196.

Council of Europe (2002). *Crime Analysis: Organized crime - Best practice survey no. 4*, Economic Crime Division, Department of Crime Problems, Directorate General I - Legal Affairs, Council of Europe, Strasbourg, France.

Council of Europe (2007). Council Conclusions setting the EU priorities for the fight against organized crime based on the 2007 organized crime threat assessment, *Council of the European Union*, 1048 Brussels, Belgium.

Curtis, G.E. (2008). Legal and Regulatory Environments and Ethics: Essential Components of a Fraud and Forensic Accounting Curriculum, *Issues in Accounting Education*, 23 (4), 535-543.

D'Ovidio, R., Mitman, T., El-Burki, I.J. and Shumar, W. (2009). Adult-Child Sex Advocacy Websites as Social Learning Environments: A Content Analysis, *International Journal of Cyber Criminology*, 3 (1), 421-440.

Davidson, J. (2008). *Child Sexual Abuse - Media representations and government reactions*, Routledge, Abingdon, UK.

Davidson, J., Martellozzo, E (2008) '*Protecting vulnerable young people in cyberspace from sexual abuse: raising awareness and responding globally*' Police Practice & Research An International Journal. ISSN 1561-4263.

Dion, M. (2008). Ethical leadership and crime prevention in the organizational setting, *Journal of Financial Crime*, 15 (3), 308-319.

Dion, M. (2009). Corporate crime and the dysfunction of value networks, *Journal of Financial Crime*, 16 (4), 436-445.

Dion, M. (2010). Corruption and ethical relativism: what is at stake? *Journal of Financial Crime*, 17 (2), 240-250.

DN (2008). - *Private granskere tapper politiet (Private investigators empty the police)*, Dagens Næringsliv (Norwegian daily newspaper), downloaded July 28, 2009, http://www.dn.no/forsiden/politikkSamfunn/article1288478.ece.

DN (2009). Føler meg rettsløs, tygd på og spyttet ut (Feeling without justice, chewed on and spitted out), *Dagens Næringsliv (Norwegian Financial Times newspaper*), Tuesday, August 25, No. 195, page 1.

DN (2010). Lurte aksjerobot 2200 ganger (Cheated stock robot 2200 times), *Dagens Næringsliv (Norwegian Financial Times)*, Tuesday 17 August 2010, pages 4-5.

Dombrowski, S.C., Gischlar, K.L. and Durst, T. (2007). Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet, *Child Abuse Review*, 16, 153-170.

Dowling, G.R. (2006). Communicating Corporate Reputation through Stories, *California Management Review*, 49 (1), 82-100.

Dunaigre, P. (2001). Paedophilia: a psychiatric and psychoanalytical point of view, in: Arnaldo, C.A. (editor), *Child Abuse on the Internet - Ending the Silence*, Unesco Publishing (Paris) and Beghahn Books, Oxford, UK, pp. 43-49.

Einwiller, S.A., Carroll, C.E. and Korn, K. (2010). Under What Conditions Do the News Media Influence Corporate Reputation? The Roles of Media Dependency and Need for Orientation, *Corporate Reputation Review*, 12 (4), 299-315.

Elvins, M. (2003). Europe's response to transnational organised crime. In: Edwards, A. and P. Gill (editors), *Crime: Perspectives on global security*, London: Routledge, pp.29-41.

Ferraro, M.M. and Casey, E. (2005). *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science*, Elsevier Academic Press, New York.

Fidelie, L.W. (2009). Internet Gambling: Innocent Activity or Cybercrime? *International Journal of Cyber Criminology*, 3 (1), 476-491.

Financial Intelligence Unit (2008). *Annual Report*, Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim), Oslo, Norway.

Finkelhor D (1984) *Child Sexual Abuse: New Theory and Research*, The Free Press, New York.

Fisher, J. (2008). The UK's faster payment project: avoiding a bonanza for cyber crime fraudsters, *Journal of Financial Crime*, 15 (2), 155-164.

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace, *Journal of Financial Crime*, 14 (2), 190-207.

Friedman, B.A. (2009). Human Resource Management Role Implications for Corporate Reputation, *Corporate Reputation Review*, 12 (3), 229-244.

