Policing White-Collar Crime

Petter Gottschalk , BI Norwegian Business School

Introduction

White-collar crime is financial crime committed by white-collar criminals. Sensational white-collar crime cases regularly appear in the international business press and studies in journals dealing with ethics and crime. With a larger sample, we can study white-collar crime convictions using statistical techniques.

White-collar crime is financial crime committed by upper-class members of society for personal or organizational gain. White-collar criminals are individuals who tend to be wealthy, highly educated and socially connected, and they are typically employed by, and within, legitimate organizations. Ever since Edwin Sutherland first introduced the concept of "white-collar" crime in 1939, researchers have discussed what might be encompassed by this concept and what might be excluded. The discussion has been summarized by scholars such as Benson and Simpson (2009), Blickle et al. (2006), Bookman (2008), Bucy et al. (2008), Hansen (2009), Podgor (2007), Robson (2010) and Schnatterly (2003).

The purpose of this article is to introduce four policing strategies for policing white-collar crime, after first presenting an empirical study on convicted white-collar criminals. The empirical part of this paper focuses on those who committed white-collar crimes in Norway between 2009 and 2012.

Second, the paper introduces four strategies for policing white-collar crime, i.e. a value shop configuration, a knowledge management strategy, an information management strategy and an information technology strategy. A value configuration strategy is concerned with the choice between a value chain, value shop and value network. A knowledge management strategy is concerned with personnel and their knowledge areas. An information management strategy is concerned with issues such as sources of information and the quality of information in police work. Finally, an information technology strategy is concerned with information and communication technology used to store and retrieve electronic information. These strategies may be partly mutually exclusive, but they may also in part compliment and support one another.

This paper thus discusses both white-collar criminals and the strategies that are needed for policing this type of crime.

Portrait of white-collar criminals

Several options exist to identify a substantial sample of white-collar criminals and to collect relevant information about each criminal. However, in a small country like Norway, with a population of only five million people, there are limits to the available sample size.

Policing White-Collar Crime

Petter Gottschalk
BI Norwegian Business School

This is the author's final, accepted and refereed manuscript to the article published in

Reviews of the Police College of Finland, 3 / 2013

One available option would be to study court cases involving white-collar crime and criminals. A challenge here would be to identify the relevant laws and sentences that cover our definition not only of white-collar crime, but also the required characteristics of white-collar criminals.

Another available option is to study newspaper articles where the journalists have already employed some kind of selection process for higher class, white-collar individuals convicted in court of financial crime. An advantage of this approach is that the cases are publicly known, which makes it easier to identify cases by their individual white-collar names. The selective and otherwise filtered information in newspapers might be a problem in other kinds of studies, but it is considered acceptable for the purposes of this study. Therefore, the latter option was chosen in this research project.

Based on this decision, our sample consists of the same persons, groups and characteristics as those focused on by the newspapers when presenting the news: famous individuals, famous companies, surprising stories, important events, substantial consequences and matters of principle and significant public interest. The sample consists of high-profile and large yield offenses. This is in line with research by Schnatterly (2003), who searched through the Wall Street Journal for several years in her study of white-collar crime, which was published in the Strategic Management Journal.

The two main financial newspapers in Norway are “Dagens Næringsliv” and “Finansavisen”, both of which are conservative-leaning business newspapers. In addition, the business-friendly national daily newspaper, “Aftenposten”, regularly reports news of white-collar criminals. Left-wing newspapers such as “Klassekampen” very seldom cover specific white-collar criminal cases, although they generally report on white-collar crime. It is important to understand the agenda-setting and framing functions of the press and media, perhaps the two most important schemes in journalism, media and communication studies; both functions are clearly relevant as the theme and focus of this article.

It is important to keep in mind that our data deal with newspaper accounts of white-collar crime, not with the distribution of white-collar crime in society, because that is not what is being measured. Using a newspaper sample is different from focusing on the overall number of white-collar crime cases. We argue that a newspaper account is one of the characteristics of white-collar crime, as defined previously. Therefore, news reports are relevant reflections of knowledge about white-collar crime.

