Forensic investigation and its relationship with information assurance and corporate governance

By Maarten Van Horenbeeck

A thesis submitted in partial fulfilment of
the requirements for the post academic certificate of
Multidisciplinary Forensic Investigation

Katholieke Universiteit Leuven
Postacademic Education

2005

Abstract

Forensic investigation and its relationship with information assurance and corporate governance

By Maarten Van Horenbeeck
Supervisor: Prof. Dr. Willy Geysen

This thesis will present some of the changes that have occurred in the field of Information Assurance and Corporate Governance regulation in the past two decades. It will investigate the impact these have had on how forensic investigations need to be conducted within a corporation. The first changes are already being observed in how adherence to legislation and policy is afterwards interpreted in court.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e - mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e - mail address, logo, person, place or event is intended or should be inferred.

Product names or company names mentioned in this report may be the trademark of their respective owners.

Acknowledgements

Hereby I would like to thank the program committee of the post academic course in Multidisciplinary Forensic Investigation, 2005, for the organization of an excellent and useful course. I truly enjoyed the lectures given which provided a great deal of very useful information. Thank you.

Second, I would also like to take the opportunity to thank each of my fellow students. Many interesting discussions resulted from this course, which inspired me significantly to further research certain subjects. Thank you all.

Additional thanks go out to Tom Nijs and the other DPAV associates that answered my many questions throughout the year.

Table of Contents

Introduction

This paper has as goal to investigate the impact recent changes in information assurance and corporate governance policy and legislation have had on how forensic investigations are conducted within a corporate context. It provides samples of where information assurance processes have or should be implemented in the actual forensic process, as well as the impact such changes within organizations have had on the efficiency of a forensic investigation.

The importance of this matter has been stressed over the last few years due to a significant increase in the amount of investigations taking place within high profile organizations. Good examples of this are the recent Enron and Worldcom/MCI fraud investigations. In addition, courts have also become much more stringent in identifying the way information was gathered, as has been demonstrated in the very public OJ Simpson trial.

Samenvatting in het Nederlands (Dutch Summary)

As requested by the program committee of the course, the following is a brief Dutch language introduction and summary of the rest of this paper. Thank you for allowing me to write the rest of this paper in English.

Deze scriptie beoogt tot doel het beschrijven van de invloed die Corporate Governance (goed ondernemingsbestuur) en Information Assurance (Informatie beveiliging) tot gevolg hebben gehad op het uitvoeren van een multidisciplinair forensisch onderzoek binnen een onderneming.

Uitgebreide gerechtelijke onderzoeken naar financiële criminaliteit bij onderandere Enron, Lernout & Hauspie en MCI/Worldcom hebben de laatste jaren de investeringswereld op zijn grondvesten doen donderen. Naar aanleiding van deze gebeurtenissen is verscheidene wetgeving, zoals Sarbanes Oxley en Gramm-Leach-Bliley in de VS, en ondermeer de Code Lippens in België in plaats gebracht die tot doel heeft om het concept van hoe een deugdelijk bedrijf geleid dient te worden, in kaart te brengen. Deze wetgeving verplicht ondernemingen van extra procedures en processen in plaats te brengen die het mogelijk maken van fraude op een snelle manier op te merken.

Omdat dergelijke wetgeving in het verleden gebleken is niet te werken zonder duidelijk de verantwoordelijkheid vast te leggen, voert bijvoorbeeld Sarbanes Oxley een statement in waardoor de CEO en CFO van een organisatie zelf aan dienen te geven in financiële rapportering dat zij verantwoordelijk zijn voor het in plaats stellen van een duidelijk audit en controlesysteem. We zien ook hoe, voor het bestaan van Sarbanes Oxley, een grote onderneming op korte tijd ten val kwam wegens het naleven van een interne policy die door een Amerikaanse jury niet consequent met hun waarden geacht werd.

De invoering van dergelijke wetgeving heeft voor een forensisch onderzoek voornamelijk tot gevolg gehad dat er een grote uitbreiding is geweest van

interne controleorganen. Door deze additionele controle is het theoretisch gezien mogelijk om meer informatie te bieden aan eventuele forensische onderzoeken die vanuit overheidsopdracht zouden plaatsvinden. Zoals echter vaak het geval is bij additionele wetgeving is de samenstelling van het bedrijf en zijn controleorganen vaak in ernstige mate complexer geworden. Dit kan op zichzelf wederom een detrimenteel effect hebben op de snelheid waarmee een onderzoek kan plaatsvinden.

Dit paper duidt ook op het belang van de CIA drielettercombinatie die de basisverwachtingen reflecteert van informatie: we willen dat informatie **confidentieel** blijft, **integer** is en **beschikbaar (available)**. Als voorbeeld van hoe integriteit slechts behaald kan worden mits aan enkele essentiële voorwaarden voldaan is, bespreek ik in meer detail Behavioral Profiling, en het gebruik in real-time en post-mortem modus, alsook Scientific Content Analysis techniek en leugendetectie.

