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.