As suggested by Barak (2007), news-making criminology refers to the conscious efforts and activities of criminologists to interpret, influence or shape the representation of newsworthy items about crime and justice. News-making criminology as a perspective on the theory, practice and representations of crime and justice is an important approach for understanding white-collar crime. However, Barak’s work focused on how the media constructs images of crime. In this study, the media is used as a source of potentially objective information, where factual information in terms of quantitative numbers is collected from newspaper accounts.

White-collar criminals in Norway

Most white-collar criminals are men. This is confirmed in the sample of 255 persons, which included only 20 female criminals and 235 male criminals. Thus, less than 8 per cent of the white-collar crime discussed in newspaper articles was committed by women — sometimes they are labelled pink-collar criminals.

The youngest white-collar criminal in Norway was 21 years old and the oldest was 77 years old. A distinction is made between the person's age when convicted and the person's age when committing crime. On average, a person was convicted five years after the crime had been committed, thus the average age when committing a crime is 43 years old, since the average age when convicted was 48 years old.
Most anecdotal cases, such as those of Rajaratman and Schilling, were men in their 50s or older. This is confirmed in our sample, where the average age is 48 years old when convicted in court. These average numbers are similar to those presented in a study by Blickle et al. (2006) on 76 convicted German white-collar criminals. Their sample consisted of six female criminals and 70 male criminals. The mean age of the offenders in Germany was 47 years. In a study reported by Benson and Simpson (2009), the average age of common criminals was 30 years, while the average age for white-collar criminals was 40 years. It is unclear whether the age of 40 years can be compared to the age of 48 years when convicted or to the age of 43 years when committing the crime in Norway.

The average jail sentence for 255 convicted white-collar criminals in Norwegian courts was 2.2 years, with a maximum of 10 years and a minimum of 15 days. The longest jail sentence of 10 years was given to a person involved in bank fraud, where millions were transferred from a rich widow's account in Norway to a friend's account in Dubai. Since the convicted criminal was operating in a group of criminals, he was convicted of organized crime, which in Norwegian law results in the jail sentence for a criminal act being extended from a more normal level, say six years, to ten years in his case.

A distinction can be made between the leader and follower in crime. Followers tend to be naive and unaware of what is really happening, or they are simply taken in by the personal charisma of the leader and are intensely loyal to that person (Bucy et al., 2008). In our sample of 255 criminals, we found 140 leaders and 115 followers.

Another distinction is often made between corporate crime and occupational crime. While corporate crime is mainly for the benefit of the organization, occupational crime is mainly for the benefit of the individual (Hansen, 2009). In our 255 cases, we found 88 corporate criminals and 167 occupational criminals. These are compared in the following table.

Table 1. Comparison of characteristics of occupational crime versus corporate crime

Total: 255 criminals	**88 corporate criminals**	**167 occupational criminals**	**T-statistic difference**	**Significance of t-statistics**
Age convicted	49 years	47 years	1.615	.108
Age at time of crime	44 years	42 years	1.337	.183

Years in prison	2.1 years	2.2 years	-.270	.787
Amount of crime	117 millions	26 millions	3.891	.000
Involved individuals	3.1 persons	4.7 persons	-3.366	.001
Personal income	388 000 kroner	295 000 kroner	1.267	.206
Personal tax	165 000 kroner	120 000 kroner	1.543	.124
Personal wealth	1 258 000 kroner	1 499 000 kroner	-.291	.771
Business revenue	217 millions	191 millions	.518	.605
Business employees	145 persons	113 persons	.829	.408

The number of persons involved in financial crime is significantly different among the two groups. While 4.7 persons on average were involved in occupational crime, the average for corporate crime was 3.1 persons. This result may seem counterintuitive, as crime on behalf of the corporation would seem to require more involvement by others than is necessary for occupational crime. However, we have to remind ourselves that only convicted criminals are included in this sample.

The next item in the table is the personal income of offender. Although there is no statistically significant difference in monetary terms, the corporate criminal made more money than the occupational criminal. While making more money, the corporate criminal also pays a little more money in tax to the government. However, corporate criminals are less wealthy than occupational criminals.

Value shop configuration

The empirical observations presented so far serve as background to illustrate the need for a number of policing strategies. First, policing white-collar crime requires an iterative rather than sequential investigation approach in terms of the value shop configuration. Second, knowledge about financial crime areas and motives is needed in order to police successfully. Third, the information strategy is concerned with sources of information on financial crime. Finally, the information technology strategy is needed to handle electronic information acquired when using the information strategy and to support knowledge work based on the knowledge management strategy.

