COMPUTER INFORMATION SYSTEMS IN FINANCIAL CRIME INVESTIGATIONS

PETTER GOTTSCHALK
Norwegian School of Management
0484 Oslo, Norway

HANS SOLLI-SAETHER
Norwegian School of Management
0484 Oslo, Norway

ABSTRACT

Information technology to support knowledge work of police officers is improving. For example, new information systems applying data mining techniques that support police investigations are evolving. Police investigation is an information-rich and knowledge-intensive practice. The purpose of this article is to explore information and communication technology in the context of computer information systems to support financial crime investigations. White-collar 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, accounting and computer forensics are currently the investigators best tools in detection and implemented in most white-collar investigations in recent years.

Keywords: Data mining, business intelligence, stages of growth, knowledge management systems.

INTRODUCTION

White-collar 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 [6] 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.

The purpose of this article is to explore information and communication technology in the context of computer information systems to support financial crime investigations. Systems to support knowledge work in police investigations are identified as knowledge management systems, and knowledge management systems are organized according to stages of knowledge management technology in this article.

The article starts by describing financial crime and financial crime investigations in terms of detective knowledge work. Next, the example of business intelligence focused on data mining in financial crime investigations is presented. Finally, the stage model for knowledge management technology is introduced to financial crime investigations.

FINANCIAL CRIME

In the fall of 2008, a man of West African origin was sentenced to 4 years and 6 months imprisonment by a court in Norway. He was charged with being an accomplice to the illegal smuggling and distribution of 1 kilo cocaine, and with the aggravated handling of the proceeds of crime for having exchanged approximately 2.2 million Norwegian kroner (300,000 US dollars) and transferred approximately 1.4 million Norwegian kroner (200,000 US dollars) out of the country (Norway), and with having used false ID documents [3].

The Financial Intelligence Unit [3] in Norway had in this case prepared an analysis based on information from several messages (suspicious transaction reports from financial institutions in Norway) received one year before. The messages were received due to large and frequent currency exchanges and money transfers out of the country. Persons who did not appear to have legal access to the amounts of money in question conducted the currency exchanges and transfers.

The Financial Intelligence Unit [3] reported the matter to the local police district in Norway, which prosecuted the African, and the court sentenced him to 4 years and 6 months imprisonment. This is an example of a financial intelligence case on which this article is based.

Financial crime is often defined as crime against property, involving the unlawful conversion of property belonging to another to one's own personal use and benefit. Financial crime is profit-driven crime to gain access to and control over property that belonged to someone else.

Pickett and Pickett [15] define financial crime as the use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities. They use the terms financial crime, white-collar crime, and fraud interchangeably. Fraud can be defined as an intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right.

Financial crime often involves fraud. Financial crime is carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud, and health care fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, and social engineering. Embezzlement and theft of labor union property and falsification of union records used to facilitate or conceal such larcenies remain the most frequently prosecuted Labor-Management Reporting and Disclosure Act offences in the US [20].

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

Received: August 1, 2009 Revised: September 13, 2009 Accepted: September 22, 2009

Interpol [10] argues that financial and high-tech crimes – currency counterfeiting, money laundering, intellectual property crime, payment card fraud, computer virus attacks and cyber-terrorism, for example — can affect all levels of society.

Michel [14] argues that financial crime is opportunity driven. Opportunity is a flexible characteristic of financial crime and varies depending on the type of criminals involved. Types of financial crime can vary as much as the criminal organizations and criminal businessmen involved. The opportunity emerges when a weakness in a procedure has been discovered. Opportunities appear when a risk exists.

When comparing legal and illegal activities, Michel [14] argues that the reasons why businessmen retain the services of experts in the financial market are the same as those of criminals. The assignment will be justified for reasons of competency.

While white-collar crime may have many similarities with non-criminal business activities, there are certainly significant differences. White-collar crime contains several clear components [15]:

