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:

1. *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.
2. *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.
3. *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.
4. *Entitlement technique* is used by individuals who feel that they are entitled to engage in an activity because of some consideration in their life.
5. *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.