We start with the value shop configuration. The investigation and prevention of white-collar crime has the configuration of a value shop. As can be seen in Figure 2, the five activities of a value shop are interlocking and, although they follow a logical sequence (much like the management of any project), the difference from a knowledge management perspective arises in terms of the manner 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 pertains to a policing unit and the manner in which it carries out its core business of conducting reactive and proactive investigations.

The sequence of activities commences with understanding the problem, moves into alternative investigation approaches, investigation decisions and investigation implementations and ends up with a criminal investigation evaluation. 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 due to 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 when it comes to managing the knowledge collected during, and applied to, a specific investigation in a value shop manner.

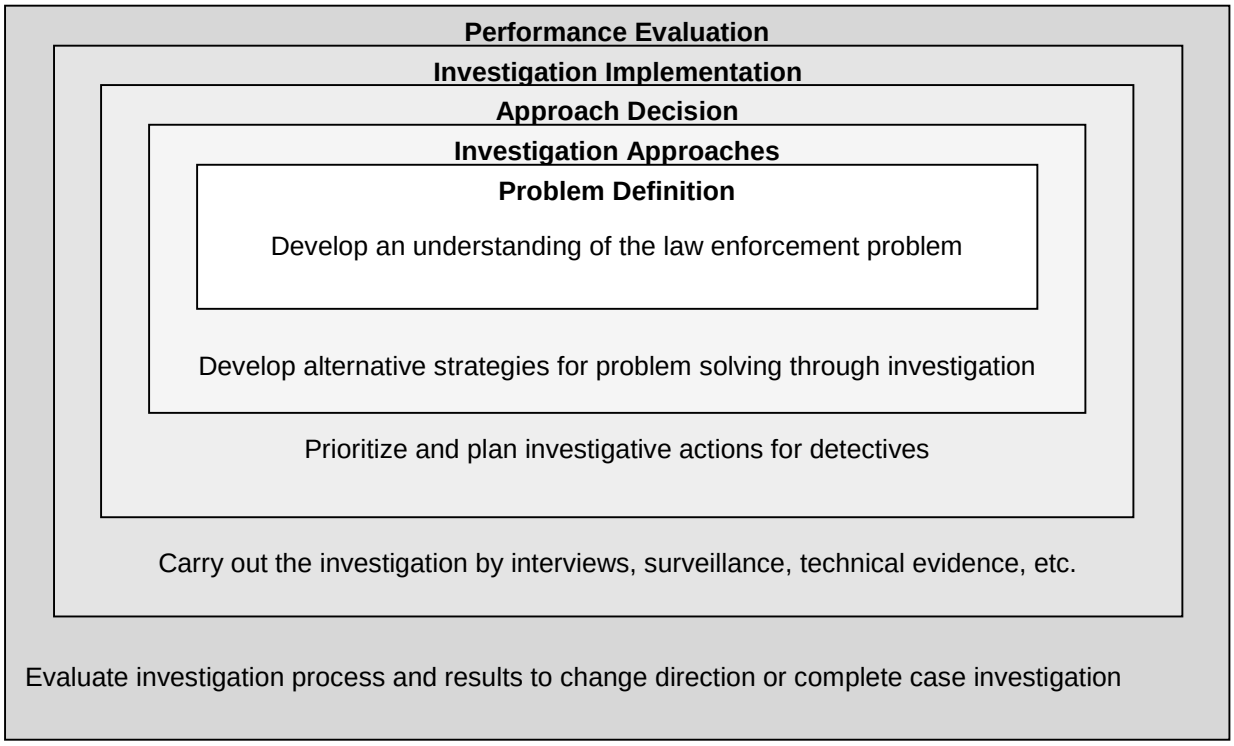

Figure 1. The knowledge organisation of investigation and prevention unit as value shop activities.