Galbreth, M.R. and Shor, M. (2010). The Impact of Malicious Agents on the Enterprise Software Industry, *MIS Quarterly*, 34 (3), 595-612.

Gallaher, M.P., Link, A.N. and Rowe, B.R. (2008). *Cyber Security – Economic Strategies and Public Policy Alternatives*, Edward Elgar Publishing, Cheltenham, UK.

Gallant, M.M. (2009). Uncertainties collide: lawyers and money laundering, terrorist finance regulation, *Journal of Financial Crime*, 16 (3), 210-219.

Gallouj, F. and Savona, M. (2009). Innovation in services: a review of the debate and a research agenda, *Journal of Evolutionary Economics*, 19, 149-172.

Garcia-Morales, V.J., Llorens-Montes, F.J. and Verdu-Jover, A.J. (2006). Organizational learning categories: their influence on organizational performance, *International Journal of Innovation and Learning*, 3 (5), 518-536.

Garud, R. and Kumaraswamy, A. (2005). Vicious and virtuous circles in the management of knowledge: the case of Infosys Technologies, *MIS Quarterly*, 29 (1), 9-33.

Hagen, J.M., Sivertsen, T.K. and Rong, C. (2008). Protection against unauthorized access and computer crime in Norwegian enterprises, *Journal of Computer Security*, 16, 341-366.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., and Tatham, R.L. (2006). *Multivariate Data Analysis*, Sixth Edition, Prentice Hall, Upper Saddle River, New Jersey.

Hansen, L.L. (2009). Corporate financial crime: social diagnosis and treatment, *Journal of Financial Crime*, 16 (1), 28-40.

Hardouin, P. (2009). Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing, *Journal of Financial Crime*, 16 (3), 199-209.

Harfield, C. (2008). Paradigms, Pathologies, and Practicalities - Policing Organized Crime in England and Wales, *Policing*, 2 (1), 63-73.

Harreld, J.B., O'Reilly, C.A. and Tushman, M.L. (2007). Dynamic Capabilities at IBM: Driving Strategy into Action, *California Management Review*, 49 (4), 21-43.

Harvey, J. and Lau, S.F. (2009). Crime-money, reputation and reporting, *Crime Law and Social Change*, 52, 57-72.

Heath, J. (2008). Business Ethics and Moral Motivation: A Criminological Perspective, *Journal of Business Ethics*, 83, 595-614.

Hemphill, T.A. (2006). Corporate internal investigations: balancing firm social reputation with board fiduciary responsibility, *Corporate Governance*, 6 (5), 635-642.

Hemphill, T.A. and Cullari, F. (2009). Corporate Governance Practices: A Proposed Policy Incentive Regime to Facilitate Internal Investigations and Self-Reporting of Criminal Activities, *Journal of Business Ethics*, 87, 333-351.

Henning, J. (2009). Perspectives on financial crimes in Roman-Dutch law: Bribery, fraud and the general crime of falsity, *Journal of Financial Crime*, 16 (4), 295-304.

Higgins, G.E. (2007). Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value, *International Journal of Cyber Criminology*, 1 (1), 33-55.

Higgins, G.E., Wolfe, S.E. and Marcum, C.D. (2008). Music Piracy and Neutralization: A Preliminary Trajectory Analysis from Short-Term Longitudinal Data, *International Journal of Cyber Criminology*, 2 (2), 324-336.

Highhouse, S., Brooks, M.E. and Gregarus, G. (2009). An Organizational Impression Management Perspective on the Formation of Corporate Reputations, *Journal of Management*, 35 (6), 1481-1493.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, *International Journal of Cyber Criminology*, 1 (1), 1-26.

Hinduja, S. (2009). US cybercrime units on the world wide web, *Policing: An International Journal of Police Strategies & Management*, 32 (2), 278-296.

Hipp, C. (1999). Knowledge-Intensive Business Services in the New Mode of Knowledge Production, *AI & Society*, 13, 88-106.

Hodgson, T.W. (2008). From famine to feast – The prosecution of multi-jurisdictional financial crime in the electronic age, *Journal of Financial Crime*, 15 (3), 320-337.

Holt, T.J. and Graves, D.C. (2007). A Qualitative Analysis of Advance Fee Fraud E-mail, *International Journal of Cyber Criminology*, 1 (1), 137-154.

