BUSINESS CRIME PREVENTION IN EUROPE

Implementing an Early Warning Strategy

FALCONE 2001

With financial support from the FALCONE Programme

European Commission

Co-financed by Pirelli S.p.a.

Ernesto U. Savona
Mara Mignone
Leonardo Dal Negro

TRANSCRIME

IN COOPERATION WITH:
PIRELLI S.P.A
(MILAN, ITALY)

ISMA-INTERNATIONAL SECURITY MANAGEMENT ASSOCIATION
(BUFFALO, U.S.A.)

EUROPOL
(THE HAGUE, THE NETHERLANDS)

UNIVERSITÀ DEGLI STUDI DI TRENTO

UNIVERSITÀ CATTOLICA DEL SACRO CUORE

BUSINESS CRIME PREVENTION IN EUROPE

IMPLEMENTING AN EARLY WARNING STRATEGY

FINAL REPORT

EXECUTED BY

TRANSCRIME

IN COOPERATION WITH

PIRELLI S.P.A. (MILAN, ITALY)

AND

ISMA – INTERNATIONAL SECURITY MANAGEMENT ASSOCIATION (BUFFALO, U.S.A.)

AND

EUROPOL (THE HAGUE, THE NETHERLANDS)

FOR THE

EUROPEAN COMMISSION

WITH FINANCIAL SUPPORT FROM THE 2001 FALCONE PROGRAMME
EUROPEAN COMMISSION (CONTRACT JAI/2001/FALCONE/114)
CO-FINANCED BY PIRELLI S.P.A.

Università degli Studi di Trento

August 2002

Transcrime Reports n.4

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The BUSINESS CRIME PREVENTION: IMPLEMENTING AN EARLY WARNING STRATEGY Project is the result of co-operation among various public and private institutions: Transcrime – University of Trento (Italy), which co-ordinated the study, Pirelli S.p.A., which also co-financed the research, the International Security Management Association (ISMA), and Europol. The research project has been directed by Ernesto U. Savona, Professor of Criminology and Director of Transcrime – University of Trento and co-ordinated by Mara Mignone, researcher at Transcrime – University of Trento, with the assistance of Leonardo dal Negro, research assistant at Transcrime – University of Trento.

This Final Report has been written by Ernesto Savona and Mara Mignone, with the assistance of Leonardo dal Negro.

We gratefully acknowledge the valuable assistance provided by the partners in the project who followed and participated in every stage of the research.

We wish to thank the following persons in particular:

Pirelli S.p.A

- Giuliano Tavaroli
- Silvia Vanini
- Alessandra Cerreta

International Security Management Association (ISMA)

- David Burrill
- Susan Pohlmann
- Jane Watts

European Round Table of Industrialists (ERT)

- Joanna Rau
- Wim Philippa

Europol:

- Rolf Hegel
- Europol analysts

European Commission:

- Jonathan Sweet
- Martin Power

All the companies and their representatives who have kindly accepted to participate in our survey. In order to respect the confidentiality clause and not to make them recognizable, they will not be nominated.

EXECUTIVE SUMMARY

This Final Report presents the results of the BUSINESS CRIME PREVENTION IN EUROPE: IMPLEMENTING AN EARLY WARNING STRATEGY Research Project awarded by the European Commission under the EU Falcone Programme (Contract JAI/2001/FALCONE/114) and carried out by Transcrime, Research Centre on Transantional Crime of the University of Trento (Italy), together with Pirelli S.p.A., the International Security Management Association (ISMA), and Europol. Pirelli S.p.A. has co-financed the Project.

This Final Report is supplementary to the Intermediate Report delivered in April 2002. Given that the two Reports focus on different issues, for the sake of completeness the most important findings of the Intermediate Report have been partly reproduced in what follows.

The aim of the FALCONE 2001 - BUSINESS SECURITY research project is to develop and propose a strategy to prevent the infiltration of the legitimate private sector by crime. It deals in particular with the penetration of that sector by organised crime and the growth of occupational crimes against businesses. The project is based on the idea that statistical analysis of recurrent criminal episodes against companies is able to identify early warning signs which will alert security managers when a specific area of their company is under threat of organised and/or occupational crimes. Crucial for the development and implementation of this methodology, and to achieve concrete and applicable results, is relevant information. Indeed, the availability and management of accurate and detailed information and data provide the keys to *knowing*, *understanding*, *reducing*, and above all *preventing* a variety of serious criminal threats and dangers to business.

A correct, scientific-based approach to business security management is of fundamental importance for both the public and the private sectors. In fact, the consequences of crimes against businesses cannot be underestimated, for they wreak great damage not only on the companies targeted but also on the regular activities of the lawful market in its entirety.

As regards companies, while on the one hand they are vulnerable to petty crimes, pilfering and minor embezzlement, on the other, they are exposed to frauds, attacks against computer systems, and thefts of sensitive proprietary information. They are confronted by a challenge of great complexity, for the use of new technologies means that internal and external attacks grow increasingly sophisticated. At the moment, the private sector is an area in which offenders can readily maximise the proceeds from crime, especially when the target are intangible assets; it is also an area where there is less likelihood of law enforcement. Public institutions, in fact, still tend to consider companies only as 'criminals', that is the perpetrators of the so-called 'corporate crimes'.

The point is that public sector cannot leave companies to cope on their own with crimes that also threaten community safety and economic development. Public authorities and law enforcement agencies must for their part recognize that only if the public and the private sectors co-operate will tangible and consistent results in terms of crime control and prevention be achieved.

Starting from these premises, the intention of the FALCONE 2001 – BUSINESS SECURITY is to increase the knowledge of the business crime related issues, and to do so mainly by:

- collecting and organizing information with which to qualify and quantify crimes against businesses, in an endeavour to improve knowledge of the phenomenon and to formulate definitions of key concepts;
- developing an experimental method for business crime prevention and business security management based on the so-called 'early warning signs approach';
- developing a multidisciplinary network of information by means of a website, the purpose being to create a database of useful data, information, best practices, literature and references, and also to provide a virtual meeting forum that is freely accessible to private and public subjects, practitioners, law enforcement authorities, professionals and academics. It is generally recognised, in fact, that keeping best practices and information secret, while competing rather than co-operating, are not the most productive methods in business. Only full co-operation among private subjects, with the assistance of the public authorities, will minimise the economic and social costs of crime.

The development of the first two specific objectives is the principal theme of this Report.

In order to respond to the need of deeper knowledge, Part I of the Report consists in a general overview about business security and business crimes; in particular, it opens with working definitions of the most relevant key concepts, then focusing on a quantitative and qualitative analysis of the business and occupational crimes targeting European companies. The so-called *cyber-menace* is considered with particular attention. The main findings of this analysis are as follows:

- precise data on crimes against businesses are extremely difficult to obtain and statistics describe only the tip of the iceberg. The main result of this situation is that it is impossible to provide a complete picture of the criminal risks and dynamics affecting the private sector;
- the private sector has always been rather reluctant to furnish information about its experiences and/or vulnerabilities. Fortunately, it seems that this situation is changing: the majority of companies now realize that their co-operation is essential;
- according to the data and information collected, the conclusion is that businesses are vulnerable to crime: 42,5% of the larger European companies questioned, in fact, had been victim of fraud in the previous two years. The average cost to them of fraud was €6,7 million. No industry sector is spared and 60% of frauds are committed by people within the organization. The problem is that, as regards detection, accident and/or chance are still determinant and companies seem not to learn from their past troubles: they do not make changes or introduce new measures to improve their risk management procedures;
- companies seem to underestimate occupational crime. Although embezzlement and breach of trust are extremely common, companies seem to be entirely unaware of their real incidence;
- with regard to future trend, computer crimes require particular attention: they are on the increase and they are common to all business sector, even to companies which are essentially routine-based. As regards the perpetrators, at one extreme of an increasing scale of potential hazard are teenagers with their

home computers and modems, while at the other are ultra-dangerous and high-skilled criminals who break into public and private networks for various purposes. There is also growing concern about attacks perpetrated by organised offenders; some examples are: hacking groups, activists and terrorists. Also traditional organised crime seems to be involved in cyber-attacks. The ICT revolution is raising new challenges for the way in which business security is administered.

Part II of the Report presents the findings of the survey conducted. One of the main objectives of the FALCONE 2001 - BUSINESS SECURITY, in fact, was to conduct a victimisation survey in the business sector. In the intention of the research design, achievement of this goal should have yielded a twofold result: on the one hand, it should have improved knowledge of the most frequent and serious business crimes, while creating an information database which should have enabled the sharing of information among the interested subjects; on the other, it should have contributed to the academic research on business security issues by developing a model for assessment of the risk of criminal infiltration of business and occupational crimes.

The project encountered some problems in its implementation and changes had to be made to both the research design and the methodology. Notwithstanding the efforts of Transcrime – University of Trento, International Security Management Association (ISMA) and European Round Table of Industrialists (ERT), the final result of the questionnaire administration procedure was disappointing. Only ten questionnaires were returned. This marked and unexpected lack of participation together with the willing to profit from the information collected made the adoption of a case-study methodology approach necessary.

On this base, the main objective was to understand individual cases in and of themselves, with no other theoretical inference or empirical generalization being drawn. The main aim of the case-study analysis was to use the information collected by the questionnaire to determine how the companies interviewed manage security related issues. Therefore, technically speaking this study is not a victimization survey, but rather a pilot study. However, in profiting from this experience, and especially of from the study's findings, it could be followed by further research in the near future.

From the theoretical point of view, it is necessary to specify that the research is based on a model – what can be called the 'risk-model' – around which the questionnaire was designed in its entirety. The model is as follows:

$R=f(G,F,S)$

the probability (R) that a company may be a victim of a crime is hypothesised as being:

- strictly dependent on the *quantity* and *quality* of ASSETS potentially at risk (G)
- proportional to the MEANS and OPPORTUNITIES available to employees and criminals to commit and/or participate in the crime (F)
- inversely proportional to the MEASURES taken to protect the company's assets (S)

Once the questionnaire had been collected, it was clear that the model could not be properly tested with so little information. Nevertheless, the cases were analysed with particular attention to all the information and data that shed light on:

- *assets*: is there a relationship between the assets affected by crimes and the types of crimes?
- *means* and *opportunities*: who were the offenders, what means they use, and what opportunities they exploit?
- *preventive* and *repressive measures* adopted by the company interviewed: did the company manage security in an appropriate manner?

The case-study analysis was also supported and completed by a literature analysis, developing the most important issues.

Stated that almost all the companies experienced crime in the previous two years, the main results are as follows:

assets: almost all the assets individuated in the questionnaire (production line and products, human resources, Information Technologies, know-how and capitals) are targeted by criminals. In particular, as regards ICT one of the feature that emerge from the case-study analysis is the widespread nature of these crime and infringements. Traditional laptop thefts, together with the web site home page defacement and Denial of service seem to be the most recurring offences;

damage: companies seem not to be fully aware of the real damage provoked by crimes; moreover, although the workplace climate is extremely important, little attention is paid to employees' reaction to criminal episodes affecting the company for which they work;

perpetrators: the results on this point are entirely unsatisfactory and not always convincing. They reveal that companies have only imprecise and vague knowledge about the subjective profile of the criminals who targeted them. With regard to insiders, almost all companies indicated 'employee' as the most recurrent profile. This result seemingly confirms the general rule that crimes committed by high-status employees are extremely difficult to detect, although this does not mean that they are less numerous than those committed by employees. *Profit* is cited as the most frequent reason for the commission of crimes and abuses against the company. As regards organised crime, on the contrary, the case-study analysis does not evidence that criminal groups are highly involved in business crimes;

means and opportunities: according to the questionnaires, one of the factors with the greatest impact on the occurrence of the crimes experienced was management responsibilities (*management override on internal controls* and *lack of managerial control over outsourced services* were among the reasons most frequently cited). From a theoretical perspective, the case-study analysis matches the assumptions of so-called opportunity theories. Employees – the personal attitude towards crime notwithstanding – have opportunities for crime provided by the organizational environment in which they work. They will thus exploit and make use of them to commit every kind of occupational crime;

security measures: this issue, together with *managers' perception of security*, is analysed in detail in Part II of the Report. It is important to highlight that, according to the information collected, the companies interviewed should be absolutely secure, given that they had already implemented almost all the security measures

indicated in the questionnaire. The problem is that these measures are not generally supported by an effective control activity, especially on the part of management. The conclusion is that security is still managed in a superficial way: just to make an example, not all the companies have a department specialised in security problems and a database of information on crimes experienced. Early warning strategies and corporate governance measures are not given particular consideration: it seems that companies still prefer traditional security measures and there is a general lack of concern for, and a lack of direct controls over, internal human resources. In other words, business security management still provide opportunities for crime. These conclusions are confirmed also by the answers given by the managers interviewed and based on their personal experience and perception.

Part III of the Report focuses on the possible use of early warning strategies in the private sector; a part from some exceptions, however, their application in the business environment is still at the beginning. However, early warnings are used in other context, for different purposes. In order to clarify their relevance and to point out their utility and value, this Part is enriched also with a general overview of the most important experiments to date and their results. This Part ends with an analysis of the early warning applications in order to prevent workplace violence and employee theft.