The five primary activities of the value shop depicted above in relation to a financial crime investigation and prevention unit can be outlined as follows:

1. *Problem Definition*. This involves working with parties to determine the exact nature of the crime, and hence, how it is to be defined. For example, depending on how responding officers perceive of and/or choose to define it, a physical assault in a domestic violence situation can be either upgraded to the status of grievous bodily harm to the spousal victim or it may be downgraded to a less serious, common, garden-variety assault and defined as a case where a bit of rough handling took place towards the spouse. This understanding of the concept of crime, an understanding that has to do with whether or not detectives choose to make incidents into a crime, is highly relevant here and accounts for why this first activity has been changed from a problem-finding term originally used in the business management realm into 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 in Figure 1) in terms of undertaking the key task, usually headed 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 because it establishes 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 the 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 during the second activity. Despite being 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, it involves trying to ensure as much as is possible that what is decided upon is the best option to follow in order to achieve an effective investigative result. A successful solution choice is dependent upon two requirements. First, the alternative investigation steps need to be identified in the problem-solving approaches activity. It is important to think in terms of alternatives, otherwise no choices can be made. Second, the criteria for decision-making must be known and applied to the specific investigation.

4. *Investigation Implementation.* As the name implies, executing a solution entails communicating, organizing, investigating and implementing decisions. This is an equally important process or phase in an investigation because it involves sorting through the mass of information coming into the incident room concerning 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 expended on an investigation are used here in this fourth activity of the value shop.

5. *Performance Evaluation.* Control and evaluation involves monitoring activities and measuring 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 a determination about the quality and quantity of the evidence is made in terms of whether or not to charge and prosecute an identified offender in a court of law.

Knowledge management strategy

A knowledge management strategy focuses on personnel resources, where the knowledge of each police officer as well as the combined knowledge in the police department represents resources that are to be explored and exploited for better police work. The knowledge management strategy process includes developing a working definition of knowledge, developing a working definition of knowledge management, performing a

knowledge audit, defining knowledge management objectives and strategy approaches, and implementing a strategy with quality measures (Chaffey and White, 2011).

While data are numbers and letters without meaning, information is data in a context that makes sense. When combined with interpretation and reflection information, it becomes knowledge; knowledge accumulated over time, such as learning, constitutes wisdom. In this hierarchical structure, we find that intelligence amounts to more than information and less than knowledge. Intelligence is analyzed information, as illustrated in the following figure.

The word intelligence can refer to a product, a process, the individual organization that shapes raw data into a finished intelligence product, and also the larger community in which these organizations operate. The word intelligence also often refers to the military or to agencies like MI5 (the Security Service) or MI6 (Secret Intelligence Service) in the UK. However, in this paper intelligence relates to criminal actions and is defined as a goal-oriented means of gathering, systematizing and analyzing information (Wilhelmsen, 2009).

Data is considered the raw material that constitutes information. As is the case with notes, information is data endowed with relevance and purpose. The same can be said of intelligence in that it is a form of insight to which some relevance has been attached through an attempt to offer an organized analysis of the information received by a crime analyst/ intelligence officer. Accordingly, intelligence is placed on the above continuum between information and knowledge, since, ideally (as argued), intelligence represents a form of validated information.

Investigation is a core part of police work and law enforcement — it is a truism in policing that information is the lifeblood of an investigation. An investigation goes nowhere if information is not forthcoming concerning an incident. Information is the raw data that breathes life into an investigation. It comprises ordinary rank and file employees working in human resource departments and accounting departments or sitting at a computer conducting searches and background checks or doing more sophisticated crime mapping and intelligence analysis reports and collecting and collating information.