- *It is deceitful.* People involved in white-collar crime tend to cheat, lie, conceal, and manipulate the truth.
- *It is intentional.* Fraud does not result from simple error or neglect but involves purposeful attempts to illegally gain an advantage. As such, it induces a course of action that is predetermined in advance by the perpetrator.
- *It breaches trust.* Business is based primarily on trust. Individual relationships and commitments are geared toward the respective responsibilities of all parties involved. Mutual trust is the glue that binds these relationships together, and it is this trust that is breached when someone tries to defraud another person or business.
- *It involves losses.* Financial crime is based on attempting to secure an illegal gain or advantage and for this to happen there must be a victim. There must also be a degree of loss or disadvantage. These losses may be written off or insured against or simply accepted. White-collar crime nonetheless constitutes a drain on national resources.
- *It may be concealed.* One feature of financial crime is that it may remain hidden indefinitely. Reality and appearance may not necessarily coincide. Therefore, every business transaction, contract, payment, or agreement may be altered or suppressed to give the appearance of regularity. Spreadsheets, statements, and sets of accounts cannot always be accepted at face value; this is how some frauds continue undetected for years.
- *There may be an appearance of outward respectability.* Fraud may be perpetrated by persons who appear to be respectable and professional members of society, and may even be employed by the victim.

DETECTIVE KNOWLEDGE WORK

According to Tong [21], the secretive nature of the detective world has attracted little attention from researchers. However, competing perspectives about detective work can be discerned from available literature. Detective work has been characterized as an art, a craft, a science, and a combination of all three. The old regime of the seasoned detective highlighted the notion of detective work as a craft. An alternative perspective highlights the scientific nature of detective work, which focuses on the skills needed for crime scene management, the use of physical evidence, investigative interviewing, informant handling, offender profiling, management of the investigative process, and knowledge management. Detective work as an art suggests only tacit knowledge and creativity as components in police investigations.

Tong [21] constructed the following profile of an effective detective after analyzing the academic literature relating to detective skills and abilities:

1. *Personal Qualities.* Intelligence, common sense, initiative, inquisitiveness, independence of thought, commitment, persistence, ability to talk to people, flexibility, ability to learn, reflexivity, lateral thinking, creative thinking, patience, empathy, tolerance and interpreting uncertain and conflicting information, ability to work away from family and home, interpreting feelings, ideas and facts, honesty and integrity.
2. *Legal knowledge.* Knowledge of the law referring to police powers, procedure, criminal justice process, a good grounding in criminal law, awareness of changes to legislation, courtroom protocol, rules of disclosure, use of evidence, format of case file and awareness of defense arguments.
3. *Practical knowledge.* Technology available to detectives and used by criminals, understanding the context in which crime is committed and awareness of investigative roles of different functions of the police organization and specialist advisors. Recognition that crime changes with time and place and may require police responses that are tailored to specific context. Forensic awareness and practical expertise (e.g. crime scene preservation and packaging of evidence).
4. *Generic knowledge.* Recognition that knowledge changes, awareness of developments in practice will allow the detective to remain up to date.
5. *Theoretical knowledge.* Understanding of theoretical approaches to investigative reasoning and theories of crime.
6. *Management skills.* The management and control of case information, implementing investigative action, formulating investigative strategies, verify expert advice, prioritize lines of enquiry, formulate media strategies, awareness of resource availability and knowledge of roles of personnel available to the investigation. Manage knowledge and learning through the use of research skills to enable the detective to remain up to date.
7. *Investigative skills.* Interview technique, presenting evidence, cultivating informants, extracting core information (from files, reports, victims and witnesses), file construction, appraising and evaluating information, ability to absorb and manage large volumes of information, statement taking, problem-solving, formulating lines of enquiry, create slow time, assimilate information from crime scene, continually review lines of enquiry, question and challenge legal parties.
8. *Interpersonal skills.* Ability to communicate and

establish a rapport with a range of people, remain open minded, awareness of consequences of actions and avoid speculation.

Stelfox and Pease [18] argue that there has been surprisingly little empirical research into the way in which individual officers approach the task of investigating crime. In their own research they found that investigators are practical people. Assuming that the cognitive abilities of the average investigator are no more nor less than the population as a whole, it can be anticipated that he or she will remain liable to make the same cognitive errors as the rest of us. Assuming also that the decision-making environment the detective works in is unlikely to change much, it can be anticipated that errors will recur.

Intelligence has emerged as an important component of contemporary policing strategies. However, Innes et al. [8] argue that crime intelligence analysis is used in line with traditional modes of policing; is a way of claiming 'scientific objectivity' for police actions; and is largely shaped by police perspectives on data. They argue that the sense of enhanced objectivity often attributed to the products of 'intelligence work' is frequently overstated. Therefore, the products of crime analysis might better be understood as an artifact of the data and methods used in their construction, rather than providing an accurate representation of any crime problems.