Finally, the last section of the Report is a concluding discussion on the research findings, the aim being to propose a new approach to business security at both theoretical and practical level. The research conducted to compile the FALCONE 2001 – BUSINESS SECURITY Study has led to the conclusion that a critical shortcoming is the lack of common definitions and scientific studies in the field of business security; it seemed thus important to develop a model which could schematise the main components of criminal threats to the private sector was developed: the result is a general and flexible model which can be called the *Business Security Incident* (BSI). It has been constructed laying no claim that it is a definitive, exhaustive and ultimate scheme; on the contrary, its value consists in the fact that it can be continually updated as and when information and data become available.

INTRODUCTION

This Final Report presents the results of the BUSINESS CRIME PREVENTION IN EUROPE: IMPLEMENTING AN EARLY WARNING STRATEGY Research Project awarded by the European Commission under the EU 2001 Falcone Programme (Contract JAI/2001/FALCONE/114) and carried out by TRANSCRIME, Research Centre on Transnational Crime of the University of Trento (Italy), together with Pirelli S.p.A., the International Security Management Association (ISMA), and Europol. Pirelli S.p.A. has co-financed the Project.

This Final Report is supplementary to the Intermediate Report delivered in April 2002. Given that the two Reports focus on different issues, so that this Final Report is as complete as possible the most important findings of the Intermediate Report have been partly reproduced in what follows.

The research project has been directed by Transcrime – University of Trento and it has benefited from the expertise of the partners to the project who form the Steering Committee, the members of which are G. Tavaroli, S. Vanini, A. Cerreta (Pirelli S.p.A.), E. U. Savona, M. Mignone, (Transcrime – University of Trento), J. Sweet (European Commission), R. Hegel (Europol), and D. Burrill (ISMA).

The aim of the FALCONE 2001 – BUSINESS SECURITY research project is to develop and propose a strategy to prevent the infiltration of the legitimate private sector by crime. It deals in particular with the penetration of that sector by organised crime and the growth of occupational crimes against businesses. The project is based on the idea that statistical analysis of recurrent criminal episodes against companies is able to identify early warning signs which will alert security managers when a specific area of their company is under threat of organised and/or occupational crimes. Crucial for the development and implementation of this methodology, and to achieve concrete and applicable results, is relevant information. Indeed, the availability and management of accurate and detailed information and data provide the keys to *knowing*, *understanding*, *reducing*, and above all *preventing* a variety of serious criminal threats and dangers to business.

A correct, scientific-based approach to business security management is of fundamental importance for both the public and the private sectors. The consequences of crimes against businesses cannot be underestimated, for they wreak great damage not only on the companies targeted but also on the regular activities of the lawful market in its entirety. In an economic system which requires companies to be constantly efficient, flexible and competitive, criminal risks are dangerous impediments that the business sector must necessarily remove. Likewise, the public sector cannot leave companies to cope on their own with crimes that also threaten community safety and economic development.

It is evidently of extreme importance that senior managements should be made more sensitive to security issues. They must understand that underestimating the magnitude of the problem may undermine the effectiveness of any form of crime prevention. And they must in particular be made aware that they are confronted by a challenge of great complexity, for the use of new technologies means that internal and external attacks grow increasingly sophisticated; while on the one hand

their companies are vulnerable to pilfering and minor embezzlement, on the other, they are exposed to frauds, attacks against computer systems, and thefts of sensitive proprietary information. Public authorities and law enforcement agencies must for their part recognize that they have a crucial role to perform, and above all that only if the public and the private sectors co-operate will tangible and consistent results in terms of crime control and prevention be achieved.

The rapidly changing nature and the increasing dangerousness of business crimes are focusing increasingly closer attention on the problem in both the public and private sectors. The European Union has recently recognised the important role of the private sector in the fight against organised crime, emphasising that certain obstacles against it must be removed as rapidly as possible. In fact, the business sector is well known to be an area in which offenders can readily maximise the proceeds from crime, especially when the targets are intangible assets; and it is also an area in which there is less likelihood of law enforcement. Moreover, companies have less awareness of crime due to their lack of experience in dealing with the phenomenon, and also because of a lack of information and best practices in crime prevention. A further problem is the fear that a company's reputation and image may be damaged by its involvement in a crime.

In order to break this vicious circle, various European institutions have already recognised the need for closer involvement of the public sector in the prevention of business crime; and they have also emphasised that the private sector must be more actively involved in the fight against organised crime. This has given rise to a number of important initiatives.[1]

---

[1] The programme adopted by the European Council on 27 March 2000 entitled *Prevention and Control of Organised Crime: a Strategy of the European Union for the Next Millennium* emphasised that "(...) *the business community and other sectors of society should be encouraged to develop partnerships between them and with the authorities in preventing and controlling organised crime*".

In a Communication to the Council and European Parliament proposing a Council Decision for "*establishing a programme of incentives and exchanges, training and cooperation for the prevention of crime, (Hippocrates)*" – dated 29 November 2000 – "*the Commission envisaged the development of initiatives such as the round table of European Industrialists on questions of security and crime prevention* (...)"

The 2001 Falcone programme has itself promoted the "*multidisciplinary analysis of the risk and impact of certain forms of transnational economic crime...*" recommending that such analysis should also concern itself with the "*development of techniques used both by public authorities and by businesses in order respectively to combat and to prevent economic crime*".

The Strategy for the new Millennium and other European initiatives have stressed that organised crime shifts its activities to where opportunities for economic gain are greater and the law enforcement risk is lower. Preventive measures should therefore seek to ensure that "*committing a crime is made more difficult, that offending involves greater risks to the offender and that the possible benefits to the criminal of committing the crime are reduced or eliminated*".

Of particular importance is the EU Forum on Organised Crime Prevention, the first of whose sessions was held in May 2001. One of its permanent workshops deals with the role of the private sector in the prevention of crime, analysed from an European perspective. As emphasised by the Commission itself, the aim of the initiative is to create a global framework within which various actors can develop dialogue on the prevention of organised and economic crime. This would encourage the European networking and partnerships indispensable for the creation of concrete prevention projects. To be stressed is that the Commission "*considers that sensitisation of the private sector and its co-operation with the public authorities are central elements of any global crime prevention strategy*". (European Commission, Directorate General "Justice and Home Affairs", *First meeting of the EU Forum on the prevention of organised crime*. "Discussion paper on the role of the private sector in the prevention of crime – a European perspective", 17-18 May 2001). Moreover, one of the principal objectives of this initiative is to create a

In acknowledgment of these initial efforts by both the public and the private sectors, the intention of the FALCONE 2001 – BUSINESS SECURITY Study is to increase knowledge of the problem, and to do so mainly by:

- collecting and organizing information with which to qualify and quantify crimes against businesses, in an endeavour to improve knowledge of the phenomenon and to formulate definitions of key concepts;
- developing an experimental method for business crime prevention and business security management based on the so-called 'early warning signs approach';
- developing a multidisciplinary network of information by means of a website, the purpose being to create a database of useful data, information, best practices, literature and references, and also to provide a virtual meeting forum that is freely accessible to private and public subjects, practitioners, law enforcement authorities, professionals and academics. It is generally recognised, in fact, that keeping best practices and information secret, while competing rather than co-operating, are not the most productive methods in business. Only full co-operation among private subjects, with the assistance of the public authorities, will minimise the economic and social costs of crime.

The singling out of these three specific objectives – and consequently the organisation of the FALCONE 2001 – BUSINESS SECURITY Project in its entirety – are the result of previous research intended to specify the problems raised by the current approach to business security related issues. This exploratory analysis showed that a lack of information, experience and best practices in the prevention of business crimes increases the vulnerability of businesses to criminal infiltration, and also neutralises the advantages of a preventive strategy and co-operation between the private and the public sectors. By contrast, the availability to management of accurate information on the security of a company greatly influences the effectiveness of any crime prevention strategy. In fact, besides increasing economic and social costs and reducing the effectiveness of security functions, a shortage of information has further and more general harmful consequences. For example:

- it reduces awareness of this type of crime, restricting the problem and related costs to the level of a 'mere company's issue';
- it hinders the development of economies of scale in the gathering and handling of information;
- it limits the opportunities to devise and test new security management models within the company;

European partnership between the public and private sectors which will also involve third-countries *representatives, because of the international nature of the illegal economic activities undertaken by organised crime.*

The private sector, too, has set up voluntary initiatives: for example, it is co-operating in the drafting of codes of conduct, especially as regards corruption and specific types of fraud. Other initiatives are under way in the fields of labour relations, environmental management, consumer protection, as well as others. Efforts have recently been made to harmonize management, reporting and auditing standards. In addition, various projects are in progress for the implementation of these measures and the devising of follow-up mechanisms.

Also to be emphasised is that businesses are seeking to develop a common culture in the prevention of crime and risk-management. They also take active part in the organization of partnership initiatives, the most important of which involve the development of exchange of information systems, joint training programmes, and joint awareness-raising campaigns.

- it reduces opportunities for co-operation between the public and the private sectors in their fight against crime.

All these issues will be analysed in the course of this Report.

Before entering into detail, we would stress that, as briefly explained in this Introduction, the Study explores a relatively new area of research. Therefore, and also with regard to its results and findings, this FALCONE 2001 - BUSINESS SECURITY Final Report should be treated as a pilot study intended to prepare the way for productive dialogue between the public and private sectors, providing useful information and its scientific analysis. It will certainly be followed up and integrated by further studies and research; for, as said, the collection and the retrieval of information on business security is fundamental for the implementation of effective strategies to combat crime.

As specifically regards the early warning signs method proposed, this may be used for data collection and analysis, as well as for the devising and implementation of preventive measures in all European Union based companies. In fact, implementation of the method in different settings would give greater homogeneity to the data and information obtained, and it would create a valuable common basis for co-operation between the public and private sectors.

The Report is organised as follows:

- Acknowledgements;
- Executive summary;
- Introduction;
- The research design: goals, tasks and methodology;
- Part I – Business security and business crime: general overview;
- Part II – The case-study analysis;
- Part III – Early warning signs and business security;
- Research implications.

THE RESEARCH DESIGN: GOALS, TASKS AND METHODOLOGY

According to the EU Falcone 2001 Programme guidelines, and in order to examine the most urgent business-security related issues, the FALCONE 2001 – BUSINESS SECURITY Study has been designed to achieve three main goals, and for each of these Goals, specific tasks and the related methodology have been also specified.

In order to clarify the research design structure, the Goals, the tasks and the methodology are set out below. The Goals are as follows:

Goal 1- Definition of key concepts in the field of business security which facilitate precise identification of the research object and interaction with the companies involved in the research project.

Goal 2 – The experimental development of a strategy for business crime prevention based on a survey of company victimisation which will enable the creation of a database of adequately classified information and able to single out recurrent criminogenic factors.

Goal 3 – The development of a Business Crime Prevention web-site. A virtual 'security workshop' will enable the classification and retrieval of information on business crimes and business security, the trialling and discussion of new prevention strategies, and the exchange of ideas arising from company security experiences.

Goal 1 was developed in the Intermediate Report; specifically, the analysis centred on the following tasks:

task 1) the different types of business crime, and specifically those which involve organised crime, were analysed in order to define common standards and a common methodology for identifying the phenomenon.

task 2) a detailed glossary of terms specific to business crime and business crime prevention was created.

Goal 2 is the principal theme of this Final Report, which focuses on the following tasks in particular:

task 4) analysis and classification of recorded and documented business crime;

task 5) development of a simplified theoretical model. The risk that a company may to be a victim of a crime is hypothesised to be:

strictly dependent on the amount and type of the company's assets potentially at risk;

proportional to the means and opportunities available to employees to commit the crime;

inversely proportional to the measures taken to protect the company's assets;

task 6) creation of specific questionnaires to be distributed to multinational companies in the following three stages:

a pilot survey of multinational companies with headquarters in Italy;

distribution of the questionnaires to a reduced sample of multinational companies with European headquarters;

distribution to a larger representative sample of multinational companies, preferably with headquarters in Europe;

task 7) statistical analysis of the relationship between past cases collected by the questionnaires and the anomalies detected will be conducted to highlight recurrent features as well as the presence of possible anomalies signalling, in advance, illicit phenomena;

task 8) criminological profiles will be drawn up to facilitate identification of the potential risks of criminal infiltration.

Part II of this Report will describe how these tasks were developed in detail, together with the methodology used and the findings.

The project set itself the following task as regards *Goal 3*:

task 9) the Business Crime Prevention web site will be organised as a virtual research centre. It will be divided horizontally according to the type of research area or service provided, and vertically according to the crime type concerned. The horizontal division will be made up of eight sectors with a central section, the Laboratory, which will classify and organise information for all the others. The Laboratory will be composed of an impartial committee consisting of experts from both the private and public sectors.

This task was discussed and partly changed by the Steering Committee during its first meeting held at Pirelli S.p.A. headquarters on 14 September 2001. As stated in the minutes of the meeting, the Steering Committee:

identified detailed design of the web site, i.e. the identification of its possible structure and main contents, as the first step. Subsequently, the project for the web site will be sent to the Members of the Steering Committee, for further comments and suggestions and to make a decision on how to proceed;

agreed that the web site will include the main results of the project (business crime legislation, case-study, etc.), although the questionnaire and the data collected from the survey will not be included;

agreed that the web site will be hosted by Transcrime's web site.