Home Office (2005a). *Guidance on statutory performance indicators for policing 205/2006*. Police Standards Unit, Home Office of the UK Government, www.policereform.gov.uk.

Home Office (2005b). *Senior Investigating Officer Development Programme*. Police Standards Unit, Home Office of the UK Government, www.policereform.gov.uk.

Innes, M., Fielding, N. and Cope, N. (2005). The appliance of science: The theory and practice of crime intelligence analysis, *British Journal of Criminology*, 45, 39-57.

Innes, M. and Sheptycki, J.W.E. (2004). From detection to disruption: Intelligence and the changing logic of police crime control in the United Kingdom, *International Criminal Justice Review*, 14, 1-24.

Interpol (2009). *Financial and high-tech crimes*, International Criminal Police Organizaton (Interpol), 69006 Lyon, France, http://www.interpol.int/Public/FinancialCrime/Default.asp, retrieval July 3, 2009.

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal, *International Journal of Cyber Criminology*, 1 (1), 1-6.

Jaschke, H.G., Bjørgo, T., Romero, F.del B., Kwanten, C., Mawby, R. and Pogan, M. (2007). *Perspectives of Police Science in Europe*, Final Report, European Police College, CEPOL, Collège Européen de Police, Hampshire, England.

Jayasuriya, D. (2006). Auditors in a changing regulatory environment, *Journal of Financial Crime*, 13 (1), 51-55.

Johnson, A.C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study, *MIS Quarterly*, 34 (3), 549-566.

Joyce, E. (2005). Expanding the International Regime on Money Laundering in Response to Transnational Organized Crime, Terrorism, and Corruption. In: Reichel, P. (editor), *Handbook of Transnational Crime and Justice*, London: Sage Publications, pp. 79-97.

Kao, D.Y. and Wang, S.J. (2009). The IP address and time in cyber-crime investigation, *Policing: An International Journal of Police Strategies & Management*, 32 (2), 194-208.

Kark, R. and Dijk, D.van (2007). Motivation to lead, motivation to follow: the role of the self-regulatory focus in leadership processes. *Academy of Management Review*, 32 (2), 500-528.

Kayrak, M. (2008). Evolving challenges for supreme audit institutions in struggling with corruption, *Journal of Financial Crime*, 15 (1), 60-70.

Keh, H.T. and Xie, Y. (2009). Corporate reputation and customer behavioral intentions: The roles of trust, identification and commitment, *Industrial Marketing Management*, 38, 732-742.

Kennedy, A. (2007). Winning the information wars – Collecting, sharing and analyzing information in asset recovery investigations, *Journal of Financial Crime*, 14 (4), 372-404.

Kiely, J.A. and G.S. Peek (2002). The Culture of the British Police: Views of Police Officers, *The Service Industries Journal*, 22 (1), 167-183.

Kierkegaard, S. (2008). Cybering, online grooming and ageplay, *Computer Law & Security Report*, 24, 41-55.

King, W. R. and Teo, T. S. H. (1997). Integration Between Business Planning and Information Systems Planning: Validating a Stage Hypothesis. *Decision Science, 28*(2), 279-308.

Koker, L.de (2009). Identifying and managing low money laundering risk - Perspectives on FATF's risk-based guidance, *Journal of Financial Crime*, 16 (4), 334-352.

Kranacher, M.J., Morris, B.W., Pearson, T.A. and Riley, A. (2008). A Model Curriculum for Education in Fraud and Forensic Accounting, *Issues in Accounting Education*, 23 (4), 505-519.

Ksenia, G. (2008). Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective? *Journal of Financial Crime*, 15 (2), 223-233.

Lahneman, W.J. (2004). Knowledge-Sharing in the Intelligence Community After 9/11, *International Journal of Intelligence and Counterintelligence*, 17, 614-633.

Larsson, P. (2006). Developments in the regulation of economic crime in Norway, *Journal of Financial Crime*, 13 (1), 65-76.

Lassen, C.; Laugen, B.T., and Næss, P. (2006). Virtual mobility and organizational reality - a not on the mobility needs in knowledge organizations, *Transportation Research*, Part D, 11, 459-463.

Laudon, K.C. and Laudon, J.P. (2010). *Management Information Systems: Managing the Digital Firm*, Eleventh Edition, Pearson Education, London, UK.