Added to which, Innes et al. [8] found that there has been increasing frustration within certain sections of the police organization, with the perceived failure of community-policing programs to facilitate the routine supply of high-quality information to the police from members of the community. Any such concerns with low policing have been reinforced and amplified by recent developments at the 'high policing' level, where there is a well documented shift towards trying to effect enhanced national security from threats posed by terrorist groups, drug cartels and organized-crime networks.

One of the bottlenecks in international police cooperation is the targeting of the proceeds of crime. International agencies such as Interpol and Europol are sometimes involved in the interaction between the authorities and enforcement organizations of the countries concerned. Borgers and Moors [1] studied bottlenecks in international cooperation for the Netherlands in targeting the proceeds of crime. While no bottlenecks were found in cooperation with countries such as Belgium and the United Kingdom, bottlenecks were found in relation with countries such as Spain and Turkey. In relation to Turkey, the Netherlands acts mainly as the requesting state and not the requested state [1: 8]:

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

To fight organized crime, law enforcement in the UK reorganized. The United Kingdom's Serious Organized Crime Agency (SOCA) commenced operations in 2006 with an annual budget of £400 million. SOCA amalgamates the National Crime Squad, the National Criminal Intelligence Service (NCIS), and investigators from Customs and the Home Office's Immigration Service [16].

BUSINESS INTELLIGENCE

In the private sector, a term called "business intelligence" has received substantial attention in recent years. Although different from police intelligence, business intelligence has some interesting perspectives for police intelligence as well [12, 24].

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

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

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

Data have to be captured and organized before they are available for analysis. Data redundancy in terms of the presence of duplicate data should be avoided. Data inconsistency, where the same attribute may have different values, should be avoided as well. Rather than having traditional files where data are stored, it is much better to have data in databases, data warehouses, and data marts. Database technology cuts through many of the problems of traditional file organization. A database is a collection of data organized to serve many applications efficiently by centralizing the data and controlling redundant data [12: 240]:

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

A data warehouse is a database that stores current and historical data of potential interest to decision makers throughout the organization. The data originate in many core operational transaction systems, such as systems for sales, customer accounts, and manufacturing, and may include data from web site transactions. The data warehouse consolidates and standardizes information from different operational databases so that the information can be used across the enterprise for management analysis and decision-making [12].

A data mart is a subset of a data warehouse in which a summarized or highly focused portion of the organization's data

is placed in a separate database for a specific population of users. A data mart typically focuses on a single subject area or line of business, so it usually can be constructed more rapidly and at lower cost than an enterprise-wide data warehouse [12].

The following components constitute IT for BI:

- OLAP — On Line Analytical Processing. It refers to IT tools that allow for navigation in databases for hierarchies, relationships, developments and other perspectives. OLAP provides multidimensional and summarized views of business data and is used for modeling, analysis, reporting and planning of business activities. OLAP enables users to obtain online answers to ad hoc questions.
- Data Mining. This component takes advantage of statistical analysis techniques such as correlation analysis and regression analysis. Data mining is more discovery-driven than OLAP.
- Performance Management. For example, a balanced score card collects and exhibits performance in key areas such as finance, personnel, production, and market.

Similar to police intelligence, business intelligence is concerned with the identification of critical information for business performance. Business intelligence applications and their underlying critical information concepts support the needs of the business provided they are tightly integrated to both business environment and information technology infrastructure [24].

DATA MINING

Data mining will here be treated not as a sub-set of business intelligence, but rather as a complementary approach. Watkins et al. [23] explored data mining technologies as tools to investigate money laundering. Money laundering enforcement operations have developed into a combination of informant information and other intelligence sources, as well as sophisticated analysis of voluminous, often complex financial transaction arrays. The idea is to uncover patterns. The volume of electronic records and the complexity of the relationships call for innovative techniques aiding financial investigators in generating timely, accurate leads.

Data mining as a component in business intelligence takes advantage of statistical analysis techniques such as correlation analysis and regression analysis. Data mining is more discovery-driven than OLAP. Data mining provides insights into organizational data that cannot be obtained with OLAP by finding hidden patterns and relationships in large databases and inferring rules from them to predict future behavior. The types of information obtainable from data mining include associations, sequences, classifications, clusters, and forecasts. Associations are occurrences linked to a single event. Sequences are events linked over time. Classifications recognize patterns and frequencies. Clustering differentiates groups.

Data mining techniques can be applied in policing to find relevant information and combine information in data warehouses [17: 4295]:

> Data mining is a process of extracting nontrivial, valid, novel and useful information from large databases. Hence, data mining can be viewed as a kind of search for meaningful patterns or rules from a large search space that is the database.