Trascrime – University of Trento is still working on the website. As indicated in the timescale for completion, it will be presented in October, at the end of the research project.

PART I – BUSINESS SECURITY AND BUSINESS CRIMES: GENERAL OVERVIEW

1. BUSINESS SECURITY, BUSINESS CRIME, OCCUPATIONAL AND ORGANISED CRIME: WORKING DEFINITIONS

'Business security', as well as 'business crimes' and 'occupational crimes', are not technical terms. In general, they are expressions used with reference to the legitimate private sector and its need for protection against criminal acts by a wide variety of subjects operating both within and without companies. Accordingly, 'business security' and 'business and occupational crimes' serve as generic labels for a variety of security-related issues.

As regards 'business security' in particular, if this term appears to be too general, and a more technical one is required, useful synonyms are 'private security', or also 'corporate security'.

A common meaning can be identified if one bears in mind that 'business security', 'private security' and 'corporate security' all have their primary duty to the employer corporation.[2] This means in concrete terms that the aim of business security is to protect and preserve people, assets, intellectual property and information technology within a company.[3] In other words, as the American Society for Industrial Security (ASIS) puts it, business security assesses and addresses the causes and effects of criminal activities upon an organization's employees, customers, physical and intangible assets, computer systems/information technology and intellectual property. That is to say, 'by definition, business security provides a process by which an organization identifies, assesses and selects treatment methodology for its security risk or security perils'.[4]

Of these various definitions, the definitive one may be that proposed by Fayol, who according to Williams et al., wrote that security activity has as its final objective, '(…) to safeguard property and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social disturbances and natural disturbances liable to endanger the process and even the life of the business. It is the master's eye, the watchdog of the one-man business, the police, or the army in the case of the state. It is, generally speaking, all measures conferring security upon the undertaking and requisite peace of mind upon the personnel'.[5]

For the purposes of this Report, therefore, the terms 'business security' and 'private/corporate security' will be used mainly as synonyms.

---

[2] Ferreira B. R., "Situational Crime Prevention and Displacement: The Implications for Business, Industrial and Private Security Management", in *Security Journal*, 6 (1995), p. 155-162.

[3] Zuckerman M. M., "Moving towards a Holistic Approach to Risk Management Education – Teaching Business Security Management", in *Security Journal*, 11 (1998), p. 81-89.

[4] Head G. L., *Essentials of Risk Control*, 3rd ed. (vol. II), Insurance Institute of America, Chapter 11, 1995.

[5] Williams C. A., Smith M. L., Young P. C., *Risk Management and Insurance*, 8th ed., McGraw-Hill Inc., 1998, p. 26-354.

Brief discussion is required of the terms 'business crimes' and 'occupational crimes'. It should first be noted that the term 'crime' will not be used here in its legal sense. Consequently, crime is not considered to be an intentional act committed in breach of criminal law but rather as a synonym for 'infringement', 'violation' or 'fraud'. The last of these terms is more technical but at the same time more general than 'crime': it denotes *any* behaviour by which one person gains, or plans to gain, a dishonest advantage over another. It is evident that not all frauds are crimes, and numerous crimes cannot be frauds.[6]

Nuances of meaning aside, the point is that it is necessary to go beyond legal definitions in order to obtain a complete description of the actions that may damage companies.

Therefore, if 'business crimes' are not considered from a legal perspective, they can be defined as 'all crime and disorder committed by or against businesses'[7]. This definition is extremely broad and it includes, for example, internal crimes (e.g. employee theft, fraud and false accounting), external crimes (e.g. burglary, customer theft and vandalism) and contraventions of legislation on, for example, trading standards or health and safety.

This Report focuses mostly on business crimes, understood as all crime and disorder committed *against* businesses; specifically, it deals with *occupational crimes* and infiltration by organised crime.

The former may be classified as all crime and disorder committed *against* businesses, *by employees, in the course of their work*.

To cite an authoritative source, the term occupational fraud (crime) can be defined finally as 'the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets'.[8]

This definition encompasses a wide range of forms of misconduct by employees, managers and executives. Schemes may be as simple as the pilfering of company supplies or as complex and sophisticated as financial statement frauds.

Notwithstanding the differences characterizing each case, they have four features in common: occupational crime and abuse

- are clandestine;
- violate the perpetrator's fiduciary duties to the victim organization;
- are mainly committed for the purpose of direct and indirect financial benefit to the perpetrators;
- cost the employing organization assets, revenues or reserves.

---

[6] Comer M. J., *Corporate Fraud*, Gower, Network Security Management LTD, 3rd ed., 1998.

[7] This definition is taken from the Crime Reduction web site at the following URL: http://www.crimereduction.gov.uk/toolkits/br020101.htm.

[8] ACFE, *2002 Report to the Nation on Occupational Fraud and Abuse*, 2002. The text is available at the following URL: http://www.acfe.org.

Finding a suitable definition for organised crime is a much more complex undertaking, given the polysemy of the term.[9] However, for the purpose of our research it seemed advisable to give it a broad definition such as the one used in the Joint Action of 21 December 1998 adopted by the Council of the European Union on the basis of Article K.3 of the Treaty on European Union. Article 1 of this Joint Action states:

'*…a criminal organisation shall mean a structured association, established over a period of time, of more than two persons, acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, whether such offences are an end in themselves or a means of obtaining material benefits and, where appropriate, of improperly influencing the operation of public authorities'.*

2. Measuring business and occupational crimes in Europe

Precise data on crimes against businesses are extremely difficult to obtain. There are many reasons why economic crimes remain undiscovered or why they are not reported when they are investigated. The main result of this situation is that it is impossible to provide a complete picture of the criminal risks and dynamics that affect the private sector. Technically speaking, business crimes – as well as economic crimes in general – have a high '*dark number*': that is to say, the number of crimes committed is greater than the number of the crimes reported. Statistics on business crimes describe only the tip of the iceberg, to use the hackneyed expression. Useful sources of information are the surveys and analyses undertaken by academic research groups and security companies/associations. Before entering into detail, it should be noted that the private sector has always been rather reluctant to furnish information about its experiences and/or vulnerabilities. Fortunately, the situation is changing: the majority of companies now realize that their co-operation is essential if best practices are to be developed, and knowledge about these criminal phenomenon improved, so that efficient and effective preventative measures can be put in place.

As regards the European context, PricewaterhouseCoopers has recently issued its European Economic Crime Survey 2001.[10]

This survey is an extremely important source of information about the situation in Europe, considering also that there are relatively few surveys and studies on the topic. Yet it reaches conclusions that are anything but positive: 'economic crime is a major business issue', the report states, given that 42.5% of the larger European

[9] For analysis of the various definitions of "organised crime", see Adamoli S., Di Nicola A., Savona E. U., Zoffi P., *Organised Crime around the World*, report prepared by Transcrime – University of Trento for HEUNI – United Nations, HEUNI Publication Series n. 31, Helsinki, 1998, p. 4-10; 132-142.

[10] PricewaterhouseCoopers interviewed senior representatives of more than 3,400 companies, non-profit organizations and government bodies in fifteen Western and Central European countries.

companies questioned had been victims of fraud in the previous two years, and that the average cost to them of fraud was €6.7 million.

As regards the perception of the victims, it is of interest that companies believe that the risk of fraud will be at least as high in the future as it is now, and one-third of them believe that it will be even higher. Computer crimes are reported as being the main concern.

The other main results of the survey were the following.

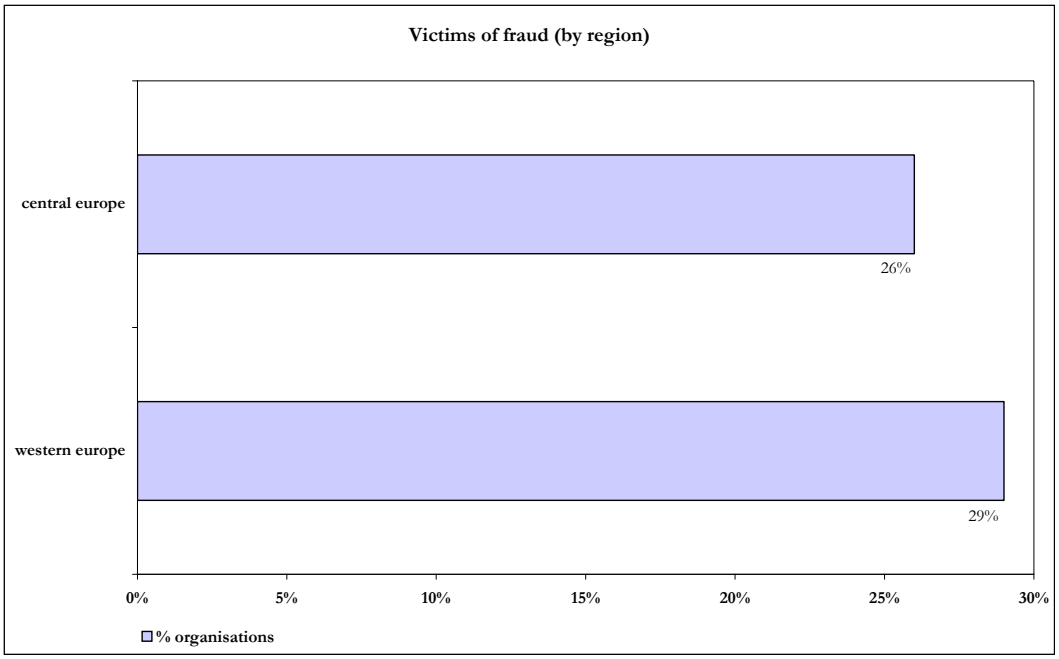
- around 60% of frauds are committed by people within the organization. However, this finding is not directly applicable to computer crimes, nor to both the European and the American contexts. Recent American surveys show that whereas about two years ago roughly 70% of malicious computer system attacks were made by insiders, the ratio has now reversed: around 70% of attacks are now committed by outsiders and only 30% by insiders. This tendency has not yet been confirmed in Europe, but a survey of UK IT managers[11] has suggested that employees are still the biggest security problem for most businesses;
- no industry sector is spared, but financial services seem to be particularly at risk;
- embezzlement (defined as the misappropriation of assets, monetary as well, by an employee) and breach of trust (misappropriation of assets or financial misrepresentation by management) are the most common types of fraud;
- according to respondents able to quantify the damage, the cost of fraud committed in the previous two years had been an estimated €3,6 billion, with an average cost – as said – of €6.7 million per organisation;
- apart from (direct and indirect) economic damage, the respondents indicated other 'collateral' damage caused by fraud and in particular, its detrimental impact on business relationships and staff morale;
- as regards detection, accident or chance seemingly played a significant role in 58% of frauds. Recoveries were infrequent: only 20% of the organizations had managed to recover more than 50% of their losses;
- as far as preventive and control measures were concerned, the companies seemed not to have learnt from their past difficulties. Fewer than half of them had made changes and/or introduced measures to improve their risk management procedures. Consequently, they are still vulnerable to fraud.

Fraud seems to target larger companies in particular. According to the survey, in fact, the threat increases as the size of the companies grows. 'The proportion of companies with over 5,000 employees that had suffered fraud [during the same period] was 42.5%'.

As for geographical location, it seems that Western European companies are more at risk than ones in Central Europe. Although the difference is only slight, this finding is important because Western European companies have always considered themselves to be 'safer' than their Central European counterparts.

[11] Leyden J., "Curious employees are the biggest security risk", The Register, 4h March 2002. The text is available at the following URL: http://www.theregister.co.uk/content/55/24282.html.

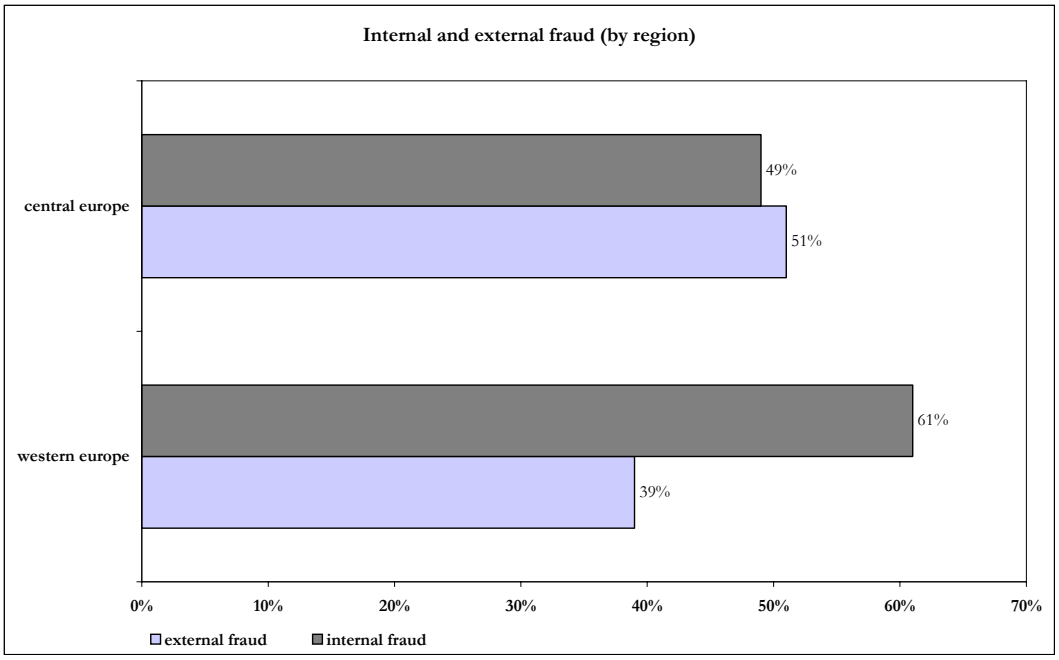
Figure 1



Source: PricewaterhouseCoopers, European Economic Crime Survey 2001

The profile of perpetrators is one of the most interesting aspects to emerge from the PricewaterhouseCoopers survey.