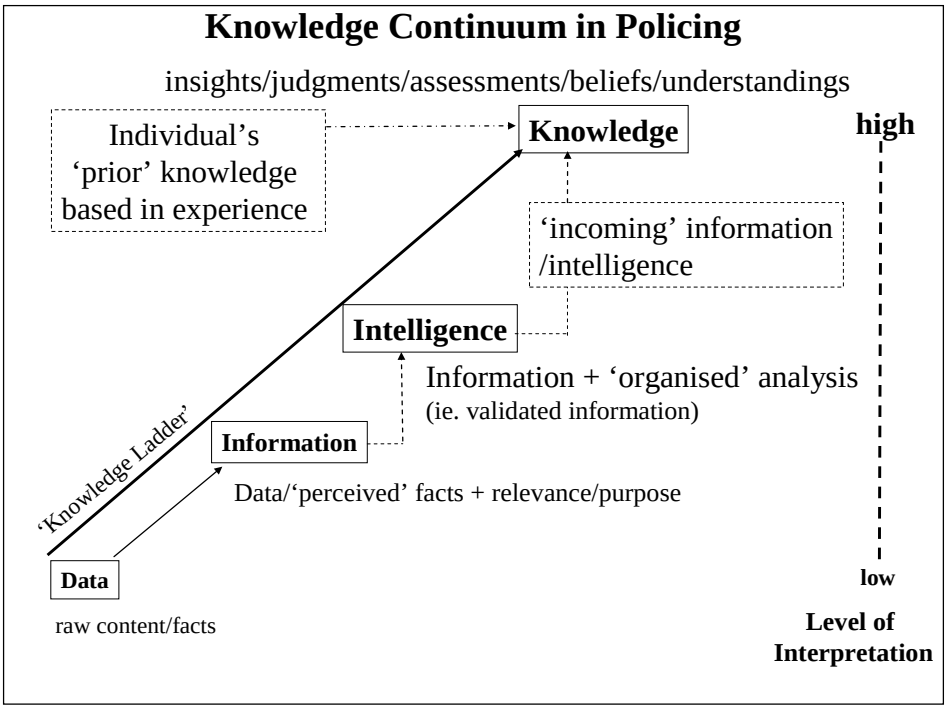

Figure 2. Hierarchy of investigation and prevention insight expressed as a continuum.

Information and, to a similar extent, intelligence thereby consist 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 data into meaningful information necessarily involves some level of interpretation of the facts as presented. However, the role of interpreting the information in this instance 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 it is in terms of information, but not as extensive as it is in the making of knowledge.

Here, we distinguish 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 managed from the perspective of law enforcement. 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, both internal and external (Jaschke et al., 2007). It also includes external factors that influence the role and behaviour 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 non-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 area of focus. The collected information is transformed and processed according to a transparent methodology to discover any criminal capacities, dispositions and goals. Transforming and processing the information generates 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 overlooking information that emerges.

7. *Legal knowledge* is knowledge of the law, regulations and legal procedures. It is based on having 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 consists of the 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.

Knowledge levels are defined here as 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 regarding a phenomenon. While know-what involves a simple perception concerning what is going on, know-why entails more complicated insights about 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, whereby an executive perceives that something is going on that might need his or her attention. The executive's insight is limited to the perception that something is happening. The executive neither understands how nor why it is happening.

2. *Know-how* is knowledge about how financial crime develops, how a criminal behaves or how criminal activity is organized. The insight of the executive or investigator is

not limited to just a perception that something is happening; he or she also understands how it is happening or the nature of the situation.

3. *Know-why* is knowledge representing the deepest form of understanding and insight into a phenomenon. The executive or investigator not only knows what is occurring and how it is occurring, he or she also has developed an understanding of why it is occurring or why it is as it is. Developing hypotheses about cause-and-effect relationships and empirically validating causality are important characteristics of know-why knowledge.

Information management strategy

An information management strategy is one of several strategies that law enforcement organizations develop and implement to improve white-collar crime detection and prevention. Police intelligence is an important element of the strategy. An information management strategy defines management approaches to the organization, control and application of police information resources through the coordination of people and technology resources in order to support policing strategies and processes. While the knowledge management strategy focuses on personnel resources, and the information systems strategy focuses on technology resources, the information management strategy focuses on identifying, retrieving, storing and applying information resources. Important issues in this strategy are information relevance and timeliness (Chaffey & White, 2011).

For an information management strategy, it is important to be aware of the variety of information sources available. In this paper, we have chosen to classify information sources into the following categories:

1. *Interview*. By means of the *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 an investigating colleague would be unable to formally approach.

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

4. *Documents*. Studying documents obtained via *confiscation* may provide information on ownership, transactions, accounts, etc. One such example is forensic accounting, which is the application of accounting tasks for an evidentiary purpose. Forensic accounting is the act of identifying, recording, settling, extracting, sorting, reporting and verifying past financial data or other

accounting activities for settling current or prospective legal disputes, or else using such past financial data to project future financial data in order to settle legal disputes (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 an important part of financial crime intelligence. One example is digital forensics, where successful cybercrime intelligence requires computer skills and modern systems of policing. Digital forensics is the art and science of applying computer science to aid the legal process. It amounts to more than a technological, systematic inspection of electronic systems and their contents for evidence or supporting evidence of a criminal act; digital forensics requires specialized expertise and tools when applied to intelligence in important areas, such as the online victimization of children.