However, data mining as any other computer software has limitations Lind et al. [13]:

> Whenever huge masses of personal data are stored at one place, and especially when tied to a system with the intelligence to tailor this data, there is enormous privacy risk. The idea is that strict access controls surround the data. Will that be the case? We can only hope. We see a risk of abuse from corrupted personnel and from hackers or other intruders. Also, there is a risk that data is overly interpreted as true, and that end users be wrongly accused. With the ease in accessing and perhaps performing data mining on huge amounts of personal data, the risk that a police investigation might take the wrong turn is much greater.

In their study of data mining technologies as tools to investigate money laundering, Watkins et al. [23] found that data mining solutions can provide a series of benefits to line level financial investigators. However, they also pointed to a number limitations associated with using technologically driven approaches in an investigative environment. For example, investigating police officers must be trained to apply and understand such systems, including fuzzy logic and genetic algorithms.

KNOWLEDGE MANAGEMENT SYSTEMS

Knowledge management is concerned with simplifying and improving the process of sharing, distributing, creating, capturing, and understanding knowledge. Information and communication technology can play an important role in successful knowledge management initiatives. The extent of information technology can be defined in terms of growth stages for knowledge management systems. In this article, a model consisting of four stages is applied to knowledge work in financial crime investigations: officer-to-technology systems, officer-to-officer systems, officer-to-information systems and officer-to-application systems respectively as illustrated in Figure 1 [5]:

1. *Officer-to-Technology Stage: Tools for end users* are made available to knowledge workers. In the simplest stage, this means a capable networked PC on every desk or 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 recognized by widespread dissemination and use of end-user tools among knowledge workers in the company. For example, lawyers in a law firm will in this stage use word processing, spreadsheets, legal databases, presentation software, and scheduling programs.

   Related to the new changes in computer technology is the transformation that has occurred in report writing and recordkeeping in police investigations. Every police activity or crime incident demands a report on some kind of form. The majority of police patrol reports written before 1975 were handwritten.