Figure 2



Source: PricewaterhouseCoopers, European Economic Crime Survey 2001

The survey shows that frauds committed by insiders (people within the company) are more frequent than those perpetrated by outsiders. It should be noted that the incidence of internal and external fraud differs according to the geographical region: organisations in Central Europe are at greater risk of fraud committed from outside the company, while Western European companies are mainly the victims of internal fraud. This situation points to the conclusion that corruption – as fraud which by definition involves third parties – is a fundamental component of the Central European economy.

Also of considerable interest in the PricewaterhouseCoopers survey is the section dealing with the economic crimes that should cause concern. The survey correlates two sets of data: on the one hand the respondents' perceptions of the most frequent types of fraud, and on the other actual incidence rates. As regards perceptions, the respondents indicated embezzlement (29%) and corruption (23%) as the most prevalent frauds. Breach of trust was cited by only 9%, and cyber crimes by only 6%. The real incidences, however, were as follows:

- 63% of the 854 companies subject to fraud reported embezzlement;
- breach of trust was more frequent than perceived (24%);
- cyber crimes were experienced by 13% of the companies that had suffered economic crime. As emphasised by the analysts, this means that cyber-crime is not just an issue for the future.

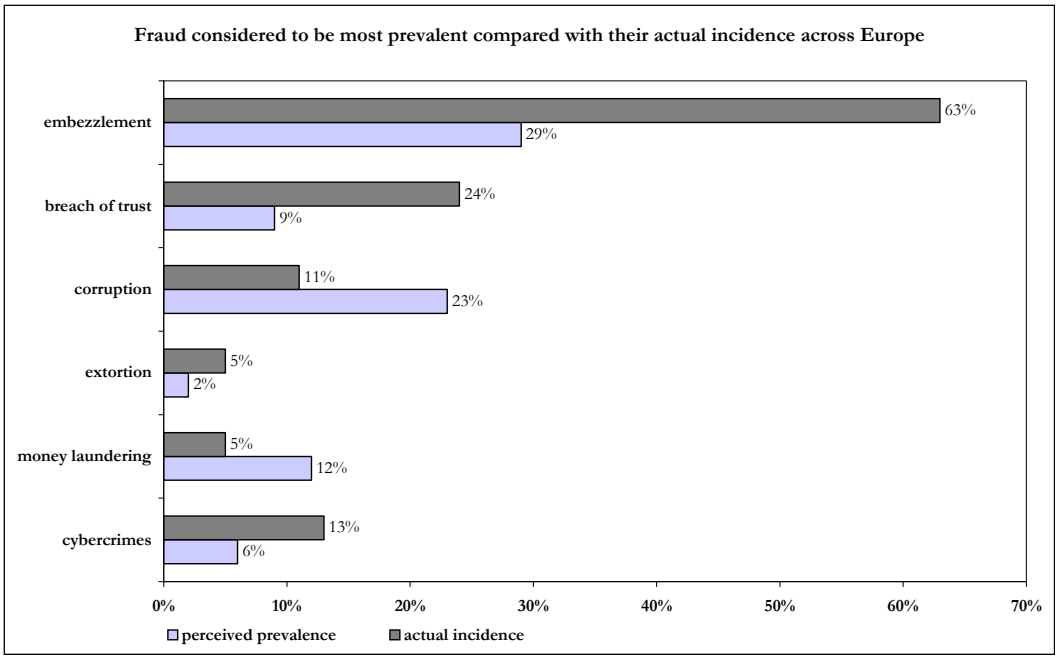
The other significant findings of the survey concern the cost and the consequences of crimes. Of the 854 organisations interviewed, 536 were able to provide an estimate of how much they had lost. The results are as follows:

- companies with more 5,000 employees suffered losses amounting to €2.6 billion;
- companies with fewer than 5,000 employees suffered losses amounting to nearly €1 billion, which means that fraud cost them €3.1 million on average;
- nine of the companies interviewed had lost more than €100 million each because of fraud in the previous two years. These are the 'mega-frauds' that, contrary to common belief, happen quite regularly.

PricewaterhouseCoopers' analysts calculated the average loss per company at €2.4 million.

Finally, an overview of economic crime risks in the future is provided by the following figure, which itemises the frauds considered most prevalent, compared with future concerns across Europe.

Figure 3



Source: PricewaterhouseCoopers, European Economic Crime Survey 2001

It is interesting to note that although embezzlement and breach of trust are two of the most recurrent types of fraud, companies seem to be entirely unaware of their real incidence. Instead, they seem to give much more importance to 'traditional' crimes like money laundering and corruption, which are overestimated when compared to their actual incidence.

With regard to future trends, particular attention should be paid to computer crimes, where the main risks will derive from:

- hackers;
- viruses;
- Internet fraud;
- abuses by employees.

European trends are confirmed elsewhere. As regards the United States and in specific InfoSecurity, for example, surveys conducted in recent years by the Computer Security Institute (CSI) and the FBI's Computer Intrusion Squad have shown that e-business is substantially at threat. In particular, the 2002 CSI/FBI Computer Crime and Security Survey reported the following:[12]

- 90% of respondents (mostly large corporations and government agencies) had detected computer security breaches in the previous 12 months;
- 80% acknowledged financial losses due to computer breaches;

[12] The survey is based on replies by 503 computer security practitioners in U.S. corporations and government agencies.

- 44% (223 respondents) were willing and/or able to quantify their financial losses;
- these 223 respondents reported almost 456M$ in losses. This figure is of particular importance if compared to the losses reported in 2001, when the 186 respondents stated that they had lost 378.5M$;[13]
- the most serious financial losses derived from theft of proprietary information and financial fraud;
- as regards the main internal vulnerabilities, for the fifth year in a row, the respondents cited their Internet connections (from 59% in 2000 to 70% in 2001 and 74% in 2002) and internal systems as the most frequent points of attack;
- the most frequent attacks took the form of:
  penetration from outside (40% of respondents, as in 2001);
  denial of service attacks (40% of respondents; 36% in 2001);
  abuses of Internet access privileges – for example, inappropriate use of e-mail systems and downloading of pornography or pirated software (78% of respondents; 91% in 2001);
  computer viruses (85% of respondents; 94% in 2001).

On the basis of these data, and confirming the results of previous years, the survey underlines the fact that a successful defence against cyber-attacks requires more than just the use of information security technologies. Security must become a 'business philosophy'. Info Security, in specific, 'requires a whole-hearted organizational commitments of resources (financial, human and technological) to an enterprise-wide program designed to evolve and adapt to new dangers. But most people are looking for a quick fix'.[14]

These conclusions are not applicable to the American context alone; on the contrary, they perfectly describe the European framework as well. Moreover, this reflection should not be referred only to Info Security but it should be applied also to business security, in general.

3. THE ICT REVOLUTION AND THE CYBER-MENACE

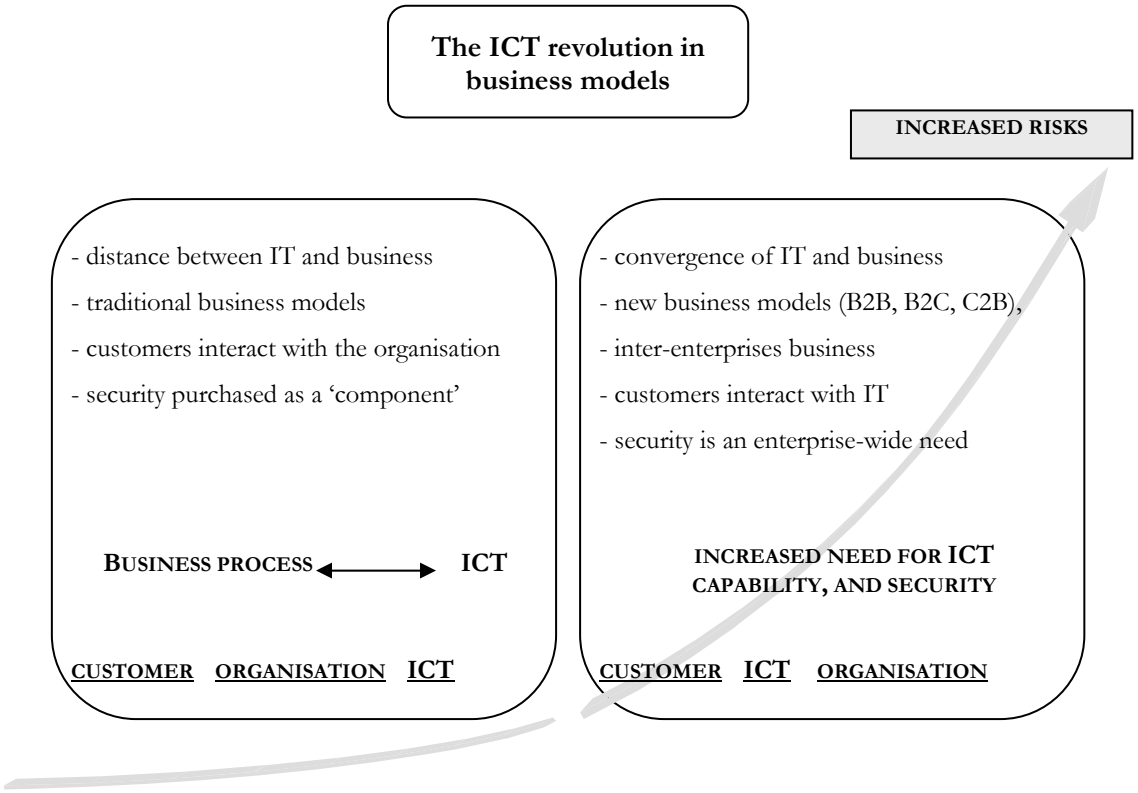
One of the most important changes to have taken place in the business environment can be called the *ICT revolution*.[15] The development and use of new information and communication technologies (ICT) in the private sector is of particular significance in two main respects: on the one hand, the ICT revolution is redesigning business models and the internal organisation of companies. On the other, it is raising new challenges for the way in which business security is administered.

[13] According to the 2001 survey, the average annual total over the three years prior to 2000 was 120.2 M$.

[14] CSI/FBI, *2002 CSI/FBI Computer Crime and Security Survey*, 2002, p. 3.

[15] The term Information and Communication Technologies is used in this Report to refer to all software and hardware components of an organization that contribute to the performing of some useful and/or critical functions.