6. *Action*. For example, this might include *provocation* and actions conducted by the investigating unit to provoke reactions that yield intelligence information. In the case of the online victimization of children, online grooming offenders in a paedophile ring are identified and their reaction after being provoked leads intelligence officers to new nodes (persons, computers) and new actual and potential victims. While the individual paedophile is mainly concerned with combining an indecent image impression and personal fantasy to achieve personal satisfaction, online organizers of the sexual abuse of children do so for profit.

7. *Surveillance*. Surveillance (visual and auditory) of places by means of *video cameras* and microphones are a part of this information source. Many business organizations have surveillance cameras on their premises to control entrants and also other critical areas. It is possible for the police to listen in on discussions in a room without the participants knowing. For example, police in a district identified the room used by local Hells Angels members for crime planning and installed listening devices in the room. Harfield (2008, p. 64) argues that when surveillance is employed to produce evidence, the product is often considered incontrovertible (hence, defence 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*. Wiretapping in terms of *interception* belongs to this information source. Police listen in on what is discussed on a telephone or transmitted via a data line without the participants being aware of it. In the UK, intercepting communications (telephone calls, emails, letters, etc.) while generating intelligence to identify more conventional evidential opportunities for committing crimes is excluded from trial evidence by law — to the evident incredulity of foreign law enforcement colleagues (Harfield, 2008).

9. *Physical material*. This involves investigating material in order to identify, for example, *fingerprints* on doors or bags, or to investigate blood splatters and identify the blood type. Another example is legal visitation: this is an approach used to identify illegal material. DNA is emerging as an important information source, and it is derived from physical material such as a person's hair or saliva. One approach to physical material collection is police search.

10. *Internet*. As an *open source*, the Internet is just as important for general information and specific happenings involving corporate crime intelligence as it is for everyone else. It is important to note that the use of open sources is by no means a new activity. Nor is it a new phenomenon found only on the Internet. The Internet is in and of itself not a source; rather, it is a tool used for finding sources. Also, there are risks involved in using open sources, such as self-corroboration.

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

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

13. *Accusations*. In the case of victimized persons and goods, a *claim* is filed with the corporate investigation unit or the unit for corporate social responsibility.

14. *Exchange*. International *policing cooperation* includes the 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*. Intelligence officers are exposed to the *news* by reading newspapers and watching TV.

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

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

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

Information technology strategy

Knowledge management systems are information systems coupled with knowledge-sharing practices that support knowledge management efforts within an organization (Durcikova et al., 2011).