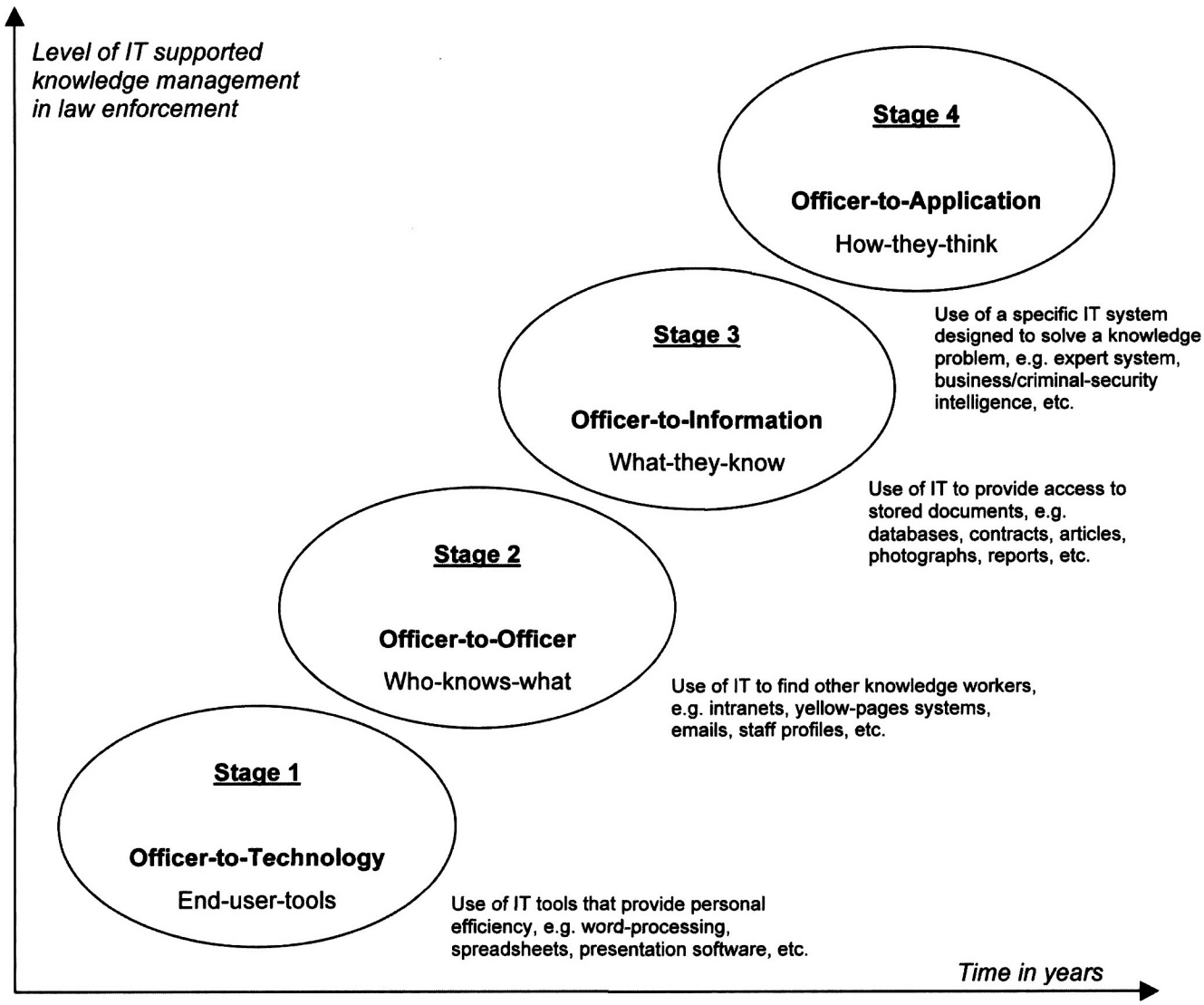

FIGURE 1 — The knowledge management systems stage model for policing

Today, officers can write reports on small notebook computers located in the front seat of the patrol unit; discs are handed in at the end of the shift for hard copy needs. Cursor keys and spell-check functions in these report programs are useful timesaving features.

An example of a specialized officer-to-technology system is a fraud examination process tool that centers on the fraud hypothesis approach, which has four sequential steps [7]:

a. Analyzing the available data: An auditor gathers document-evidence depicting all of the business.
b. Developing a fraud hypothesis: Based on what is discovered during analysis, a fraud examiner develops a hypothesis — always assuming a worst-case scenario — of what could have occurred. The hypothesis addresses one of the three major classifications of occupational (internal) fraud: asset misappropriations, corruption or fraudulent financial statements.
c. Revising it as necessary: If, for example, the facts do not point to a kickback scheme, the fraud examiner will look for the possibility of a billing scheme. Although the two schemes have several common elements, the latter raises own red flags.
d. Confirming it: Testing the hypothesis by combining theoretical elements with empirical evidence.

Stage 1 can be labeled *end-user-tools* or *people-to-technology* as information technology provide knowledge workers with tools that improve personal efficiency.

2. *Officer-to-Officer Stage: Information about who knows what* is made available to all people in the firm and to target outside partners. Search engines should enable work with a thesaurus, since the terminology in which expertise is sought may not always match the terms the expert uses to classify that expertise.

Electronic networks of practice are computer-mediated discussion forums focused on problems of practice that enable individuals to exchange advice and ideas with others based on common interests. Electronic networks have been found to support organizational knowledge flows between geographically dispersed co-workers and distributed research and development efforts. These networks also assist cooperative open-source software development and open congregation on the Internet for individuals interested in a specific practice. Electronic networks make it possible to share information quickly, globally, and with large numbers of individuals.

Information systems at stage 2 are knowledge networks systems, and they are also known as expertise location and management systems. These systems address the problem that arises when the appropriate knowledge is not represented as information in the form of a digital document at stages 1 or 3, but instead reside in the memory of expert individuals in the organization [12: 448]:

> Knowledge network systems provide an online directory of corporate experts in well-defined knowledge domains and use communication technologies to make it easy for employees to find the appropriate expert in the organization.

Some knowledge network systems go further than this by systematizing the solutions developed by experts and then storing the solutions in a knowledge support database as best practices or frequently asked questions (FAQ) repositories at stage 3.

An example of a stage 2 system in policing financial crime is knowledge network system exchanging information about self-regulation in the private sector. Self-regulation in the form of corporate governance cannot alone prevent white-collar crime. Governance in the form of clear policies and procedures, formalized cross-company communication, along with performance-based salary for board members and employees reduces incidences of white-collar crime within corporations. An ethical issue is whether there should be material reward for not committing a crime. Such a reward policy might be perceived as paying drug dealers for not selling drugs, if the same strategy were to be applied to ordinary criminals. Also it insinuates that board members and corporate executives are not well compensated already, which is not the case in many industries that are plagued with while-collar crime, including the financial sector [6].