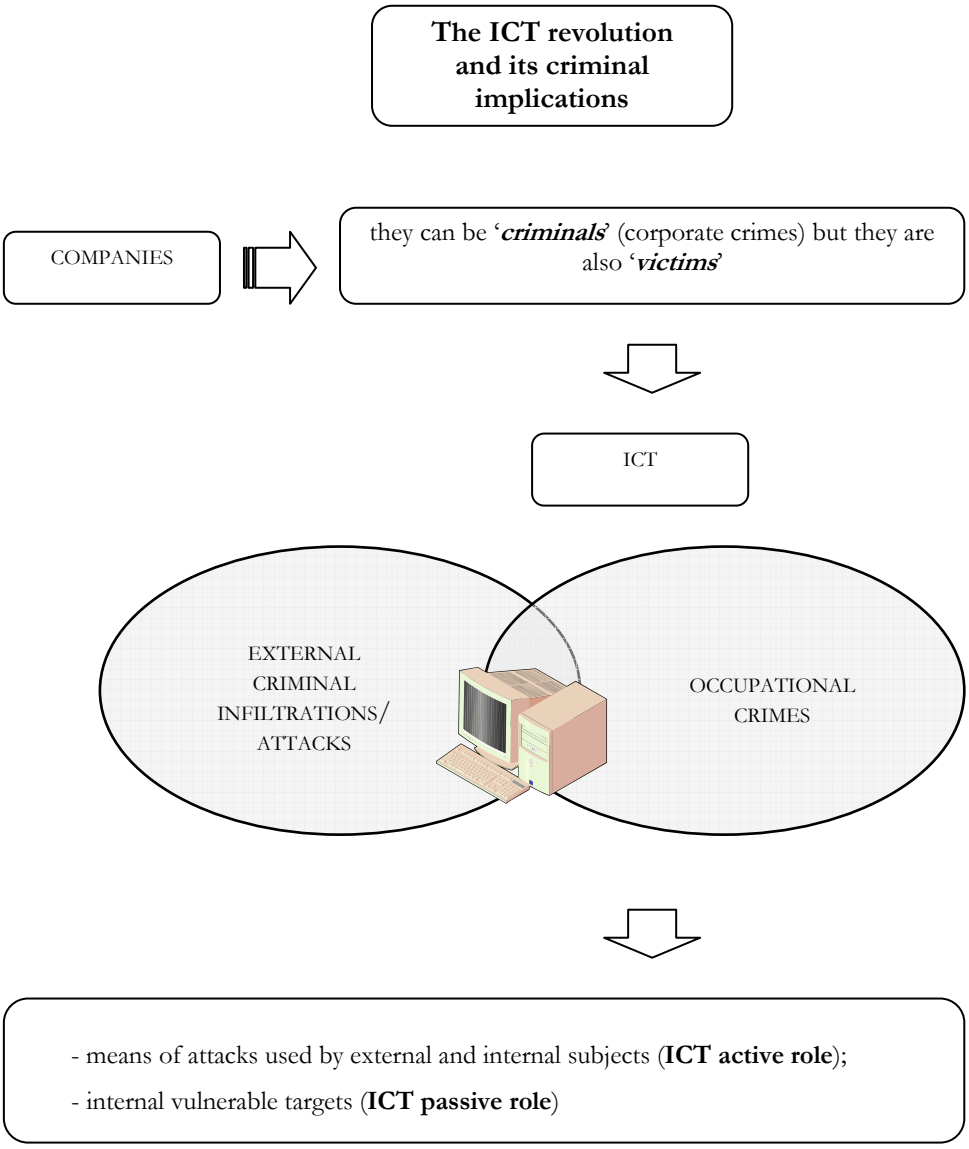
As far as internal organisation is concerned, the changes can be depicted as follows.



Before the ICT revolution, information technologies were merely one component of a business organisation; now they are an essential part of it and their role is crucial for the industrial sector. In the so-called 'old world model', traditional business models used technologies mainly for production, or at least for the internal management of data and information. Customers interacted directly with the organisation, and security was viewed as an 'adjunctive detail' which was often outsourced. This environment has changed radically; new technologies are now not only part of the manufacturing/service activity but form the core of new business models. The results of the growing convergence between ICT and business are, for example, *E-business models* such as B2B (business-to-business) and B2C (business-to-consumer), and recently also C2B (consumer-to-business). Companies are using Internet, as well as Intranet and Extranet, to open their offices and warehouses to other companies, suppliers and customers. As a consequence, new technologies form 'virtual gates' that companies must open if they are to be competitive in the changing economy. The distinctive features of the various economic sectors notwithstanding, every company must be accessible and available for its customers and suppliers, and at the same time flexible and prompt in relationships and economic transactions with its partners.

The fact that ICT are now part of business processes is of particular relevance to the security issue; if it is true that there is an urgent need for ICT capability and availability, it is to be stressed that ensuring ICT security is crucial to obtain them.

The following tries to illustrate and sum up the vulnerability of new technologies in the private sector.



The fact that the ICT are vulnerable to crime is changing the perspective from which the business sector is considered. To date, companies have been largely seen as 'criminals', the perpetrators of so-called 'corporate crimes'. Public opinion, public institutions and the law enforcement agencies have long focused on this aspect alone, underestimating all the issues related to crimes against the private sector. The risks now raised by the 'computerization' of the private sector are changing these attitudes, and they are according companies new status: that they can be (and ARE) victims.

In this scenario, computers are devices that can be used to attack a company, and at the same time they are also the targets of such attack. In other words, they are powerful instruments for assault which can be used inside and outside the company, but they are also vulnerable internal assets. As will be explained below, their vulnerability exposes companies to a wide range of criminal activities and damage.

Against the general background just described, a more precise analysis follows:

- new technologies may be the *subject* of a crime. This happens when they form the environment in which the crime is committed;
- new technologies may be the *object* of a crime. This happens when the criminal act has an effect on technologies so that they are the object (or target) of crime;
- new technologies may be used as the *tools* for the commission or planning of a crime. For example, they may be used to forge documents or to create/manipulate data and information. In these cases they constitute the *instrument* of the crime;
- in some cases, new technologies may be a *symbol* of crime. This happens, for example, when they are used to intimidate or deceive.

It is important to bear in mind that, as the potential for fraud or other serious crimes exists in the real world, the same threats carry over to the Internet as well.[16] Some forms of unlawful behaviour are long-standing and well known, but they now differ because they are committed online; others, but contrast, are new and the directly involve and target technologies.

The ICT revolution is a veritable 'Pandora's box' of criminal offences and challenges. The problem is, however, that the lid has already been removed.

Computer crime trend must not be underestimated, especially because these kinds of crimes/violations:

- are common to all business sectors, even to companies which are essentially routine-work based;
- involve hardware, as well as software and networks.
  A part from laptops thefts, which are quite common, of particular interest is also the frequency of web site home page defacement and of denials of service (DoS),[17] especially distributed (dDoS).[18]
  Defacements are particularly on the increase; the year 2001 saw over 20,000 cases, compared to the 5,000 reported in the year 2000. This figure should not be taken lightly, considering that most of these attacks are not reported, so that there is a considerable *dark number*; moreover, in 2002 the number of defacements is expected to increase further[19].
  According to the CERT Coordination Centre at Carnegie Mellon University (Pittsburgh, USA), dDos attack technology also requires particular attention. It continues to evolve and, most importantly, it is constantly used to attack and

[16] Janal D.S., *Risky Business*, John Wiley & Sons, Inc., New York, 1998, p. 4.

[17] It is the intentional degradation or blocking of computer or network resources.

[18] In a distributed denial of service attack, attackers outside a site/network send packets of mock traffic that floods servers, preventing real users from accessing the requested information.

[19] Lyttle R., "Computer Crime in 2002. An insider's Opinion", 25 January 2002.

impact Internet infrastructures[20]. In general, the impact of DoS attacks depends on the ability of the attack itself to consume available resources. As reported by CERT, today's attack methods and tools place even the most abundant resources at risk of disruption. Moreover, there is collateral damage not directly associated with the consumption of the target resource(s).

These are only some examples of crimes against computer networks and systems; it is to be stressed that their impact on the single targeted company, as well as on the community as a whole, may be extremely serious. This is the case, for example, of attacks against crucial private and/or public infrastructures such as air traffic control, telecommunications, power supplies or even medical and hospital services.[21] Attacks against them may be really disastrous: an *electronic Pearl Harbour*. [22]

According to its seriousness and to the assets that it may damage, this behaviour is labelled as either *Internet vandalism* or *cyber-terrorism.* One of the most recent but also most worrying threats to company security is that raised by activists and terrorists. Albeit in different ways, both these groups are motivated by an endeavour to affirm their ideals, which may be political, social, economic and/or religious. They usually resort to violent methods in order to achieve their results and to gain visibility; they seek to demonstrate the strength and the determination of their group by focusing mass attention on their activities and mission. The probability of activist and terrorist crimes is high; in the former case, companies are particularly concerned about the so called 'no-global' groups campaigning against globalisation. Since the September 11 attack on the World Trade Centre in New York, terrorism too has generated increasing alarm.

---

[20] CERT, *Trends in Denial of Service Attack Technology*, October 2001.

[21] As explained by Shimeall et al., "*denials of service attacks would take on new meaning where the services do not simply provide access to the Internet but are systems supporting critical, national infrastructures, systems are not designed for prolonged outages. A chronic loss of power generation and transmission capabilities, for example, would have a major impact on medical and other emergency services, communications capabilities and the capacity to manage. A failure of emergency services in major cities would not only result in the deaths of those requiring such services but also in a loss of confidence in the government's ability to provide basic services and protection. As it become apparent that the attack was impacting other infrastructure such as communications, transportation and water, the levels of fear and loss of confidence would begin to impact the basic social fabric. Attacks against the financial infrastructure would erode the capacity of business to function normally and raise questions among the public about the security of their personal finances, including retirements accounts, investments and personal savings. Military networks, all of which utilize commercial communications pathways, would also be hampered, undermining command and control, logistics and both preparedness and operations. In unrestricted cyber-warfare, virtual attacks can have consequences that are real, profound and far-reaching*".

Shimeall T., Williams P., Dunlevy C., "Countering cyber war", in *NATO review*, winter 2001/2002, p. 17-18.

[22] "*Commenting about the public's awareness of the threat to America's computers from invisible attacks, Richard Clarke, the current White House "terrorism czar" said: [CEOs of big corporations] think I'm talking about a 14-year-old hacking into their Web sites. I'm talking about people shutting down a city's electricity, shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs . . . . Imagine a few years from now: A President goes forth and orders troops to move. The lights go out, the phones don't ring, the trains don't move. That's what we mean by an electronic Pearl Harbor*". Sussman M. A., "The critical challenges from international high-tech and computer related crime at the millennium", in *Duke Journal of Comparative and International Law*, vol. 9, p. 451.

The FBI has warned of the following six trends, which should be borne in mind when developing security programmes:[23]

1. terrorism will continue to be a major international problem. Not only will it not go away, but it is continually evolving;

2. transient groupings of terrorists will emerge;

3. *terrorists will increasingly use 'soft targets' such as businesses*;

4. attacks will become more lethal;

5. more attacks will go unclaimed;

6. the dividing line between domestic and foreign terrorism will become less clear.

Who is generally involved in ICT attacks and/or incidents, and why?

At one extreme of an increasing scale of potential hazard are teenagers playing with their home computers and modems, while at the other are ultra-dangerous and high-skilled criminals who break into public and private networks for various purposes. Taxonomies of attackers and their primary motivations have been developed in the literature; it seemed reasonable to choose those that, even if more general, are more immediate.

One of the models most frequently cited is the one developed by *Russell* and *Gangemi*, who identify two main categories of attacker: *insiders* and *outsiders*. Insiders are employees, former employees, students etc. Outsiders include foreign intelligence agents, terrorists, criminals, corporate riders and hackers. This distinction is completed by an alternative approach which identifies attackers by what they typically do in relation to their reason for doing it. The classification is simple and is based on the following six categories:

hackers: these break into computer systems because it is a challenge that they must overcome to gain the status that accrues from obtaining *access*;

spies: these break into computer systems primarily for information that they will use for *political gain*;

terrorists: these want to provoke the fear and social alarm that is the key element in achieving *political gain*;

corporate riders: employees of one company break into a competitor' system for *financial gain*;

professional criminals: their *financial gain* is personal;

vandals: their intent is to cause *damage*.

As regards the term *hacker*, it must be highlighted that this is a term widely used, but also widely confused because of its multiple meanings. For the purpose of this Report, it will be used in a generic way, as a synonym of

[23] Terrorism will be analysed in detail in Part III.

attacker. Anyway, when talking about malicious hacker, it is more correct to define them *crackerz*.

There is also growing concern about organised criminals who use communication networks to attack information systems for their own purposes. There are organised hacking groups active world-wide which specialise, for example, in hacking and defacement of web-sites. Examples include the Brazilian Silver Lords, the Pakistan Gforce, but also Russian groups which seek to extort money from their victims by offering them specialised assistance after hacking into their information systems. Similar cases have been reported in Europe. The arrests of large groups of hackers suggest that hacking may increasingly become an organised crime phenomenon. In Russia, for example, it seems that traditional criminal organizations have recruited hackers (through coercion or bribery or a mix of the two) to carry out computer crimes and attacks on their behalf. Recently, there have been also sophisticated, organised attacks against e-commerce sites, together with attempts to steal substantial funds from on-line banking services.

- are committed both within and without the company;
- often affect some of the most important company assets: data and information. The so-called new economy is mainly designed around these, with the consequence that they are increasingly crucial for the company competitiveness. From the criminal perspective, however, information systems provide the opportunity and means to commit a wide range of illegal acts targeted on company data and information:[24] a part from theft and fraud, other examples are corporate and economic espionage, surveillance of business competitors, interception, theft and/or manipulation of data and information, also in breach of privacy and confidentiality laws, and the counterfeiting and forgery of electronic documents. From the commercial point of view, Internet and ICT have created a paradox: on the one hand they have improved or even started economic growth; on the other, high tech systems have made trade and commerce secretes much more difficult to protect. This is of importance not only to the individual company but also at national level; the FBI suspects, for example, that more than twenty countries are actively trying to steal the trade secrets of United States companies'.[25] The role of insiders should not be underestimated: there is today no need for a disgruntled employee to carry out boxes of confidential documents, trying to avoid the guards at the front door; while competitors do not have to bribe an insider to obtain proprietary information. An unhappy or opportunistic employee can steal a company's most important trade secrets, simply by saving them on a floppy disk and walking out the office with it in his/her pocket. Or, more easily, s/he can use the Communication Technologies, like email (if not under the company's control) and instant messaging programs (when available they are still 'secure' for fraudsters because they are very often unmonitored).
  Moreover, as said, data and information can also be stolen by gaining unauthorised access to the company's computers system. Examples abound of industrial espionage committed by hackers (or more accurately, '*crackerz*') who

[24] Smith R. G., "Criminal Exploitation of New Technologies", in *Trends and Issues in Crime and Criminal Justice*, n. 93, July, 1998.