Leonard-Barton, D. (1992). Core capabilities and core rigidities: A paradox in managing product development, *Strategic Management Journal*, 13, 111-125.

Levi, M. (2007). Policing Financial Crimes, in: Pontell, H.N. and Geis, G. (editors), *International Handbook of White-Collar and Corporate Crime*, New York: Springer Science, 588-606.

Levitt, S.D. and Miles, T.J. (2007). *Empirical Study of Criminal Punishment*, in: Polinsky, A.M. and Shavell, S., editors, Handbook of law and economics, Elsevier Publishing, Amsterdam, Netherlands.

Liebowitz, J. (2004). Will knowledge management work in the government? *Electronic Government: An International Journal*, 1 (1), 1-7.

Lillywhite, R. and Skidmore, P. (2006). Boys Are Not Sexually Exploited? A Challenge to Practitioners, *Child Abuse Review*, 15, 351-361.

Linthicum, C., Reitenga, A.L. and Sanchez, J.M. (2010). Social responsibility and corporate reputation: The case of the Arthur Andersen Enron audit failure, *Journal of Accounting and Public Policy*, 29, 160-176.

Liu, C.C. and Chen, S.Y. (2005). Determinants of knowledge sharing of e-learners, *International Journal of Innovation and Learning*, 2 (4), 434-445.

Love, E.G. and Kraatz, M. (2009). Character, conformity, or the bottom line? How and why downsizing affected corporate reputation, *Academy of Management Journal*, 52 (2), 314-335.

Lyman, M.D. and Potter, G.W. (2007). *Organized crime*, 4th edition, Pearson Prentice Hall, Uppler Saddle River, New Jersey.

Madhavaram, S. and Hunt, S.D. (2008). The service-dominant logic and a hierarchy of operant resources: developing masterful operant resources and implications for marketing strategy, *Journal of the Academy of Marketing Science*, 36, 67-82.

Maghan, J. (1994). Intelligence Gathering Approaches in Prisons, *Low Intensity Conflict & Law Enforcement*, 3 (3), 548-557.

Markovski, S. and Hall, P. (2007). Public sector entrepreneurship and the production of defence, *Public Finance and Management*, 7 (3), 260-294.

Michel, P. (2008). Financial crimes: the constant challenge of seeking effective prevention solutions, *Journal of Financial Crime*, 15 (4), 383-397.

Mintzberg, H. (1994). Rounding on the managers' job, *Sloan Management Review*, 36 (1), 11-26.

Miri-Lavassani, K., Kumar, V., Movahedi, B. and Kumar, U. (2009). Developing an identity measurement model: a factor analysis approach, *Journal of Financial Crime*, 16 (4), 364-386.

Mitchell, K.J., Wolak, J., and Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment? *Child Abuse & Neglect*, 32, 277-294.

Moore, R. and McMullan, E.C. (2009). Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students, *International Journal of Cyber Criminology*, 3 (1), 441- 451.

Naylor, R.T. (2003). Towards a general theory of profit-driven crimes, *British Journal of Criminology*, 43, 81-101.

Nhan, J., Kinkade, P. and Burns, R. (2009). Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Solicitation, *International Journal of Cyber Criminology*, 3 (1), 452-475.

Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. *Long Range Planning*, 33 (1), pp 5-34.

Nykodym, N., Taylor, R. and Vilela, J. (2005). Criminal profiling and insider cyber crime, *Computer Law & Security Report*, 21, 408-414.

Perry-Smith, J.E. and Shalley, C.E. (2003). The social side of creativity: a static and dynamic social network perspective, *Academy of Management Review*, Vol. 29, No. 1, pp. 89-106.

Picard, M. (2009). Financial services in trouble: the electronic dimension, *Journal of Financial Crime*, 16 (2), 180-192.

Pickett, K.H.S. and Picket, J.M. (2002). *Financial Crime Investigation and Control*. New York: John Wiley & Sons.

Pontell, H.N., Geis, G. and Brown, G.C. (2007). Offshore Internet Gambling and the World Trade Organization: Is it Criminal Behavior or a Commodity? *International Journal of Cyber Criminology*, 1 (1), 119-136.

Poston, R.S. and Speier, C. (2005). Effective Use of Knowledge Management Systems: A Process Model of Content Ratings and Credibility Indicators. *MIS Quarterly*, 29 (2), 221-244.