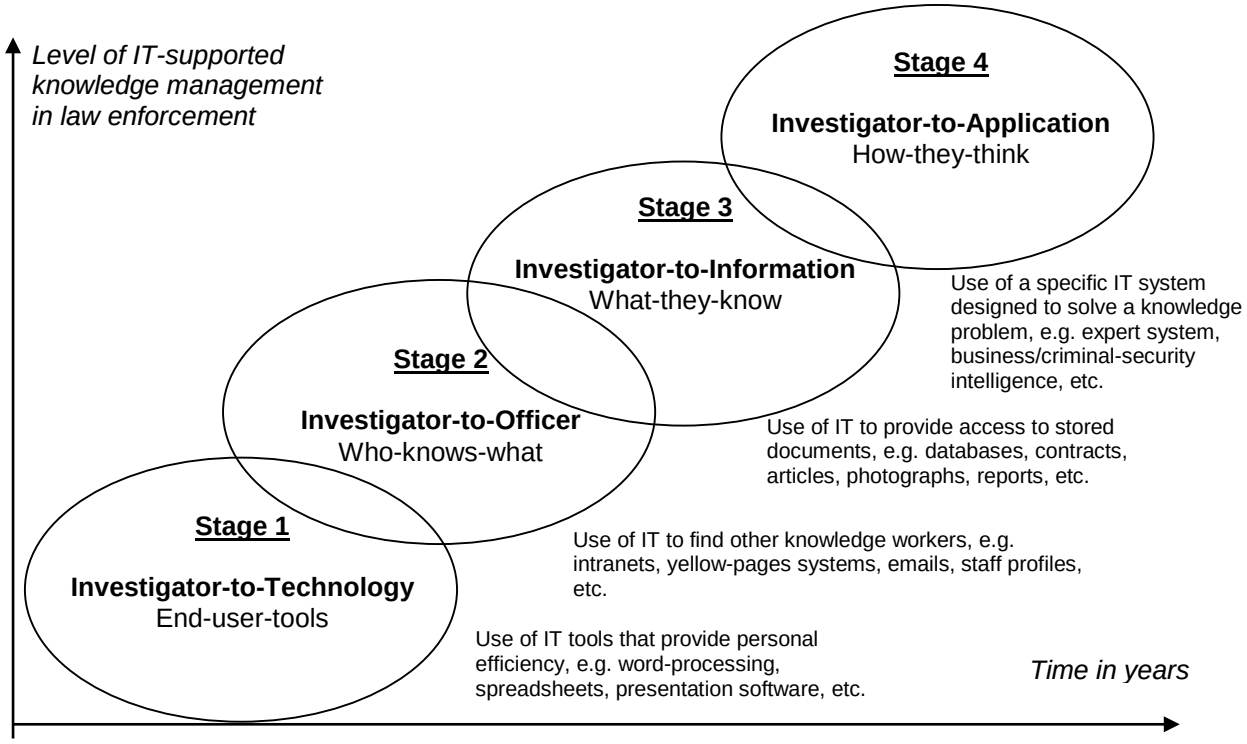

Figure 3. The knowledge management system's stage model for policing.

The stages of knowledge management technology are such that ICT is more useful to knowledge work in its later stages than it is at earlier stages. The relative concept implies that ICT is more directly involved in knowledge work at higher stages and that ICT is able to support more advanced knowledge work at higher stages:

1. *Investigator-to-Technology Stage: Tools for end users* are made available to knowledge workers. At the simplest stage, this means having a capable networked PC on every desk or laptop in every briefcase, with standardized personal productivity tools (word processing, presentation software), so that documents can be exchanged easily throughout a company. More complex and functional desktop infrastructures can also be the basis for the same types of knowledge support. Stage 1 is characterized by widespread dissemination and use of end-user tools among knowledge workers in the company. For example, at this stage, lawyers in a law firm

will use word processing, spreadsheets, legal databases, presentation software and scheduling programs.

2. *Investigator-to-Investigator Stage: Information about who knows what* is made available to all people in the firm and to select outside partners. Search engines should normally facilitate work with a thesaurus, since the terminology in which expertise is sought may not always match the terms (and hence, the search words) that the expert uses to classify such expertise.

3. *Investigator-to-Information Stage: Information from knowledge workers* is stored and made available to everyone in the firm and to designated external partners. Data mining techniques can be applied here to find relevant information and combine information in data warehouses.
4. *Investigator-to-Application Stage: Information systems solving knowledge problems* are made available to knowledge workers and solution seekers. Artificial intelligence is applied in these systems. For example, neural networks are statistically oriented tools that excel at the application of data to classify cases into categories. Another example is expert systems, which can enable the knowledge of one or a few experts to be used by a much broader group of workers. Investigator-to-application systems will only be successful if they are built on a thorough understanding of law enforcement.

Conclusion

Rather than provide anecdotal evidence about famous white-collar cases, this article has applied a systematic approach to study a large sample of convicted criminals. The sample has made it possible to analyze both corporate and occupational criminals.

Policing white-collar crime requires appropriate strategies that can be put into action. This article presented four important strategies: an information management strategy, a knowledge management strategy, an information systems strategy and a value configuration strategy. The strategies are illustrated in Figure 4.