Stage 2 can be labeled *who-knows-what* or *people-to-people* as knowledge workers use information technology to find other knowledge workers.

3. *Officer-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, as discussed earlier in this article.

An important kind of systems for policing financial crime at stage 3 is business intelligence systems. BI systems provide the ability to analyze business information in order to support and improve management decision-making across a broad range of business activities [2]. For example, Staffordshire Police in Great Britain uses a series of custom-made applications including crime recording, custody recording, file preparation, courts administration, and an intelligence system. A small number of criminals are committing most of the crime and detailed BI analysis of data reveal information about offenders and lead to their eventual prosecution. Functions in the system include general queries, property queries, statistical searches, crime profiling queries, and prolific-offender queries.

An important source of information for stage 3 policing systems is private sector organization's contribution in the control of financial crime. This contribution was by Gilsinan et al. [4] identified in terms of five distinct roles. Each role has its own dynamics and implications for successful suppression of unlawful conduct. The five roles are grudging informant, enthusiastic intelligence operative, agent provocateur, cop on the take, and officer friendly:

- The *grudging informant* is an organization that complies with the requirement to produce information for public sector enforcement activity.
- The *enthusiastic intelligence operative* is an organization that finds it profitable to have a partnership with the government.
- The *agent provocateur* is an organization that adheres to the provision requiring the chief operating and financial executives to certify that the firm's internal controls provide transparency to the financial processes of the company.
- The *cop on the take* is an organization where corporate entities have the primary responsibility for policing their own ranks for compliance with regulatory strictures.
- The *officer friendly* is an organization that acts from different motives than the government and with different abilities, and both end up engaging in a kind of token enforcement strategy.

Gilsinan et al. [4] argue that a calculus of incentives and disincentives determines which role will be adopted by the private sector. For the grudging informant, a disincentive can be found in customers who demand secrecy in their financial dealings. For the enthusiastic intelligence operative, an incentive is technology that allows private brokers to gather large amounts of information and package these data as a commodity for sale to governments. For the agent provocateur an incentive is to better manage risk and thereby increasing their stock's market appeal. For the cop on the take, a disincentive is a potential stock market bubble that encourages risk taking with the lure of enormous, quickly realized profits. For the officer friendly, an incentive is external business threats from fraudulent activity by competitors.

Gilsinan et al. [4] argue further that the temptation

towards malfeasance is high when the private sector is responsible for both the provision and production of industry regulation. Behaviors change when such provision and production is linked to fraudulent activity perpetrated by individuals external to the organization and when either government resources or likelihood of success are in short supply. In these kinds of situations, the government tends to be laid back while businesses tend to optimize their own utility.

Tellechea [19] suggests the introduction of reverse corruption, where individuals and entities are incentivized to uncover and report misconduct by quickly and efficiently giving them a share of any seized funds. There is precedent for this type of approach in the USA. If you provide sufficiently detailed information on a tax evader, then the Internal Revenue Service may award you up to 15 per cent of the amount recovered in taxes and penalties up to a maximum of $2 million. In 2003, whistleblowers in the USA received $4.1 million in rewards. In 2002, IRS paid $7.7 million and recovered $66.9 million in taxes, fines, penalties and interest. The record year was 2000, when $10.8 million was paid. Such incentives might stimulate the flow of information into stage 3 systems.

Stage 3 can be labeled *what-they-know* or *people-to-docs* as information technology provide knowledge workers with access to information that is typically stored in documents. Examples of documents are contracts and agreements, reports, manuals and handbooks, business forms, letters, memos, articles, drawings, blueprints, photographs, e-mail and voice mail messages, video clips, script and visuals from presentations, policy statements, computer printouts, and transcripts from meetings.

4. *Officer-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 using data to classify cases into one category or another. Another example is expert systems that can enable the knowledge of one or a few experts to be used by a much broader group of workers requiring the knowledge. Officer-to-application systems will only be successful if they are built on a thorough understanding of law enforcement.

An example of a stage 4 system not yet implemented is a system for evaluation of compliance levels according to recommendations by the Financial Action Task Force (FATF). The FATF was formed in 1989 by the G-7 group of countries, motivated by the General Assembly of the United Nations' adoption of a universal pledge to put a halt to money laundering, fuelled largely at that time by the laundering of illegal drug trade money. One of the FATF's first tasks was to develop measures to combat money laundering [11].