Prahalad, C.K. and Hamel, G. (1990). The core competence of the corporation, *Harvard Business Review*, 76 (3), 79-91.

Quayle, E., Vaughan, M. and Taylor, M. (2006). Sex offenders, Internet child abuse images and emotional avoidance: The importance of values, *Aggression and Violent Behavior*, 11, 1-11.

Quinn, J.B. (1999). Strategic outsourcing: Leveraging knowledge capabilities, *Sloan Management Review*, Summer, 9-21.

Quirke, B.J. (2007). A critical appraisal of the role of UCLAF, *Journal of Financial Crime,* 14 (4), 460-473.

Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula, *Issues in Accounting Education*, 23 (4), 521-533.

Ratcliffe, J.H. (2008). *Intelligence-Led Policing*, Willan Publishing, Devon, UK.

Riffe, D. and Freitag, A. (1997). A content analysis of content analyses, twenty-five years of journalism quarterly, *Journalism Mass Communication Quarterly*, 74, 873-882.

Salifu, A. (2008). The impact of internet crime on development, *Journal of Financial Crime*, 15 (4), 432-443.

Rodell, J.B. and Colquitt, J.A. (2009). Looking Ahead in Times of Uncertainty: The Role of Anticipatory Justice in an Organizational Change Context, *Journal of Applied Psychology*, 94 (4), 989-1002.

Sathye, M. (2008). Estimating the cost of compliance of AMLCTF for financial institutions in Australia, *Journal of Financial Crime*, 15 (4), 347-363.

Schneider, S. (2006). Privatizing Economic Crime Enforcement: Exploring the Role of Private Sector Investigative Agencies in Combating Money Laundering, *Policing & Society*, 16 (3), 285-312.

Scott, B.A., Colquitt, J.A. and Paddock, E.L. (2009) An Actor-Focused Model of Justice Rule Adherence and Violation: The Role of Managerial Motives and Discretion, *Journal of Applied Psychology*, 94 (3), 756-769.

Segell, G.M. (2007). Reform and transformation: The UK's serious organized crime agency, *International Journal of Intelligence and CounterIntelligence*, 20, 217-239.

Sexual Offences Act 2003 England and Wales

Sheehan, N.T. and Stabell, C.B. (2007). Discovering new business models for knowledge intensive organizations, *Strategy & Leadership*, 35 (2), 22-29.

Sheptycki, J. (2007). Police Ethnography in the House of Serious and Organized Crime, in: Henry, A. and Smith, D.J. (editors), *Transformations of Policing*, Ashgate Publishing, Oxford, UK, 51-77.

Siponen, M. and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, *MIS Quarterly*, 34 (3), 487-502.

Smith, H.L. (2003). Knowledge Organization and Local Economic Development: The Cases of Oxford and Grenoble, *Regional Studies*, 37 (9), 899-909.

Smith, N. and Flanagan, C. (2000). *The Effective Detective: Identifying the skills of an effective SIO*. Police Research Series Paper 122, Policing and Reducing Crime Unit, London, UK.

Snyder, H. and Crescenzi, A. (2009). Intellectual capital and economic espionage: new crimes and new protections, *Journal of Financial Crime*, 16 (3), 245-254.

Solaiman, S.M. (2009). Investor protection by securities regulators in the primary share markets in Australia and Bangladesh, *Journal of Financial Crime*, 16 (4), 305-333.

Spalek, B. (2004). Policing financial crime: the Financial Services Authority and the myth of the 'duped investor', in: Burke, Roger Hopkins (editor): *Hard Cop, Soft Cop - Dilemmas and debates in contemporary policing*, Devon, UK: Willan Publishing.

Stedje, S. (2004). *The Man in the Street, or the Man in the Suite: An Evaluation of the Effectiveness in the Detection of Money Laundering in Norway*, MA Social Sciences and Law Criminal Intelligence Analysis/CIA, The University of Manchester, UK.

Stelfox, P. and Pease, K. (2005). Cognition and detection: reluctant bedfellows? In: Smith, M. and Tilley, N. (editors), *Crime Science: New Approaches to Preventing and Detecting Crime*, UK: Willan Publishing.