[25] Dilworth G., "The Economic Espionage Act of 1996: an Overview", 2001. The text is available at the following URL: http://www.cybercrime.gov/usamay2001_6.htm.

sell their skills and expertise in new technologies to whoever is willing to pay. It should be stressed again that these persons may be outsiders but they could also be insiders: besides the expertise, the latter also have more detailed knowledge of the company, its vulnerabilities and the relative opportunities.

The European Commission has recently presented a proposal for a Council framework decision on attacks against information systems.[26] On the one hand, this document emphasises that communication networks and information systems are an essential part of the daily lives of EU citizens and also play a key role in the development and success of the EU economy. On the other, it stresses the concrete risk that international attacks which will jeopardise the achievement of a safer Information Society and an Area of Freedom, Security and Justice. In consequence, the aim of this Proposal is to contribute to the harmonisation of criminal law regarding attacks against information and communication systems.

The Proposal also proposes a typology of cyber-attacks which may prove useful for general classification of the most common forms of unlawful behaviour:[27]

a) unauthorised access to information systems. This definition also encompasses the notion of 'hacking' as the gaining of unauthorised access to a computer or a network of computers. This may be undertaken for various purposes, ranging from simple exploitation of the stored information to more serious attacks and passwords interception. Generally, hacking is motivated by malicious intent to copy, modify, steal, manipulate or destroy data. The corruption of web sites and access to services protected by conditional access without payment may also be among the purposes of unauthorised access;
b) disruption of information system; apart from denial of service, this category includes, for example, disruption of servers operating the domain name system (DNS) and attacks on routers.
c) execution of malicious software that modifies or destroys data; the most common examples are worms and viruses. According to the Proposal, about 11% of European users have caught viruses on their personal computers;
d) interception of communications (sniffing);
e) malicious misrepresentation; this category comprises all cases of fraud perpetrated by exploiting the opportunities provided by ICT and Internet.

---

[26] European Commission, *Proposal for a Council Framework Decision on Attacks against Information Systems*, Brussels, 19 April 2002, COM(2002) 173 final, 2002/0086 (CNS).

[27] These classification has already been used in the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *Network and Information Security: Proposal for a European Policy Approach* of 6 June 2001. COM (2001) 298 final.

PART II - THE CASE-STUDY ANALYSIS

4. RESEARCH DESIGN AND DATA COLLECTION PROCEDURE

One of the main objectives of the FALCONE 2001 - BUSINESS CRIME PREVENTION: IMPLEMENTING AN EARLY WARNING STRATEGY Research Project was to conduct a victimisation survey in the business sector. This was stated in Goal 2 of the research proposal:

Goal 2 - *the experimental development of a new strategy for business crime prevention based on a survey of company victimisation which will enable the creation of an information database appropriately classified and able to single out recurrent criminogenic features*.

In the intention of the research design, achievement of this Goal should have yielded a twofold result: on the one hand, it should have improved knowledge of the most frequent and serious business crimes, while creating an information database should have enabled the sharing of information among the interested subjects. On the other, it should have contributed to academic research on business security issues by developing a model for assessment of the risk of criminal infiltration of businesses and occupational crimes against them.

The methodology and the various research tasks required to fulfil these aims were stated by the project proposal.

The methodology was described as follows:

With reference to Goal 2, a questionnaire distributed to major companies in each Member State will enable the collection of data on business crimes and prevention strategies. The co-operation provided by the International Security Management Association (ISMA), as stated in the letter of patronage attached to the project, will facilitate contacts with companies. Furthermore an in-depth survey on business security will be conducted in 41 countries in Europe using national contacts provided by Pirelli S.p.A. An analytical theory will be tested, refined and compared with the empirical data, the intention being to identify early warning signals.

The tasks were the following:

task 6) creation of specific questionnaires distributed to multinational companies in the following 3 stages:

- *pilot survey of multinational companies with headquarters in Italy;*
- *distribution to a reduced sample of multinational companies with European headquarters;*
- *distribution to a larger representative sample of multinational companies, preferably with headquarters in Europe;*

task 7) statistical analysis of the relationship between past cases collected by questionnaires and the anomalies detected will seek to highlight recurrent features

as well as the presence of possible anomalies as indicators signalling, in advance, illicit phenomena;

task 8) criminological profiles will be drawn up to facilitate identification of the potential risks of criminal infiltration .

As explained, the project encountered problems in its implementation, and changes had to be made to both the research design and the methodology. The following sections explain these changes in detail.

5. The Steering Committee guidelines and the main stages of the research

The drafting and administration of the questionnaire, as well as the implementation of the other tasks, were discussed during the meeting of the Steering Committee held at Pirelli S.p.A. headquarters on 14 September 2001. As stated in the minutes of the meeting, the Committee reached the following conclusions:

As regards the *questionnaire*, the Committee suggested that the draft version should be altered by:

- reducing the number of questions;
- simplifying the language and the questions;
- paying closer attention to organised crime, rather than to crimes committed by individuals;
- placing greater emphasis on IT crimes;
- giving clear contact details of the person responsible for the project.

The Members of the Committee asked to receive a copy of the revised questionnaire, when ready, so that they might make further comments and suggestions. In particular, Europol promised to give assistance with regard to methodology.

During discussion of the *administration* of the questionnaire, the Committee agreed that the survey should focus on the 15 Member States. In practice, this entailed simplification of task 6) from the above-cited initial 3 steps of the victimisation survey into a single phase. As regards addressees, Transcrime - University of Trento was invited to involve members of ISMA and ERT (European Round Table of Industrialists). The Steering Committee hoped that all the ISMA associates in Europe would participate in the research and invited Transcrime-University of Trento to include American enterprises willing to co-operate. Their replies would enhance the value of the survey, although they would not be included in the comparative analysis of European enterprises.

Prof. Savona was invited by Mr. Burrill to attend the ISMA-ERT Meeting in Brussels on October 5th in order to explain the project and to persuade enterprises to take part.

Furthermore, the Committee emphasised that the maximum level of confidentiality should be guaranteed for private companies participating in the survey. It accordingly determined that the names of such companies would never be mentioned in any phase of the project.

The research was consequently divided into the following stages in strict observance of the Steering Committee's guidelines:

- Prof. Savona attended the ISMA meeting held in Brussels on 5 October 2001, on which occasion he presented the FALCONE 2001 – BUSINESS SECURITY Research Project;
- the questionnaire was modified, integrated and finalised in accordance with the Steering Committee's suggestions; it was then sent to each Member to collect their final impressions. In particular, it was sent to Mr. Hegel, at Europol, so that it could be given final revision by Europol analysts. Therefore, the definitive version of the questionnaire is the result of a joint effort by Transcrime – University of Trento and the Members of the Steering Committee;
- as regards confidentiality, a note was inserted in the questionnaire which explicitly assured the respondent that all the information given would be treated with the maximum confidentiality. It explained that the results would be made public only in aggregate form, so that it would be impossible to identify the various companies completing the questionnaire.
- the final version of the questionnaire was then administered with the co-operation of Mr. Burrill and the ISMA and ERT Secretariats.

6. THE QUESTIONNAIRE AND ITS ADMINISTRATION

As said, the questionnaire was the outcome of joint revision by the Members of the Steering Committee of the initial draft version prepared by Transcrime – University of Trento.

The result of this revision was a complete and detailed document containing not only the questions but also general information about the Research Project and its purposes. Indeed, it seemed only proper to explain the background and aims of the Research Project to all the companies willing to be interviewed. Moreover, it was necessary to provide these companies with information indispensable for understanding the exact meaning of the questions.

On this basis, the questionnaire was structured into the following sections:

- *contacts and information:* this section contains all the information about the project manager at Transcrime – University of Trento to be contacted for all explanation and information required;
- *preliminary statement:* this section briefly explains the purpose of the research, and in particular the importance of precise information if measures against crimes affecting businesses are to be effective;
- *some key concepts*: this section provides a glossary of the terms most frequently used in analysis of business security issues;

- *the pattern of reference*: this section explains the simplified theoretical model that provides the basis of the research and which will be tested by the information collected. Formulated after exploratory analysis of the documentation and literature available on business security,[28] the model is as follows:
  the probability (R) that a company may be a victim of a crime is hypothesised as being:
  – strictly dependent on the quantity and quality of assets potentially at risk (G)
  – proportional to the means and opportunities available to employees and criminals to commit and/or participate in the crime (F)
  – inversely proportional to the measures taken to protect the company's assets

  (S)
  in sum:
  R=f(G,F,S)

  Explanation of the model was included in the questionnaire in order to prompt suggestions and comments from the interviewees, whose practical approach, combined with their knowledge of the private sector, would be extremely useful to the Project for refinement of its theoretical perspective and analysis;

- *addressees of the questionnaire*: this section explained to whom the survey is addressed;
- *the structure of the questionnaire*: this section provided information about how the questionnaire was organised.
- *confidentiality*: this section emphasised that all information and data would be strictly confidential and treated with the maximum discretion;
- *the questionnaire*: the following table sums up its structure.

	G – assets at risk	F – factors involved in the crime	S – security measures
Part I (identification of subject/company interviewed)	Questions 1 – 13		
Part II (recording of cases in the previous two years)	Questions 14 – 16	Questions 17 – 26	Questions 27 – 42
Part III (recording of managers' perceptions of security)	Questions 43 – 50		

As said, the questionnaire was sent together with an accompanying letter which presented the project and the partners involved.

[28] Of especial relevance is the model developed by Tim Ozenne for bank robberies. Ozenne T., "The Economics of Bank Robbery", in *Journal of Legal Studies*, Vol. 3, 1974.

The questionnaire was administered by Transcrime – University of Trento jointly with ISMA, and with the co-operation of ERT.

ISMA used its internal mailing list to send the questionnaire and the accompanying letter to all its members, asking them to help with the research. The list of ISMA European Members – updated to 6 March 2002 – was immediately made available to Transcrime –University of Trento in order to facilitate direct contacts with those companies willing to participate. A total of 34 European companies belong to ISMA.

ERT for its part wrote to all 45 of the ERT Associates (representatives) of ERT Members (CEOs) asking them to send the name of the Heads of Security in their companies.

Transcrime – University of Trento then endeavoured to send the questionnaire and the accompanying letter only to those requesting them.

Moreover, thanks to ISMA's co-operation, the research was also presented to its American members, who were invited to participate even though their replies would not be used for the study.

7. THE QUESTIONNAIRE'S RESULTS: FROM THE VICTIMIZATION SURVEY TO A *CASE-STUDY* APPROACH

Notwithstanding the efforts of Transcrime - University of Trento, ISMA and ERT, the final result of the questionnaire administration procedure was disappointing.

Only ten completed questionnaires were returned, in fact, [29] plus a further questionnaire completed by an American company.

Most of the companies contacted did not reply either to requests to complete the questionnaire or to reminders sent before the deadline. In order to encourage participation the latter was postponed at least three times: from the end of March to the middle of April to the middle of May. But even this had no effect.

However, it should be stressed that some companies realized when they had read the questionnaire that, for different reasons, they were unable to participate, in the great majority of cases adducing a lack of information on internal business crimes and security related issues as the reason. When this information was available, it was often in disaggregated form, or it had been collected only for some of the company's branches (not always located in Europe), and consequently could not be used to determine the real situation of the company.

We would also stress that some of the contact persons (mainly Heads of Security) stated that their companies had not experienced crimes during the previous two years (the period covered by the questionnaire). Or, when they had occurred, they had mainly been 'secondary offences'; in other words, they were not serious enough to warrant investigation or did not exceed the internal 'tolerance level'.

[29] In order to respect confidentiality, the names of these companies are not given.

Nevertheless, aside from the victimization survey, these companies expressed close interest in the BUSINESS CRIME PREVENTION: IMPLEMENTING AN EARLY WARNING STRATEGY Research Project, in its findings and in its methodological approach to business security related issues. They will thus be ready to co-operate in the future, as well as to share their data and information for research purposes.

To return to the results of the questionnaire administration, the lack of participation obviously created problems for management of the project. This marked and unexpected under-participation made revision of the research design absolutely necessary. From the methodological point of view, in fact, it was impossible to undertake a victimization survey in the absence of a representative sample.

In order to profit from the information collected, it was thus decided to adopt another approach: namely *case study methodology.*[30]

Case study is the investigation of a relatively small number of cases, sometimes just one; information is gathered on a large number of features in each case and then analysed. The most important aspect of this methodology is that it does not give priority to the quantification of data, and its primary concern is not to control variables in order to measure their effects. Rather, it is principally interested in qualitative data.[31]

On this basis, the main objective is to understand individual cases in and of themselves, with no other theoretical inference or empirical generalization being drawn, although the findings can be used at a later stage for comparative analysis or as the starting point for further, more general research.

In order to clarify the methodology used to analyse the questionnaire, it is explained, step by step, in the following section.