Een additioneel item dat ik in deze thesis trachtte te bekijken is in hoeverre met de basisvoorschriften van information assurance en corporate governance rekening gehouden dient te worden bij het uitvoeren van een forensisch onderzoek. Er zijn reeds een aantal bekende zaken (waarvan de OJ Simpson strafrechtzaak wellicht de uitgebreidste is) geweest die, ondanks een grote hoeveelheid bewijsmateriaal, geseponeerd werden, of waar de beklaagde onschuldig verklaard werd, puur door een gebrek aan aantoonbare bewijskracht of net bewijs van corruptie langs de kant van het politiewezen.

Door de toenemende specialisatie van gerechtsdeskundigen is er eveneens een grote toename geweest van het aantal verschillende mensen dat werkt rond een bepaald onderzoek. De toenemende informatisering van zowel het gerecht als het politiewezen heeft er ook toe geleid dat toegang tot informatie geleidelijk aan eenvoudiger wordt. Hierbij moet echter wel rekening gehouden worden met een ruim aanbod aan mogelijke risicos: diefstal van laptops met confidentiële informatie, inbraak via het internet/via het netwerk, onbevoegde personen die foutief toegang verleend worden.

Ik hoop dat deze scriptie erin slaagt van enkele kanttekeningen te maken bij de huidige evolutie van het forensisch onderzoek, voornamelijk binnen een zakelijke context en wens u alvast een aangename lezing toe.

1. The information society

With the advent of information systems into today's business, governmental and even social processes there is little denial of the fact that we are more and more becoming an information society. Even the classic discoverers embarking upon yet unknown locations usually carry a satellite enabled mobile phone to update the home front using web logs, image archives and telephone communications.

Businesses are more and more integrating their business processes into information management systems. The advantages are obvious. Information can travel between separate business units freely and can be accessed in real time by all who require this information. The CEO of an organization truly has the capability of obtaining a "business dashboard" where he can, in real-time obtain information on revenue and sales results.

Within a government context, the use of information systems has also seen a significant increase. Virtually every western government has an "information society" program running, usually translating directives from the "European Information Society" program lead by the European Union[1]. Information transfer is also becoming more and more important in modern law enforcement. Exchange of information between government departments makes it possible to monitor many different sorts of crime, from human trafficking to white collar acts of mischief. Having an immediate link between an index of properties belonging to Belgian citizens overseas as well as their tax results, while subject to significant privacy concern, would doubtlessly aid in increasing the catch rate of illegal tax evasion.

As such, it is only logical that information society is embraced by government organizations to increase the efficiency of their operations.

No new evolution however is without its drawbacks. Despite the obvious merit these new technologies and their introduction have, a number of new

[1] Europe's Information Society at http://europa.eu.int/information_society/index_en.htm

questions have shown up on how they can efficiently be integrated. These questions include but are not limited to the topics of privacy, security of information and “fair use”.

In order to answer these questions efficiently, new legislation has been put in place which either directly forces organizations to place certain matters into competent hands, or indirectly triggers new policies which do exactly the same thing. Much of this legislation can be identified as part of the new **corporate governance** and **information assurance** guidelines recently published.

2. Information at the core of a forensic investigation

Gathering the required information

Methods of information gathering

Forensic investigations in all instances deal with information. While no single global definition exists, forensics is commonly interpreted as being "the use of science and technology to investigate and establish facts in criminal or civil courts of law". This means that "events" are investigated, "facts" are established and later used in a court setting. Information is gathered, analyzed and processed throughout an investigation.

The gathering of information is performed in a wide variety of fields, including, but not limited to the below:

- Questioning of victim, suspect or witnesses
- Medical investigations of victim or suspect
- Forensic investigations of crime scene (IT equipment, fire and explosion analysis, …)

Each of these techniques is by definition incomplete. They are purely based on the state of the art in their respective fields of science, and by no means offer a complete picture of what happened. From a scientific point of view, every contact that has taken place leaves traces[2]. The art of forensic science is to identify those actions that took place on or related to the crime being investigated. While in some cases, much-encompassing information such as video material may be available; this will not always be true. In these cases, it is the investigator who needs to form a complete as possible picture of what happened.

To achieve this goal, he requires the aid of forensic specialists, who do not need to provide a complete picture of what happened, merely an analysis of where their own field is related to the event. Based on this information,

[2] Edmond Locard, Police inspector of Lyons and pioneer of forensic science

investigators can achieve a view on the situation, which can either be confirmed or discarded in a potential future court of law.

Integrity of the information

In this stage, there can already be an issue regarding the integrity of the information provided. Each of the scientific techniques used is still very much subject to interpretation due to its relative incompleteness.

Good examples of these are the interrogation techniques currently in use, such as the SCAN technique, as presented by C. Verbandt. The results of a regular interrogation investigation can be influenced by both interrogator as well as suspect[3]. Influence of the interrogator can be avoided by having the suspect "tell his entire story", as in the Scientific Content Analysis method. One is invited to write down his entire story, after which form and content of the story are analyzed according to a set of predefined rules. Based on the length of certain aspects of the story, validity can be assessed. Unfortunately, suspects who are consciously aware of the technique being used can also easily evade the investigative technique. As such, integrity of the information cannot easily be obtained. One requires a trained investigator as well as the certainty that the subject is not aware of the technique – this is often difficult to establish.