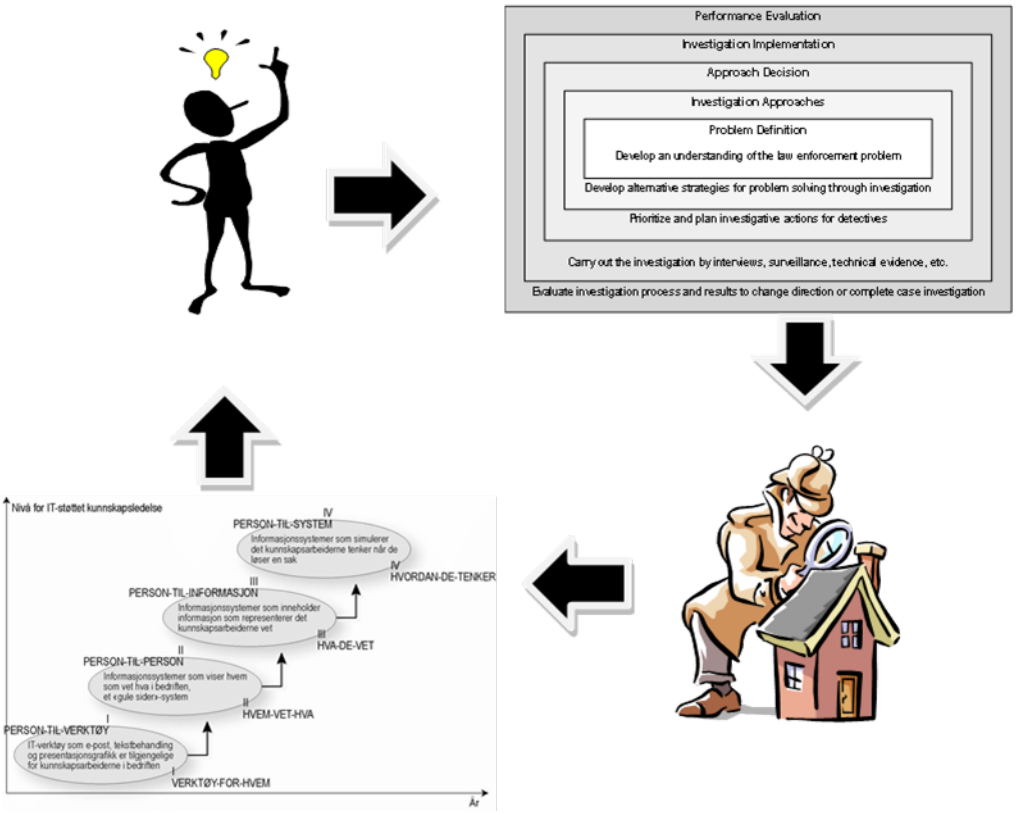

Figure 4. Four strategies for policing white-collar crime.

In general, police strategy is concerned with the choices that are made in order to reach policing goals (Ortmeier and Davis, 2012, p. 29):

> "A policing strategy is an approach to delivering police services based on specific assumptions about matters such as how police and community residents should interact, what causes crime to worsen, and how technology might be leveraged. Each strategy has unique advantages and disadvantages. Some strategies are mutually exclusive, while others complement or support one another."

An information management strategy is concerned with issues such as the sources of information and quality of information in police work. A knowledge management strategy is concerned with personnel and their knowledge areas. An information systems strategy is concerned with using information and communication technology to store and retrieve electronic information. A value configuration strategy is concerned with the choice between a value chain, value shop and value network. These strategies may in part be mutually exclusive, and they may also partially compliment and support one another.

References

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

Blickle, G., Schlegel, A., Fassbender, P. and Klein, U. (2006). Some Personality Correlates of Business White-Collar Crime. *Applied Psychology: An International Review* 55 (2), pp. 220-233.

Bookman, Z. (2008). Convergences and Omissions in Reporting Corporate and White Collar Crime, *DePaul Business & Commercial Law Journal* 6, pp. 347-392.

Bucy, P.H., Formby, E.P., Raspanti, M.S. and Rooney, K.E. (2008). Why do they do it?: The motives, mores, and character of white collar criminals, *St. John's Law Review* 82, pp. 401-571.

Chaffey, D. and White, G. (2011). *Business Information Management*, Second Edition, London: Prentice Hall.

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), pp. 535-543.

Durcikova, A. and Gray, P. (2009). How Knowledge Validation Processes Affect Knowledge Contribution, *Journal of Management Information Systems* 25 (4), pp. 81-107.

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

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

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.

Podgor, E.S. (2007). The challenge of white collar sentencing, *Journal of Criminal Law and Criminology* 93 (3), pp. 1-10.

Robson, R.A. (2010). Crime and Punishment: Rehabilitating Retribution as a Justification for Organizational Criminal Liability, *American Business Law Journal* 47 (1), pp. 109-144.

Schnatterly, K. (2003). Increasing firm value through detection and prevention of white-collar crime, *Strategic Management Journal* 24, pp. 587-614.

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.