A set of Forty Recommendations was issued by the FATF. They were designed to provide a comprehensive strategy for action against money laundering. FATF members have been evaluated over a number of years against these recommendations and more recently against the Nine Special Recommendations using self-assessment and/or mutual assessment procedures. Self-assessment is a questionnaire-based yearly exercise. Mutual evaluation involves an onsite visit by experts from other member countries in the areas of law, financial regulation, law enforcement, and international co-operation [11].

The result of a mutual evaluation may be one of the following compliance levels [11]:

a. Non-Compliant (NC). There are major shortcomings, with a large majority of the essential criteria not being met.
b. Partially Compliant (PC). Some substantive action has been taken, and there is compliance with some of the essential criteria.
c. Largely Compliant (LC). Only minor shortcomings, with a large majority of the essential criteria being fully met.
d. Fully Compliant (FC). The recommendation is fully observed with respect to all essential criteria.

To be able to compare compliance across countries, each compliance level was assigned a numerical level: NC = 0, PC = 0.33, LC = 0.67 and FC = 1.0. The highest compliance scores were achieved by the following countries [11]:

Belgium	0.77
UK	0.70
USA	0.69
Portugal	0.69
Norway	0.68
Switzerland	0.64
Ireland	0.63

Johnson [11] argues that the results here should be used as a guide only to the ranking and compliance of countries rather than some exact measurement of compliance. This is because compliance levels are very broad, where substituting a single value for each compliance level provides only a crude measure of compliance for comparisons to be made. Only a future system based on artificial intelligence might provide an exact measure of compliance.

An example of a stage 4 system in policing is dynamic emergency response information system (DERMIS) conceptually introduced by Turoff et al. [22]. They developed a set of general and supporting design principles and specifications for DERMIS by identifying design premises resulting from the use of indexes. The principles are based on the assumption that implicit in crises of varying scopes and proportions are communication and information needs that can be addressed by today's information and communication technologies. What is required, however, is organizing the premises and concepts that can be mapped into a set of generic design principles.

Turoff et al. [22] identified the following eight design premises for DERMIS design:

Crime \ Stage	Officer-to-technology	Officer-to-officer	Officer-to-information	Officer-to-application
Financial crime			Business intelligence systems for analyzing	Artificial intelligence etc.
White-collar crime		Network system exchange information about self-regulation	Data mining tools to investigate money laundering	
Fraud	Fraud examination process tools		Data warehousing etc.	

TABLE 1 — Synthesizing framework for CIS use in financial crime investigation

a. System training and simulation. An emergency system that is not in use on a regular basis before an emergency will never be useful in an actual emergency.
b. Information focus. People responding to an emergency are working 14-18 hour days and have no tolerance or time for things unrelated to dealing with the crisis.
c. Crisis memory. Learning and understanding what actually happened before, during, and after the crisis is extremely important for the improvement of the response process.
d. Exceptions as norms. Almost everything in a crisis is an exception to the norm.
e. Scope and nature of crisis. The critical problem of the moment is the nature of the crisis, a primary factor requiring people, authority, and resources to be brought together at a specific period of time for a specific purpose.
f. Role transferability. It is impossible to predict who will undertake what specific role in a crisis situation. The actions and privileges of the role need to be well defined in the software of the system and people must be trained for the possibility of assuming multiple or changing roles.
g. Information validity and timeliness. Establishing and supporting confidence in a decision by supplying the best possible up-to-date information is critical to those whose actions may risk lives and resources.
h. Free exchange of information. Crises involve the necessity for many hundreds of individuals from different organizations to be able to exchange information freely, delegate authority, and conduct oversight, without the side effect of information overload.

Some of the premises remind us of stage 2, where communication and information exchange between people is the most important feature. Thus, a DERMIS may be developed according to the stage model by first including communication aspects at stage II, then move into information bases at stage 3, and finally combine systems users and information sources into information services in emergency situation.

Stage Four can be labeled *how-they-think* or *people-to-systems* where the system is intended to help solve a knowledge problem.

DISCUSSION

The preceding presentation has attempted to provide a well-researched overview of modern police information system processes and tactics with regard to financial crime. Problems and challenges were described within the context of today's national organizational IT structures that are increasingly aligned to provide information across multiple data sources. The information technology and management based solutions presented for tracking these efforts should have merit in terms of providing a view into the increasing flexibility and innovation of law enforcement agencies.