As such, the definition that Sapir gave when he introduced the technique, that "SCAN is equally reliable as a polygraph test" is incorrect[4]. While the result of a polygraph test can be impacted by the questions asked and the way they are asked, it is difficult to influence by an average subject, even though he obviously has awareness of the technique. An exception to this would be a psychopath, but these are not considered "average" subjects.

Even when this definition would be adhered too, the difference in Belgium would not be very large. Polygraph tests are accepted in Belgium as a specialized interrogation method (as defined in the Ministerial mailing dd.

[3] Carla VERBANDT, session 5, "Analyse van Verbaal Gedrag"
[4] LSI, "SCAN: Deception Detection by Scientific Content Analysis", Law and Order vol.38 n.8

13/02/2003)[5]. It can never be used as excluding evidence – merely as an element of proof. This is approximately the same validity a SCAN analysis would contain when used in a court of law. Usually however, SCAN is not presented as such, but used as an investigative tool to provide assistance during questioning – in the end hopefully leading up to a full fledged confession.

In other countries, such as the United States, adhering to this definition would have much greater impact. As the US Supreme Court has not yet ruled on its admissibility, each state has jurisdiction on its own whether or not to accept polygraph tests. Usually, when both parties agree in advance, the result of a polygraph test is considered binding. The judge can also overrule such decision or enforce its admissibility based on the good standing of the polygrapher[6].

An additional example is located in the field of Behavioral Profiling, also presented by C. Verbandt. This is a technique which has been in use for a very long time, initially documented in the UK Jack the Ripper case[7] – but only truly professionalized in its current form in Israel, where it has proven very useful in real-time analysis of subjects. Originally implemented at Tel Aviv's Ben Gurion airport, it is a technique which can be implemented both in real-time as in post-mortem mode:

- In real-time mode, investigators are actively monitoring people behavior. Specific items of behavior, which are specified on a list that is kept confidential, are awarded points. Whenever a preset number of points per person is exceeded, this person will be selected for a more stringent security test. [8]
- In post-mortem mode, investigators attempt to create an image of the perpetrator by analyzing the crime committed. Hereby they aim to

[5] Gregorio CORNELIS, Session 11: "Polygrafie"
[6] Supreme Court of the United States, "United States vs Scheffer", March 31st, 1998
[7] Brent TURVEY, "Criminal Profiling: Behavioral Evidence Analysis", chapter on Sadistic Behavior
[8] Strategic Forecasting Inc., "Situational Awareness: A key to avoiding danger on subways"
The Miami Herald, April 2004, "Airport's eyes track behaviour"

> reduce the list of suspects by matching them to the physical and mental characteristics found.[9]

While integrity of the resulting information can still not be guaranteed, a good result can be achieved by using proven scientific techniques, and taking into account a wide range of alternate possibilities (such as that there may have been a third party involved which is responsible for part of the crimes committed).

The nice aspect of such behavioral profiling is that it, when well implemented, has an excellent failure mode. With this I mean that in case of the real-time implementation, the actions taken when certain thresholds are exceeded can be brought in line with the actual monitoring. Instead of preventing people to board, as with the disputed "*no fly list*" maintained in the United States, people can be taken through successive security verifications – ultimately excluding the potential of an armed attack. In the post-mortem analysis, the weight given to a behavioral analysis can be brought in line with the factual information available. These reasons may explain the recent uptick in popularity of profiling – real-time behavioral profiling is currently being performed at Logan International Airport in Boston, MA while television series such as Profiler enjoy great popularity with the viewing audience. Profiling is also a special and accentuated component of newer media series such as Cold Case – in the end a spin off of a popular crime fiction series, CSI, which shows very low audience attrition patterns for this type of series. It truly seems this type of crime investigation has triggered significant interest in Media.

Quality assurance of the information

During the process of information collection, many different parties may be involved. Each of these parties needs to be monitored and audited to make sure the quality of their work is consistent and the resulting information can be used in the further investigation or a court of law.

[9] Brent TURVEY, "Criminal Profiling: Behavioral Evidence Analysis"

The data gathering phase is most likely the most difficult one to control. Different methodologies have been employed to make sure the quality of information is consistent. These are mostly detailed in the field of Crime Scene Management.

Several different steps are implemented in today's crime scene management to prevent compromise or contamination of facts during the data gathering phase, such as the use of access perimeters[10].

After data has been gathered, analysis also needs to take place on it, to make sure information is deduced from it. The resulting information could e.g. be a blood type, a DNA pattern, or a fingerprint. Within Belgium, there are a number of laboratories that can perform these types of investigations. Regulations differ for each type of investigation, but in all, certain quality control is required[11].

In order to perform a DNA investigation, for example, a laboratory requires accreditation by ISO 17025, allow permanent access to provide samples and employ at least one professional with more than 3 years of experience in forensic DNA analysis. In practice however, the 24/7 requirement is merely theoretical, and reduced to an on-call cell phone number. It is hardly ever used as DNA material requires registration by the court registry, which is only opened during business hours (9-17h on weekdays)[12].