SYPIS (2007). *South Yorkshire Police Intelligence Strategy 2007 - Breaking the chain*, South Yorkshire Police, UK, www.policereform.gov.uk.

Taylor, A. and Greve, H.R. (2006). Superman or the fantastic four? Knowledge combination and experience in innovative teams. *Academy of Management Journal*, 49 (4), 723-740.

Thomas, A. and Mancino, A. (2007). The relationship between entrepreneurial characteristics, firms' positioning and local development, *Entrepreneurship and Innovation*, 8 (2), 105-114.

Toner, G.A. (2009). New ways of thinking about old crimes: Prosecuting corruption and organized criminal groups engaged in labor-management racketeering, *Journal of Financial Crime*, 16 (1), 41-59.

Tong, S. (2007). *Training the Effective Detective: Report of Recommendations*, University of Cambridge. Author contact details: Dr Stephen Tong, Senior Lecturer in Policing, Canterbury Christ Church University, Kent, UK.

Tufekci, Z. (2008). Grooming, Gossip, FaceBook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society*, 11 (4), 544-564.

Turner, K.L. and Makhija, M.V. (2006). The role of organizational controls in managing knowledge, *Academy of Management Review*, 31 (1), 197-217.

United Nations (2008). *United Nations e-Government Survey 2008*, Department of Economics and Social Affairs, Division for Public Administration and Development Management, United Nations, New York.

Uretsky, M. (2001). Preparing for the Real Knowledge Organization. *Journal of Organizational Excellence*, 21 (1), 87-93.

Walker, K. (2010). A Systematic Review of the Corporate Reputation Literature: Definition, Measurement, and Theory, *Corporate Reputation Review*, 12 (4), 357-387.

Wasko, M.M. and Faraj, S. (2005). Why Should I Share? Examining Social Capital and Knowledge Contribution in Electronic Networks of Practice. *MIS Quarterly*, 29 (1), 35-57.

Whittaker, J. (2004). *The Cyberspace Handbook*, Routledge, Taylor & Francis Group, London, UK.

Wilhelmsen, S. (2009). *Maximising Organizational Information Sharing and Effective Intelligence Analysis in Critical Data Sets*, Dissertation for the degree of philosophiae doctor (PhD), University of Bergen, Norway.

Williams, J.W. (2005). Governability Matters: The Private Policing of Economic Crime and the Challenge of Democratic Governance, *Policing & Society*, 15 (2), 187-211.

Williams, C.C. (2006). *The Hidden Enterprise Culture - Entrepreneurship in the Underground Economy*, Edward Elgar Publishing, Cheltenham, UK.

Williams, S. and Williams, N. (2003). The Business Value of Business Intelligence, *Business Intelligence Journal*, Fall, 30-39.

Witten, R.M. and Koffer, T.J. (2009). Navigating the increased anti-corruption environment in the USA and elsewhere, *Journal of Securities Law, Regulation & Compliance*, 2 (2), 125-143.

Wolak, J., Finkelhor, D. and Mitchell, K. (2009). *Trends in Arrests of "Online Sex offenders"*, Crimes Against Children Research Center, Durham, NH, www.unh.edu/ccrc

Yusuf, T.O. and Babalola, A.R. (2009). Control of insurance fraud in Nigeria: an exploratory study, *Journal of Financial Crime*, 16 (4), 418-435.

Zahra, S.A., Kuratko, D.F. and Jennings, D.F. (1999). Entrepreneurship and the Acquisition of Dynamic Organizational Capabilities, *Entrepreneurship Theory and Practice*, Spring, 5-10.

Zander, I. (2007). Do you see what I mean? An entrepreneurship perspective on the nature and boundaries of the firm, *Journal of Management Studies*, 44 (7), 1141-1164.

Zapata-Phelan, C.P., Colquitt, J.A., Scott, B.A. and Livingston, B. (2009). Procedural justice, interactional justice, and task performance: The mediating role of intrinsic motivation, *Organizational Behaviour and Human Decision Processes*, 108, 93-105.

Zheng, W., Yang, B. and McLean, G.N. (2010). Linking organizational culture, structure, strategy, and organizational effectiveness: Mediating role of knowledge management, *Journal of Business Research*, 63, 763-771.

Økokrim (2008). *Annual Report 2007*, Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime, Oslo, Norway.