It is important to summarize the review of literature presented in this paper, thereby increasing one of its venues of contribution. We salvage the paper by synthesizing the vast amount of information in Table 1, so that the venues are summarized and presented in a single view.

From a pure academic perspective, this research paper should be valuable in sparkling further innovative inquiry into the areas of criminal profiling, data mining and artificial intelligence. However, from a practical point of view, the steps and procedures outlined only make a simple mention of modern international collaboration between law enforcement agencies. Within the last decade, collaboration at the political, regulatory, organizational, process and systems levels seem to have international white-collar crime fighting a model of improved efficiency and success. Many information technology professionals and scholars lack insight and international perspective to understand the complexity of white-collar crime fighting with regard to financial transaction. To that end, the international perspective needs to be expanded in future research into computer information systems in financial crime investigations.

CONCLUSION

This paper has presented a foundation for understanding white-collar crime and the process-centric stages and systems that are deployed to address large scale fraud and other kinds of financial crime. The main research topic addressed is exploring the landscape for computer information systems in financial crime investigation.

Information technology to support knowledge work of police officers is improving. For example, new information systems supporting police investigations are evolving. Police investigation

is an information-rich and knowledge-intensive practice. Its success depends on turning information into evidence. However, the process of turning information into evidence is neither simple nor straightforward. The raw information that is gathered through the investigative process is often required to be transformed into usable knowledge before its value as potential evidence can be realized. Hence, in an investigative context, knowledge acts as an intervening variable in this transformative process of converting information via knowledge into evidence.

REFERENCES

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

[2] Elbashir, M.Z., Collier, P.A. and Davern, M.J. (2008). Measuring the effects of business intelligence systems: The relationship between business process and organizational performance, *International Journal of Accounting Information Systems*, 9, 135-153.

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

[4] Gilsinan, J.F., Millar, J., Seitz, N., Fisher, J., Harshman, E., Islam, M. and Yeager, F. (2008). The role of private sector organizations in the control and policing of serious financial crime and abuse, *Journal of Financial Crime*, 15 (2), 111-123.

[5] Gottschalk, P. (2008). Stages of financial crime by business organizations, *Journal of Financial Crime*, 15 (1), 38-48.

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

[7] Ilter, C. (2009). Fraudulent money transfers: a case from Turkey, *Journal of Financial Crime*, 16 (2), 125-136.

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

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

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

[11] Johnson, J. (2008). Is the global financial system AML/CFT prepared? *Journal of Financial Crime*, 15 (1), 7-21.

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

[13] Lind, H., Hjelm, J. and Lind, M. (2007). Privacy surviving Data Retention in Europe? *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, www.w3.org.

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

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

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

[17] Srinivasa, K.G., Venugopal, K.R. og Patnaik, L.M. (2007). A self-adaptive migration modell genethic algorithm for data mining applications, *Information Sciences*, 177, 4295-4313.

[18] Stelfox, P. and Pease, K. (2005). Cognition and detection: reluctant bedfellows? In: Smith, M. and Tilley, N. (editors), *Crime Science: New Approaches to Preventing and Detecting Crime*, UK: Willan Publishing.

[19] Tellechea, A.F. (2008). Economic crimes in the capital markets, *Journal of Financial Crime*, 15 (2), 214-222.

[20] Toner, G.A. (2009). New ways of thinking about old crimes: Prosecuting corruption and organized criminal groups engaged in labor-management racketeering, *Journal of Financial Crime*, 16 (1), 41-59.

[21] Tong, S. (2007). *Training the Effective Detective: Report of Recommendations*, University of Cambridge. Author contact details: Dr Stephen Tong, Senior Lecturer in Policing, Canterbury Christ Church University, Kent, UK.

[22] Turoff, M., Walle, B. V. d., Chumer, M. and Yao, X. (2006). The Design of a Dynamic Emergency Response Management Information System (DERMIS), *Annual Review of Network Management and Security*, Volume 1, 101-121.

[23] Watkins, R.C., Reynolds, K.M., Demara, R., Georgiopoulos, M., Gonzalez, A. and Eaglin, R. (2003). Tracking dirty proceeds: exploring data mining technologies as tools to investigate money laundering, Police Practice and Research, 4 (2), 163-178.

[24] Williams, S. and Williams, N. (2003). The Business Value of Business Intelligence, *Business Intelligence Journal*, Fall, 30-39.