As presented by Prof. Dr. E. Dequeker, the Belgian organization in charge of providing ISO 17025 accreditation of laboratories is BELTEST, part of the BELAC (Belgian Organization for Accreditation). They perform testing to make sure a laboratory confirms with the guidelines put forward in ISO 17025. This means an organization should have certain documents, policies and procedures in place, such as a Quality Handbook, Standard Operating

[10] US Department of Justice, "Crime Scene Investigation: A guide for Law Enforcement", 2000
[11] E. DEQUEKER, session 19, "Kwaliteitsnormen inzake laboratoriumonderzoek"
[12] P. VAN RENTERGHEM, session 23, "Beheer van de DNA databank"

Procedures and qualified personnel. The end goal of this testing is to ensure that an organization is able to provide:

- The source of a DNA sample
- Ensure that a DNA sample contains meaningful information
- A correct communication regarding the meaning of the DNA sample

The impact of a lack of integrity of the provided results of a DNA analysis were painfully indicated in June 2003, when it became apparent that the US Kansas Bureau of Investigation had incorrectly marked a blood sample in 1991 belonging to a suspect in several sexual crimes[13]. Due to this incorrect marking, the suspect was cleared of all charges. Twelve years later he was arrested again, and a new investigation showed that he was indeed responsible for the earlier crimes. This type of event severely impacts public opinion of investigative techniques, and in disputed privacy cases such as a DNA database, could lead to further limitations to investigative powers.

Where is the information stored ?

National databases

As discussed at multiple times throughout the course, information can be stored in a diversity of databases throughout the forensic process. A number of databases are either popularly known or were identified during the course:

- The National DNA Database managed by the NICC probably is the most known and in the past, most disputed database in the country. Significant privacy concerns were identified during its initial installation.

[13] Kansas Bureau of Investigation, "Press release by Director Larry Welch", June 5, 2003

These concerns have, together with resource issues, lead to the fact that Belgium, while initially one of the first countries to start with DNA analysis, was in the end the last EU country to start an actual database[14]. Use of the database is also fairly limited as it cannot contain "suspects", only actual felons. This makes the database less useful if a very recent crime pattern is being investigated.

Many of the initial privacy concerns have been relieved by removing personal information from the actual database entries. A tracking number is kept per person, and the name of a suspect can only be requested by moving through a different procedure. Profiles can only be kept for a limited timeframe as well. International exchanges of profiles are also still very tiresome, but change is underway by definition of a separate Schengen agreement for DNA exchange. There is also an international Interpol database, mainly pursued by Croatia, but with very little information from Belgium and the Netherlands.

- In Belgium, so called "information crossroads" are used[15]. These are available in each borough, and collect information on all matters pertaining to crime in their region. On a daily basis, they summarize this information and also introduce it into the General National Database (ANG) so they can be exchanged between boroughs.

- A national database of fingerprints (dactyloscopy) is also available, much larger than the current DNA database[16]. In 2005, it contained a total of around 4 million prints (10 prints per person). It is maintained by the GID (Judicial Identification Service) in Brussels. Fully automated comparisons are available as of 1990 using the Automatic Fingerprint Identification System. On average 1500 identifications are registered on the system yearly. This is a high quality database, as

[14] P. VAN RENTERGHEM session 25, "Beheer van de DNA databank"
[15] Session 13, "Multidisciplinaire sessie" and www.polfed.be (Federal Police of Belgium), "Het Arrondissementeel Informatiekruispunt onthuld"
[16] G. VOLCKERYCK, session 12, "Vingersporenonderzoek"

Belgium requires 12 typica, unique points in a print used, to be stored for future comparison. This is significantly more than e.g. China (where 6 typica are required), or the United States and the UK, where there is no minimum requirement. A disadvantage of this database is the lack of judicial regulation surrounding it. The current implementation fails to address privacy as well as legal concerns.

Scientific databases

Perhaps an even wider range of databases are introduced into the investigative sphere from the scientific world. While a number of directly important databases may be managed by the government (as is the case in some countries regarding databases of materials – containing for example the locations where certain types of soil are located), many other databases are maintained by academic organizations, research institutions and think tanks. Often, this information is used in investigations without proper audit on the source material.

An example of this type of database usually accompanies the commercially available simulation programs for traffic accidents. A very interesting presentation was given on this subject by ir. D. Christiaens. Here he presented a number of tools, such as PC-Crash, of Austrian origin, and Karat (Germany) that can be used to investigate automobile accidents[17].

While most of the science behind this software is based on actual scientific calculations made at the time of processing, there is a certain degree of information contained in this software as part of a database. When a simulation takes place of a car crash, the size and type information for each vehicle is stored within the software. While this information is considered correct "as is", it is difficult to show that it indeed is.

[17] D. CHRISTIAENS, session 18, "Forensisch onderzoek van verkeersongevallen 1"

It is not entirely impossible that a vehicle vendor would pay off a rogue employee at the software vendor to have certain specifics changed – in order to hide vehicle fault. This is exactly where corporate governance and information assurance come into play. Corporate governance would assist in proving neutrality of the organization in question – being clear and open would prevent large payments by an automobile vendor from taking place. Information assurance could safeguard the organization from allowing one rogue employee to have access to too much information inside the database.