Finally, we would emphasise that, technically speaking, this study is not a victimization survey, but rather a *pilot study*. However, in profiting from this experience, and especially from the study's findings, it could be followed by further research in the near future.

[30] Hagan F. E., *Research Methods in Criminal Justice and Criminology*, 4th ed., Allyn and Bacon, 1997.

[31] Gomm R., Hammersley M., Foster P. (edited by), *Case Study Method*, Sage Publications Ltd, 2000.

8. THE CASE-STUDY ANALYSIS: METHODOLOGY

The main aim of the following case-study analysis is to use the information collected by the questionnaire to determine how the companies interviewed managed security related issues.

As said, from a theoretical point of view, the research was based on a model – what can be called the '*risk-model*' – around which the questionnaire was designed in its entirety. The model is as follows:

R=f(G,F,S)

the probability (R) that a company may be a victim of a crime is hypothesised as being:

- strictly dependent on the *quantity* and *quality* of **ASSETS** potentially at risk (G)
- proportional to the **MEANS** and **OPPORTUNITIES** available to employees and criminals to commit and/or participate in the crime (F)
- inversely proportional to the **MEASURES** taken to protect the company's assets (S)

Once the questionnaires had been collected, the main problem was that the model could not be properly tested using a case-study methodology and with so little information. Accordingly, the victimization survey could not be replaced or substituted.

Nevertheless, it seemed that the questionnaires could be fruitfully used to describe – at least from a qualitative point of view using case-study analysis – the three main variables of the model and their characteristics with reference to the cases available.

The cases were therefore analysed with particular attention to all the information and data that shed light on:

- assets: was there a relationship between the assets affected by crimes and the types of crimes?
- means and opportunities: who were the offenders, what means did they use, and what opportunities did they exploit?
- preventive and repressive measures adopted by the company interviewed: did the company manage security in an appropriate manner?

It is important to stress that – fortunately – the returned questionnaires came from different economic sectors, so that it was possible to conduct comparisons among different environments and experiences. The economic sectors most represented were: services, manufacturing, and transport.

Starting from these premises and according to the questionnaire structure, the case-study analysis will be organised on the basis of the following scheme:

- part I – *profile* of the interviewee and of the company;
- part II – recording of cases during the previous two years; this part focuses on the *assets at risk* (G), on *crime factors* (F) and on *security measures* (S);
- part III – recording of managers' perceptions of security.

Each part will contain synoptic tables setting out and summarising the most relevant information.

9. THE CASE-STUDY ANALYSIS: RESULTS

PART I – PROFILES OF THE INTERVIEWEES AND THE COMPANIES

The majority of interviewees were *Heads of Security* (5) and *Chief Executive Officers* (2); the other three were *Head of Internal Audit*, *Chief Financial Officer* and *Assistant Manager*.

None of them had changed their function/role with the company during the previous two years.

The company areas in which the interviewees carried out their functions were mainly *Security* and *Human Resources Management*. *Purchases*, *Research and Development*, *Sales*, *Administration and Finance*, *Internal Audit* were also indicated. Because of their central roles and high-level positions in the company, these respondents should have possessed detailed knowledge of the internal situation.

Despite the low number of questionnaires, it should once again be stressed that almost all economic and industrial sectors were covered:

Case 1: *Business risk consultancy*;

Case 2: *Financial services*;

Case 3: *Manufacturing*;

Case 4: *Petroleum and petrochemicals. Chemicals*;

Case 5: *TLC*;

Case 6: *Transport*;

Case 7: *Recruitment services*;

Case 8: *Textiles, Clothing, Cork, Real estate, Tourism, Insurance, Capital development*;

Case 9: *TLC – mobile*;

Case 10: *Manufacturing*.

The economic profile of the companies surveyed is as follows: annual turnover was on average substantial; the majority of the companies (6 out of 10), in fact, had turnovers estimated as over 2,500 million Euros. The approximate budget of the Department in which the interviewees worked was not always stated. In eight out of ten cases, the company is quoted on the stock exchange.

The following table schematises the geographic location of the companies: all of them were multinational enterprises with their headquarters in Western Europe but operating world-wide. In order to ensure confidentiality and anonymity, headquarters are generically labelled as located in 'Europe'.

CASE	HEADQUARTERS	BRANCHES (number of countries worldwide)
1	EUROPE	14
2	EUROPE	82
3	EUROPE	185
4	EUROPE	20
5	EUROPE	20
6	EUROPE	'all over the world'
7	EUROPE	'global'
8	EUROPE	140
9	EUROPE	South Europe – South America
10	EUROPE	more than 50 countries

As far as business activity is concerned, there were no significant differences between the two categories indicated in the questionnaire: the cases cover both *innovation-oriented* companies and *routine work* companies.

All the interviewees were able to give data on the percentages of male and female employees in their companies: with the exception of only one case, the workforce was predominantly male.

CASE	MALE EMPLOYEES (%)	FEMALE EMPLOYEES (%)
1	59	41
2	40	60
3	70	30
4	83	17
5	70	30
6	58	42
7	60	40
8	80	20
9	54	43
10	70	30

By contrast, not all companies gave figures on age and educational level:

- the question on age was: 'can you approximately indicate the percentage of employees in your company according to their age?'. 8 of the 10 companies answered the question; as regards the other two, the first one ticked the answer 'unknown' while the second did not reply. According to the figures available, employees are aged on average between 35 and 50, and between 25 and 35;

- 7 of the 10 companies answered question 12 on educational level, which asked: 'can you indicate the percentage of employees in your company according to their educational level?'. Of the other three, the first ticked the answer 'unknown', while the others gave incomplete data. According to the figures available, the vast majority of employees had secondary school diplomas.

Interestingly, the workforce's educational level is generally high in almost all business and economic sectors; this is particularly in the case of the so-called new businesses, such as TLC, consultancy and services in general. Traditional productive activities like manufacturing are typically characterized by employees who have elementary school certificates. Some examples follow:

Case 1 – business risk consultancy: 70% of employees had secondary diplomas, the other 15% had degrees and one a master's degree;

Case 3 – manufacturing: 65% had elementary school certificates, 15% had secondary school diplomas and degrees. The next 5% had master's degrees;

Case 5 – *TLC*: 20% had elementary school certificates, 60% secondary school diplomas, 15% degrees and 5% master's degrees;

Case 8 – manufacturing and services: 75% had elementary school certificates, 17% had secondary school diplomas, while only 8% had degrees.

Case 10 – manufacturing: 8% had elementary school certificates, 45% secondary diplomas, 35% degrees and 10% master's degrees (2% fall within the category 'other').

From the criminological perspective, education is of particular importance in two different and opposing respects: on the one hand, education is generally considered to exert a deterrent effect on crime. In fact, it is generally believed that the better-educated are less inclined to infringe legal and social rules. On the other hand, however, there is evidence that skilled persons are generally the authors of complex and high-damaging fraudulent schemes, which are also extremely difficult to detect and investigate. Moreover, if they occupy a senior positions in a company, they will be facilitated by their insider knowledge and by the trust placed in them.

PART II – RECORDING OF CASES DURING THE LAST TWO YEARS

G – Assets at risk

The first question in this part of the questionnaire was one of the most important:

have you got any direct experience of crimes during the last two years while carrying out your functions?

Replies:

8 out of 10 respondents replied in the affirmative way, while only two said that they had not had direct experience of crime.

These two exceptions differed from each other: in the first case, neither the interviewee nor the company had experienced crimes over the previous two years; in the second, the interviewee had not had direct experience of crime but knew of crimes committed against the company.

The surprising exception is therefore the first of these two cases: the interviewee and the company had experienced no crimes over the previous two years. It is important to specify that this case concerns a European multinational company with branches in 140 countries, an annual turnover of between 500 and 2.500 million Euros, and shares partly quoted on the stock market. Its activity was both innovation-oriented and routine-work based. As in all the other cases, the person who completed the questionnaire had not changed his/her function in the previous two years and s/he belonged to top management.

Considering that these features were largely shared by the other participants in the survey, this unique exception appears to be of particular interest. In order to clarify the company's point of view on criminal risk management, we report the brief comment accompanying the completed questionnaire: 'these problems are considered by all the organization as a strategic and fundamental area. Our security policy is to prevent criminality, namely by fomenting continuous sense of ethical conduct, as well to improve our systems and processes in order to reduce the risk and, in case of any occurrence, to limit its severity. More than a material damage or loss, any occurrence consequence would be the existence of a break in the prevention system implemented'.

The approach adopted by this company closely resembles the one proposed by this research study; this case will therefore be given specific treatment during the analysis.

The following chart schematises the relationship between the different types of businesses and, when possible, the number of crimes experienced in the previous two years by the interviewees. The last columns also state the **assets** damaged and, when indicated, the estimated damages.

CASE	ECONOMIC SECTOR	NUMBER OF CRIMES EXPERIENCED BY THE COMPANY, IN THE PREVIOUS TWO YEARS	DAMAGED ASSETS	ESTIMATED DAMAGES
1	Business risk consultancy			
		1	Money/Capital	€ 2,000
2	Financial services			
		175,000	Money/Capital	> € 100 million
3	Manufacturing			
		50 (estimated)	Manufacturing establishment	£ 250,000
		4	Facilities/Equipment / Plant	£ 750,000
			Information Technologies	£ 1 million
			Image/Reputation	
			Money/Capital	£ 3 million
			Finished products	£ 15 million
4	Petroleum and petrochemicals; Chemicals			
		1	Information Technologies	not estimated
		50	Human resources	not estimated
		1	Finished products	not estimated
5	TLC			
		10	Facilities/Equipment / Plant	not estimated
		20	Information Technologies	not estimated
		20	Human resources	not estimated
		5	Process know-how	not estimated

		5	Image/Reputation	not estimated
		10	Customer relations	not estimated
		5	Partnership with vendors	not estimated
		5	Money/Capital	not estimated
		20	Finished products	not estimated
6	Transport			
		hundreds	Money/Capital	€ 3 million
		hundreds	Customer goods	€ 5 million
7	Recruitment services			
		4	Money/Capital	not estimated
8	Textiles – clothing, Cork, Real estate, Tourism, Insurance, Capital development			
		N. A.		
9	TLC - mobile			
		10	Money/Capital	not estimated
10	Manufacturing			
		N. A.		

The relationship between the type of asset damaged and the crime is particularly important; as shown by the previous table, intangible assets, like money and capital, together with Information Technologies, are most affected in all business sectors. Also human resources and plant seem to be the most frequent targets.

To clarify differences and similarities among business sectors, the following tables schematise, for each case-study, the most frequent types of crime/infringement according to the assets damaged:

- production line/products,
- human resources;
- Information technologies;
- know-how;
- capital.

The period covered is the two years prior to administration of the questionnaire. When available, the numbers of recorded cases are also indicated.

Unfortunately, not all the questionnaires were completed accurately; for example, there were sometimes contradictions among replies given in different sections, so that they are not always reliable. However, as said, the sole purpose of this specific analysis is to give an idea of the relationships between business sector, the assets damaged and the type of crime, if any.

For each case, when possible, also indicated is the crime that had generated, during the previous two years, the most significant internal crisis and its duration.

CASE 1 – BUSINESS RISK CONSULTANCY

	yes	number of cases
infringements/crimes against human resources		
theft of money/personal effects	√	1
infringements/crimes against Information Technologies		
denial of service (DoS)	√	1
distributed denial of service (dDoS)	√	1
laptop thefts	√	2

The most significant internal crisis was generated by the *denial of service* (DoS) attack; the crisis lasted 16 hours.

CASE 2 – FINANCIAL SERVICES

	yes	number of cases
infringements/crimes against capitals		
financial fraud	√	175,000

The most significant internal crisis was generated by *internal defalcation*; the crisis lasted less than a month.

CASE 3 – MANUFACTURING

	yes	number of cases
infringements/crimes against production line and products		
theft of company good/products during the manufacturing process	√	25
theft of company products from warehouses	√	8
theft of company products in transit	√	30
counterfeiting	√	hundreds
infringements/crimes against human resources		
theft of money/personal effects	√	25
extortion	√	4
corruption of employees	√	2
infringements/crimes against Information Technologies		
illicit computer penetration from inside	√	2
defacement of the web site home page	√	1
denial of service (DoS)	√	2
damage to computer systems due to computer viruses downloaded during internal surfing	√	hundreds
damage to computer systems due to computer viruses sent from outside	√	over 2,000
theft/damage/sabotage of information in databases	√	2
disclosure and use of passwords by insiders	√	hundreds
employee abuse of Internet access	√	hundreds
theft of company time	√	hundreds
theft of information by means of social engineering techniques	√	few
laptop thefts	√	100
infringements/crimes against know-how		
trademark counterfeiting	√	hundreds
unfair competition	√	hundreds
unauthorised dissemination of information by insiders	√	occasional
unintentional release of information/know-how to competitors	√	occasional
sales of information by insiders	√	1
infringements/crimes against capitals		
financial fraud	√	3
falsification of financial statement	√	3
embezzlement	√	3
inflated expense accounts	√	
transactions involving conflict of interests	√	2

The most significant internal crisis was generated by *computer viruses and worms* (specifically Nimda and Code Red); the crisis lasted less than a month, up to 48 hours in each case.