Organizations need to be able to support their correctness of operations. While the field of software is largely unregulated, the future seems to logically dictate that where there is a need to prove that a piece of software has not been tampered with; regulation will appear – quite similar to the rise of electronic voting machines. The organizations that are currently best structured to easily conform to such regulations are likely to be most successful at attracting government clients in the future. Currently, the field of vehicle crash analysis is very scientific, and there is little supervision in how the software operates and whether its source data is valid. This is likely to change in the near future.

It is not always necessary to obtain a resource within an organization to have information changed. Often information from the public domain or partners is trusted upon too much. Early 2005, there was significant rattle in Canada as it appeared that obtaining access to the country for deported criminals was quite easy[18]. Processing immigrant fingerprints is outsourced to a company called "International Fingerprinting Services". IFS handles documents received from foreign police services and directly imports this information into the national database. Apparently, this organization did not correctly verify the source of the fingerprints – merely added them if an easily faked stamp was available. As such, someone wishing to immigrate back into Canada could easily, and for a very low cost, obtain someone else's fingerprint information and submit it. The risk of having the print actually verified once in

[18] CTV Canada, "Criminals use fingerprint fraud to get back into Canada", March 22nd, 2005

the country is very low. This shows that governments, when outsourcing certain services, or using databases that have been prepared either in the public domain (scientific research results) or by partner organizations, needs to take care in auditing this data and/or its source organizations.

What requirements does law enforcement have of the information?

Law enforcement will have a number of requirements regarding the information that has been gathered throughout its investigation. The following parameters are modeled from the "CIA" guidelines of the BS7799 guidelines detailed under Chapter 4:

- Information needs to be available: investigations can take place at any time of the day or night, especially when information is shared with other countries that may operate in a different time zone.
- Information needs to be confidential: Information gathered during a forensic investigation may contain information private to the subject of the investigation, whether it is a private person or an organization. This type of information should only be accessible by those with a need to know.
- Integrity of the information needs to be safeguarded: Information is of no use should it not be certain that it has not been tampered with. In court, defense parties will go through every effort possible to disprove the quality and integrity of information provided by the prosecutor.

Availability of information speaks for itself. If information is not available during an investigation, it will not be used and will not be taken into account. This leads to issues regarding the quality of the investigation, and may also directly impact the validity of the result of the forensic investigation if the opposing party is aware of the lack of merit of the investigation.

Confidentiality of information is also very important. As discussed by Professor Frank Hutsebaut in his session on "expertise in criminal law", the preparatory investigation may be conducted in secret[19]. This has a very good reason. When a party is suspected of a certain crime but no official charges have been made yet, the release of any information pertaining to this investigation may lead to the deletion of evidence or other materials of material importance to the investigation.

Integrity of information also needs to be safeguarded. A good example here is the 1995 OJ Simpson trial in the United States. In this instance, the public prosecutor was unable to convince a jury that pro football player OJ Simpson had murdered his ex-wife and new husband, despite overwhelming evidence to his disadvantage. This was directly caused by the lack of assurance the prosecutor could give that the evidence provided by the Los Angeles Police Department had not been tampered with[20].

Some practical considerations regarding the way information is stored

As presented by Mr Van Renthergem during the session on management of the DNA database, the software used for this purpose is made available by the US Federal Bureau of Investigation, CODIS[21]. While the use of software similar to that used by other countries is in itself a great asset to the interoperability and potential interchange of this information, care should be taken regarding the secure implementation of such software. As not every country will have the available resources to do a complete review of the software for security purposes, this risk (albeit limited) should not be taken too lightly.

An example of a similar occurrence which in the end turned out to have great influence on the security posture of the Belgian government was the transfer

[19] Frank HUTSEBAUT, session 2, "Wettelijk kader I"
[20] Douglas O. LINDER, University of Missouri-Kansas City, "The OJ Simpson Trial", 2005
[21] P. VAN RENTERGHEM, session 25, "Beheer van de DNA databank"

of old Hagelin C38 encryption devices[22]. These devices were provided by the US Government as part of the Marshall plan, as they were abandoned by the US over security concerns. While this took place shortly after the Second World War, these machines were used throughout the Belgian occupation in the 60's. While the United States can at this time be considered a partner, it is still a reason of concern that such insecure cryptographic algorithms were used merely because they were a "gift" of the United States government.

In this case, **confidentiality** of the information contained in the database is the main issue.

There are also additional concerns with the storage of forensic data. In order to safeguard the fact that the information can be used within a court of law, it is necessary to maintain a stringent record of the Chain of Custody. As discussed in the session on Crime Scene Management, there is an increased specialization of experts into their respective field of interest[23]. Due to this, a much higher amount of people require access to potential evidence than in the past. In order to manage access to the evidence and maintain a detailed audit log of all access, the importance of this chain has increased significantly over the last few years. This is especially important for information that was transferred to third parties during the investigation. Due to the limited resources of police in respect to many of the sciences employed, it becomes increasingly necessary to e.g. transfer evidence such as computer hard drives to 3rd party companies. Tracking needs to be maintained during the transfer as well.

[22] Bart PRENEEL, ESAT, KU Leuven, "Technical approaches to Information Security", June 7th, 2005
[23] H. BAUDONCK, session 12, "Onderzoek 'plaats delict' (Crime Scene Management)"

3. Standards in corporate governance

Corporate governance is a term which was initially coined on Wall Street in the 1970's. The clearest definition that exists is the one used by the Organisation for Economic Co-Operation and Development, the OECD. They defined corporate governance as being "*the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance.*"[24]

There were however no benchmarks to which an organization could measure its own performance in this respect. This all changed when in 1992 two separate reports were released that defined internal control. The most important of these reports was the COSO report, which was published by the sponsoring organizations of the Treadway commission in the US. Of lesser importance was the Cadbury report of the UK, as the UK soon decided to use COSO as its mechanism for internal control[25].

Shortly afterwards, in 1994, this trend of importance of internal control was confirmed by Canada, who released two similar reports.

While going into these reports in depth would be beyond the purpose of this paper, it is important to understand the spirit in which they were written. In the late 80's and early 90's, investors became increasingly aware of the risk that an investment could turn into if it was managed with lack of integrity or reputation. Not only could deals be lost, the company as a whole would risk

[24] Organisation for Economic Co-operation and Development, 1999
[25] H. DEN BOER, "Business Control & Auditing", 1995

bankruptcy if certain ethical, moral or legal standards were superseded. As such, they were looking for assurance that a company they invested in acted according to certain ethical, moral and legal standards.

These investors were not the only ones who wanted some sort of oversight on how organizations did business. In the meanwhile, governments, in the end investors alike, wanted to see stable economies – built on stable companies. As such, they considered it only normal to have investigative reports written (such as the COSO and Cadbury reports detailed above). It did not take very long until these reports were translated into legislation, such as Basel II, Sarbanes Oxley (Sox) and a wide diversity of national and EU codes.

The Sarbanes Oxley Act, put into place in 2002 by US Congress, mainly requires the organization to include an evaluation of the internal control system, particularly regarding financial accounting, in the annual report. It is purely US legislation and as such solely applies to public companies in the US. However, it in fact has a global impact, as US companies need to adhere to this act for all their operations. This means they have to be certain, and be able to prove, that any business processes they outsource to other providers are also consistent with their corporate standards.

As such, we are seeing a lot of European and Asian service providers trying to understand Sarbanes Oxley and the requirements it put forwards[26]. While they do not officially certify, they make sure that they can provide a consistent process in which they deliver service. For many US clients, this has become a prerequisite prior to even considering doing business with a provider[27].

Sarbanes Oxley has a number of key requirements which I will detail briefly below[28]:

26 Dominic BARTON, Paul COOMBES, and Simon CHIU-YIN WONG for the Mckinsey Quarterly 2004 number 2, "Asia's Governance Challenge"
27 Gilbert VAN FRAEYENHOVEN (Ernst & Young), "Infosec in a Sox 404 context", ISSA, 2004
28 PriceWaterhousecoopers, "Sarbanes-Oxley Act of 2002: Strategies for Meeting New Internal Control Reporting Challenges"

- The organization needs to have an audit committee which oversees any external audit firm, is independent, and has a specified procedure to handle complaints.
- The CEO/CFO needs to certify accuracy and completeness of quarterly reports, as well as nature and effectiveness of disclosure controls and procedures supporting the quality of information in such reports.
- Management needs to release an annual report regarding the effectiveness of internal control over financial reporting, and an attestation by the company's auditors as to the accuracy of management's assessment.
- All periodic reports with financial statements need to be accompanied by a two item CEO and CFO certification indicating that the report fairly presents the issuer's financial condition and results of operations.

As you can see, Sarbanes Oxley effectively places end responsibility for complete operations with the CEO and CFO. The interesting thing of Sarbanes Oxley for forensic investigators is that it makes life much easier. Due to the fact that increased pressure rests on the CEO and CFO's shoulders to provide a fraudless service, they themselves are now the requesting party to have systems and procedures in place to quickly discover fraud and other items of interest.

An example commonly cited in US press was Universal Health Services, a US organization which operates in hospitals providing supporting healthcare services. Due to Sarbanes Oxley, this organization implemented additional fraud detection systems[29]. While these systems are put in place to identify potential fraud and as such safeguard the organization and CEO/CFO from prosecution should issues occur, their output can also assist forensic investigators. By easily identifying fraudulent transactions, forensic investigators can save time should they be called in. Information that required significant law enforcement experience in the past can now often be gathered

[29] ComputerWorld Magazine, "Sarbanes Oxley sparks forensic apps Interest", March 29, 2004

in an automated way – assisting those same forensic investigators to start the more demanding work earlier.

An additional legislation put into effect in the US is the Gramm-Leach-Bliley act. This act predates Sarbanes-Oxley by three years, applies to all companies that provide financial products or services and was implemented to ensure three items[30]:

- Ensure security and confidentiality of customer's personal information
- Protect against anticipated threats or hazards to such records
- Protect against unauthorized access to or use of customer information that could result in harm or inconvenience to the customer

Gramm-Leach-Bliley consists of three parts: the *financial privacy rule*, the *safeguards rule* and *additional pretexting provisions*. The financial privacy rule requires companies to provide privacy notices and explain their information collection and sharing practices. The safeguards rule requires them to have a security plan in place to protect the confidentiality and integrity of personal consumer information. The pretexting provisions prohibit so-called "pretexting", being the use of false pretences to obtain customer financial information such as bank balances.

While Gramm-Leach-Bliley is in fact corporate governance legislation, as it requires organizations to take certain action in the way it does business (the way it governs its operations), it is often considered as the US root for information security and assurance. This is mainly since virtually all financial organizations use IT systems to process financial information. The safeguards rule requires them to take action and protect this information. In order to prove that these measures exist, information needs to be available that shows them in action. This directly generates more information on the way information is accessed, thereby aiding any future forensic investigations within the organization.

[30] Marijke DE SOETE, Security4biz, "Corporate Security Governance", lecture on June 10th, 2005

Coming back to the Belgo-European context, the European counterpart of Gramm-Leach-Bliley is the Basel II accord. The Basel II accord is a regulatory edict that will take force on December 31st, 2006 which standardizes the way financial services firms' measure risk. It was published by the Basel Committee on Banking Supervision. Basel II consists of a number of documents, of which the first ones date back to July 1989, which are intended to promote safety and soundness in the financial system.

Basel II will mainly force financial organizations within Europe to comply with certain standards in risk management. It not only encompasses information technology infrastructure, but also risk induced by e.g. the departure of key personnel, such as a CFO/CTO.

The net result of Basel II will be that most financial organizations will have historical information and trending available on threats that may impact the business[31]. While this information will be confidential to the organization, it will prove useful both for the organization as well as law enforcement, should issues occur which require a legal investigation.

Within Belgium itself, corporate governance is mainly covered by the Code Lippens, which was introduced in June 2004[32]. These codes forces organizations to either comply with the standards described, or clearly explain why the organization did not comply. It also enforces duplicate monitoring: internally by the board of directors and major shareholders; externally by the minority shareholders and external supervisors, such as a statutory auditor.

[31] Charles A. ANDREWS, PriceWaterHouseCoopers, "Implementing the new Basel Accord", 2001
[32] Belgische Corporate Governance Code, from www.corporategovernancecommittee.be

4. Standards in Information Assurance

Information assurance regulation was born out of a different concern regarding the way organizations were run. While corporate governance wants to assure that an organization is run in a competent and acceptable way, Information Assurance wants to make sure the information flows within a company are confidential; their integrity is safeguarded and available.

As such, it is normal that separate standards were developed to this end. Perhaps the most known is the BS7799, better known as the British Standard. Another one pertaining mainly to financial organizations is written by the ECBS, short for European Committee for Banking Standards.

The BS7799 standard was written by the UK Department of Trade and Industry (DTI). This organization had a department called the CCSC, Commercial Computer Security Centre. This group had as one of its goals, by foundation, to develop security evaluation criteria. In the early 80's they developed the ITSEC scheme, a collection of documents that described how information technology (EDP; Electronic Data Processing) devices should operate from a security point of view.

Together with a wide variety of EDP consumers, they developed the British Standard BS7799. This document was published in 1989, and described best practices in Information Security management. In 1999, the document was submitted to the International Standards Organization (ISO). In 2000, BS7799 was officially published as ISO standard 17799. An amendment, BS7799 part 2 was published in 2002.

Part 1, dubbed "the code of practice for information security management" described a total of 127 controls in 10 areas, which detail actions an organization should take to safeguard security. These controls are, in the contrary to corporate governance guidance, usually very strictly defined. An example: "*Storage devices containing sensitive information should be*

physically destroyed or security overwritten rather than using the standard delete function".

Part 2 describes an actual Information Security Management System. It describes how controls should be implemented, the types of policies an organization should enact and further procedures regarding e.g. document management.

Organisations can have themselves certified against BS7799 by a number of different organizations which need to be licensed by the UKAS (United Kingdom Accreditation Service). Nevertheless, the standard is considered to be global and widely deployed in the Americas, Europe and increasingly in Asia[33]. It is also continuously updated, and an updated version was released in June 2005, ISO 17799:2005 which included newer controls which were not very popular when the previous version was enacted, such as vulnerability management.

BS7799 is a very popular standard which is considered as best practices in the field of information assurance. Besides this standard, there are also a number of guidelines which are published by a diversity of organizations and aim to assist companies with deploying information security. These usually provide assistance on more technical matters, and go more in depth in these fields than BS7799. While BS7799 enforces that encryption should be used to store sensitive data, these guidelines may specify which encryption algorithms should be preferred to provide this encryption.

For the purpose of this paper, Information Assurance has a lesser impact on forensic investigations than Corporate Governance. Information Assurance in most cases was born from an increased awareness of the importance information has within an organization. As such, it is likely to have a positive influence on the act of information gathering during a forensic investigation.

[33] Dominic BARTON, Paul COOMBES, and Simon CHIU-YIN WONG, "Asia's Governance Challenge", published in The Mckinsey Quarterly, 2004 number 2

One side-effect of Information Assurance is that information may be stored in encrypted form using a number of technologies which can also be used to hide information from law enforcement. As a result, in case an "encryption key", used to encipher data and as such make it unreadable to the average passer-by, is lost – which degree of importance will be given to such matter? Will an organization be liable for the loss of their key, even if they can show this was done by accident? If so, how would we define an "accident" in such case? In the US, some progress has been made in defining laws that pertain to encryption. In addition, a number of Supreme Court decisions have already formed a base for local courts to correctly judge in these matters[34].

In Belgium, legislation to this end is still lacking, and not clearly included in the computer crime law made available in 2000. While I do not directly endorse the types of law the United States has put in place, this is an especially important field that Belgian legislation should make progress in if it wishes to be able to successfully prosecute future white-collar crime, as this type of investigation tends to relate for a great deal to information transfers. If these transfers are encrypted, and keys are not timely provided, there may be little grounds to enforce further investigative actions.

[34] Conclusion based on a number of Supreme Court of the United States decisions regarding key escrow, such as Charles F. Woodbury vs United States of America; as well as the DMCA

5. Forensic investigations in a corporate context

It is easy to see where white-collar forensic investigations both require the integration of information assurance, as well as can be hampered by the implementation of information assurance within the organizations themselves.

More and more, jury and judge also expect guidance from experts on best practices. In March 2002, Arthur Andersen LLP, one of the big 5 auditing companies worldwide, was convicted for destruction of evidence in the bankruptcy investigation of Enron, once the largest Energy organization worldwide by revenue[35]. The indiction took place on violation of 18 U.S.C. §1512(b), which specifies as a crime to "knowingly us[e] intimidation or physical force, threate[n], or corruptly persuad[e] another person . . . with intent to . . . cause" that person to "withhold" documents from, or "alter" documents for use in, an "official proceeding.[36]"

The jury considered Andersen to have persuaded its employees to prevent documents from being used in government proceedings, while a SEC investigation was forthcoming. This judgement was later on confirmed by the court of appeals.

Andersen however, always maintained that it employed its regular document retention policy. Document retention policies are implemented in most organizations to safeguard client information, and are thus often considered to be part of an information assurance policy. The underlying philosophy is that client information which is no longer required for the ongoing client/provider relationship should be deleted. This protects it from being released by accident during a potential security breach.

In 2005, the United States Supreme Court unanimously shred the decision made earlier by a public jury[37]. This did not stop from Arthur Andersen being

[35] US Securities and Exchange Commission, "SEC Statement Regarding Andersen Case Conviction"
[36] Kristen HAYS, Associated Press, "Andersen convicted of obstruction"
[37] Arthur Andersen vs. United States, SUPREME COURT OF THE UNITED STATES, May 31, 2005

reduced from 85,000 employees in 2001 to little more than 200 in 2005, thereby effectively shedding virtually all of the companies' business unites. The original judgement had had a much larger social impact than the 5000 jobs that were lost at Enron itself.

The above example clearly shows the responsibility resting on the shoulders of both organizations and government investigators/experts in judging this type of case. The specific issue of document retention has now been tackled using the Sarbanes Oxley act, part of the standard corporate governance package under discussion in many boardrooms at this time[38].

[38] Duane Morris LLP, Press release, "Reversal of Arthur Andersen conviction highlights new Sarbanes-Oxley Witness-Tampering Provisions", August 4th, 2005

6. Conclusion

Introduction of new legislation, such as Sarbanes Oxley, Gramm-Leach-Bliley and Basel II has seen a further increase in detailed with which companies describe their internal processes, and monitor potential internal fraud. This can only assist governments in keeping closer watch on potential white collar crime within their constituency. We have also seen that due to the new processes that are being implemented in these companies, more information has become available to the forensic investigator.

Nevertheless, the hard work remains. While it becomes easier to identify the root of a fraud case, locating the exact scope, gathering the correct information and obtaining the necessary information from interrogations has not become any simpler. If anything, it may even have become more complex due to the fact that additional legislation generally does not simplify the way a business is being run.

In addition, we also had a look at the way information is gathered during a multidisciplinary investigation, and how additional specialization among experts has lead to a significant increase in the amount of experts generally working on a single case. This size increase of the investigate teams has stimulated the development of additional, new ways of working together, such as information databases. It has also lead to a new risk of contamination of evidence – it becomes very difficult to trust everyone on the team. In order to resolve these issues, will the government start to look at implementing information assurance and corporate governance to manage its own processes? This is a rhetorical question, but it seems some form of it is already being replicated back from industry to government.

Appendix A: List of references

Credits are given throughout the text in footnotes where specific information was used in a paragraph. The following resources were useful throughout the compilation of this essay. While information from them may not be literally mentioned, they are the true sources of inspiration:

Wim Van de Voorde, Johan Goethals en Mieke Nieuwdorp (2003), "Multidisciplinair forensisch onderzoek: juridische en wetenschappelijke aspecten", Politeia

Brent Turvey (2002), "Criminal Profiling: An introduction to behavioral evidence analysis", Academic Press

Maguire, Morgan, Reiner (2002), "The Oxford Handbook of Criminology", Oxford University Press

H. Den Boer (1999), "Business Control en Auditing", Academic Service

Various issues of The McKinsey Quarterly pertaining to Corporate Governance, McKinsey & Co, 2004-2005

Various white papers from audit firms PriceWaterHouseCoopers, KPMG, Ernst & Young and Deloitte and Touche Tohmatsu