CASE 4 – PETROLEUM AND PETROCHEMICALS – CHEMICALS

	yes	number of cases
infringements/crimes against production line and products		
theft of company products in transit	√	1
vandalism by outsiders	√	20
infringements/crimes against human resources		
theft of money/personal effects	√	50
infringements/crimes against Information Technologies		
defacement of the web site home page	√	1
damage to computer systems due to computer viruses sent from outside	√	1
laptop thefts	√	4

The crime which generated the most significant internal crisis was not indicated.

CASE 5 – TLC

	yes	number of cases
infringements/crimes against production line and products		
theft of company products from warehouses	√	
theft of company products in transit	√	
counterfeiting	√	
sabotage of plant	√	
vandalism by insiders	√	
vandalism by outsiders	√	
arson	√	
terrorist acts/diffusion of subversive materials	√	
infringements/crimes against human resources		
theft of money/personal effects	√	
identity theft	√	
extortion	√	
corruption of employees	√	
infringements/crimes against Information Technologies		

illicit computer system penetration from outside	√	
illicit computer system penetration from inside	√	
defacement of the web site home page	√	
denial of service (DoS)	√	
distributed denial of service (dDoS)	√	
damage to computer systems due to computer viruses – downloaded during internal surfing	√	
damage to computer systems due to computer viruses – sent from outside	√	
theft/damage/sabotage of information in databases	√	
disclosure and use of passwords by insiders	√	
disclosure and use of passwords by outsiders	√	
employee abuse of Internet access	√	
theft of company time	√	
theft of information by means of social engineering techniques	√	
telecom fraud/eavesdropping	√	
laptop thefts	√	
theft of transaction information	√	
cyber-terrorism	√	
infringements/crimes against know-how		
trademark counterfeiting	√	
patent infringements	√	
industrial espionage	√	
unfair competition	√	
unauthorised dissemination of information by insiders	√	
unintentional release of information/know how to competitors	√	
sale of information by insiders	√	
infringements/crimes against capitals		
administrative fraud	√	
financial fraud	√	
falsification of financial statement	√	
embezzlement	√	
purchase of goods/services for personal use	√	
inflated expense accounts	√	
transactions involving conflict of interests	√	
insider trading	√	

The most significant internal crisis was generated by *counterfeiting of products*; the crisis lasted longer than a year.

CASE 6 – TRANSPORT

	yes	number of cases
infringements/crimes against production line and products		
theft of company products from warehouses	√	thousands
infringements/crimes against human resources		
theft of money/personal effects	√	20
infringements/crimes against Information Technologies		
defacement of the web site home page	√	1
laptop thefts	√	90
infringements/crimes against capitals		
financial fraud *by means of forgery and counterfeit*	√	thousands

The most significant internal crisis was generated by *financial fraud*; the crisis lasted more than a year *permanently*.

CASE 7 – RECRUITMENT SERVICES

infringements/crimes against capitals		
embezzlement	√	2
business relations with companies involved in criminal activities/money laundering	√	2

The most significant internal crisis was generated by *embezzlement*; the crisis lasted less than a month.

CASE 8 – TEXTILES, CLOTHING, CORK, REAL ESTATE, TOURISM, INSURANCE, CAPITAL DEVELOPMENT

No crimes indicated

CASE 9 – TLC – MOBILE

	yes	number of cases
infringements/crimes against production line and products		
theft of company products in transit	√	
sabotage of plants	√	
vandalism by outsiders	√	
infringements/crimes against human resources		
theft of money/personal effects	√	
infringements/crimes against Information Technologies		
illicit computer system penetration from outside	√	
illicit computer system penetration from inside	√	
denial of service (DoS)	√	
damage to computer systems due to computer viruses – downloaded during internal surfing	√	
damage to computer systems due to computer viruses – sent from outside	√	
disclosure and use of passwords by insiders	√	
telecom fraud/eavesdropping	√	
laptop thefts	√	
infringements/crimes against capitals		
purchase of goods/services for personal use	√	

The most significant internal crisis was generated by *theft of company products in transit*; the crisis lasted less than a month.

CASE 10 – MANUFACTURING

	yes	number of cases
infringements/crimes against production line and products		
theft of company goods/ products during the manufacturing process	√	
theft of company products from warehouses	√	
theft of company products in transit	√	
sabotage of plant	√	
vandalism by insiders	√	
vandalism by outsiders	√	
terrorist acts/ diffusion of subversive	√	

materials		
unfair competition due to key employees resigning (professional roaming)	√	
infringements/crimes against human resources		
theft of money/personal effects	√	
corruption of employees	√	
infringements/crimes against information technologies		
illicit computer system penetration from outside	√	
illicit computer system penetration from inside	√	
defacement of the web site home page	√	
damage to computer systems due to computer viruses - downloaded during internal surfing	√	
damage to computer systems due to computer viruses - sent from outside	√	
theft/damage/sabotage of information in databases	√	
disclosure and use of passwords by insiders	√	
employee abuse of internet access	√	
theft of company time	√	
theft of information by means of social engineering techniques	√	
laptop thefts	√	
infringements/crimes against capitals		
administrative fraud	√	
purchase of goods/services for personal use	√	
inflated expense accounts	√	

According to the interviewee, none of the reported crimes generated an internal crisis.

Examination of the information schematised in the previous tables shows that the following groups of crimes are the most recurrent:

Almost all the questionnaires report crimes against **human resources,** and in particular the theft of money and/or personal effects. Considering that these generally occur inside the company, one may conclude that they are mainly committed by colleagues or by people with unrestricted access to the company's plants and offices. It is difficult to determine why workers rob other employees of their money or personal effects; without entering into personal motives which cannot be easily generalized, one possible explanation is that the theft of money and/or personal effects is mainly a *crime of opportunity*. This issue will be analysed in detail in Part III.

The questionnaires also report cases of extortion and the corruption of employees.

Corruption requires brief analysis. Bribery and corruption are synonymous and they refer to the same practice: a bribe is a sum of money offered to obtain a decision or an action in favour of the giver; that is, someone pays a bribe in order to corrupt someone else.

Although there is broad agreement that bribery and corruption obstruct free and fair competition, they are a normal part of international transactions. The fact that corruption is explicitly or implicitly illegal in a large number of countries does not seem to be a problem. It is obvious that this is a particular vulnerable point in the development of both the public and private sectors.

As regards the latter, companies usually consider corruption to be a 'business necessity' and a 'local practice',[32] justifying their conduct in these terms. Sometimes involved is 'grand corruption' (large bribes paid to ministers or top officials, for example), and sometimes 'petty corruption' (small bribes for junior officials), but the results do not change.

Aside from the economic, legal and political consequences of bribery and corruption, the point is that these crimes may also victimize companies: although companies are often 'corrupters', it is not rare for them to be 'victims' as well. There is a substantial body of evidence that companies which 'tolerate' corruption abroad by their employees put themselves at risk. The company may find that also its employees have been corrupted. Not surprisingly, the four main forms of unethical behaviour among top management are conflict of interest, illegal kickbacks, misuse of proprietary information and inequitable treatment of suppliers and contractors.[33]

As regards **Information and Communication Technologies**, one of the features that emerge from analysis of the questionnaires is the widespread nature of crimes and infringements against them. As already said, the term 'Information and Communication Technologies' is used in this Report to refer to all an organization's software and hardware components that contribute to performance of useful and/or critical functions.

This feature confirms the already seen characteristics of these crimes:

- crimes against ICT are common to all business sectors, even to companies which are essentially routine-work based;
- they involve hardware, as well as software and networks.
- As regards the former, the number of reported stolen laptops, for example, is significantly high. Also of particular interest is the frequency of web site home page defacement and of denials of service (DoS), especially distributed (dDoS). On the contrary, the questionnaires report only few cases of cyber-terrorism;
- are committed both within and without the company. The questionnaires, in fact, report cases of illicit computer penetration by outsiders as well by insiders, together with the disclosure and use of passwords by employees. Also very common are computer viruses, sent from outside and/or downloaded during internal surfing. In many cases, internal users are mainly responsible for virus-

[32] National Integrity Systems, The TI Source Book. Part B: Applying the Framework. Chapter 13: the Private-Corporate-Sector. The text is available at the following URL: http://www.transparency.org/documents/source-book/b/Chapter_13/index.html.

[33] Results of the Survey on Business Ethics, commissioned by the ICAC of Hong Kong, March 1994.

related damage which is generally due to the carelessness of computer users and their ignorance of new technologies. For example, e-mail attachments are frequently not pre-scanned using anti-virus software before they are opened, or else anti-virus software and firewalls are not properly set. This means that preventive technological measures and internal ICT policies become wholly ineffectual;
- often affect some of the most important company assets: data and information.

Together with crimes and abuses against human resources and information technologies, the questionnaires also indicate a large number of crimes affecting the **production line** and **products**. To be stressed is the incidence of thefts of products (during the manufacturing process and from warehouses), and counterfeiting.

Some companies have also experienced sabotage, vandalism and terrorist acts/diffusion of subversive materials. Unfortunately, they do not always state the number of cases, so that it is difficult to establish whether the private sector is effectively at risk of these kinds of crimes. The political and economic situation both national and international gives rise to some concern, but it does not warrant creating a situation of undue alarm and suspicion. Rather, companies should be made aware of their vulnerability so that they increase and adapt their countermeasures.

As regards the role of **organised crime**, the available information and figures provided by the questionnaires do not indicate that this is significantly affecting the legitimate private sector. Only one of the companies interviewed reported – over the previous two years – two cases of business relationships with other subjects/companies involved in criminal activities, such as money laundering. This apparent absence of organised crime related crimes may be due to various factors. First, there is a problem of definition: companies usually consider organised crime to consist of traditional and familiar groups like the Mafia. In reality, organised crime has rapidly changed from hierarchical and monolithic organisations to smaller, decentralised and flexible structures.[34] As Europol has pointed out,[35] in Europe the main trends in organised crime are the following:

- organised crime is undergoing structural change into smaller organisations, often linked together transnationally by mutual understandings and agreements; most organised groups are not of Mafia type and they tend to be more structured as criminal enterprises;
- for the purpose of exploiting the opportunities provided by globalisation and the ICT revolution, organised crime is rapidly recruiting professionals in order to acquire a higher level of expertise. This gives it access to the legitimate market, while minimising the risks of detection;
- although organised crime still profits from its traditional and highly lucrative activities like trafficking in drugs and human beings, it is also moving into more profitable but less risky ones like large-scale fraud, environmental crimes, counterfeiting and piracy, and the smuggling of tobacco and alcohol products.

[34] Adamoli S., di Nicola A., Savona E. U., Zoffi P., *cit.* 9.

[35] Europol, *EU Organised Crime Situation Report*, The Hague, February 2000.

Moreover, in Europe an important role is played by non indigenous groups; the criminal threat from Central and Eastern Europe is viewed with particular concern by the Member States. According to Europol, 'Central and Eastern Europe countries are increasingly mentioned as depots for drugs and illicit commodities and as logistic bases for O.C. groups impacting upon Member States'.[36] Their impact on Europe is twofold: on the one hand, these organised groups invest huge financial resources in Europe to launder money and set up apparently legal businesses. On the other, they are becoming more active in the commission of crimes in Europe, interacting or competing with native groups. In particular, a major cause for concern are Albanian, Turkish, Moroccan, Nigerian and Arabian groups.

Owing to the presence of different groups and competition among them, violence and violent crimes are predicted to increase in the EU. Moreover, as well as fraud and forgery, money laundering is expected to grow more sophisticated and complex due to the involvement of professionals like lawyers, accountants and financial consultants.

Given the complexity of organised crime, it is difficult to determine whether businesses are effectively at risk; however, considering that the threats do exist, the diffusion of information is indispensable to increase company knowledge and awareness.

To return to analysis of the questionnaires, what do they reveal about the consequences of the crimes experienced? The questionnaire asked the respondents to indicate how the crimes reported had affected the company. The results follow (in decreasing order).

- *property damage* and *waste of time* (5 out of 9[37] respondents);
- *loss of information* and *damage to image/reputation* (4 out of 9 respondents).

To be noted is that 3 out of 9 respondents also ticked *increase of insurance premiums* while 2 out of 9 did so for *loss of market share*.

The fact that *sense of distrust among employees* was indicated by only one respondent is noteworthy; perhaps still too little attention is paid to employees' reactions to criminal episodes affecting the company for which they work. However, as will explained later, the workplace climate is extremely important, not only for enhanced company productivity but also for crime prevention. Managements should therefore pay particular attention to the sense of distrust or insecurity among employees.

The following sub-section deals with the **perpetrators** of the criminal episodes recorded over the previous two years. The company interviewed was first asked to indicate the number of persons involved, and by replying to different questions, to reconstruct an overall profile (insider or outsider, individual or organised group, sex, average age and educational level, period of employment, factors with an impact on the occurrence of crimes, motives, and computer technologies used, if any).

---

[36] Europol, *cit.* 35, p. 9.

[37] Considering that - as said - the company had not experienced crimes in the last two years, case 7 did not reply to this question. The sample thus consists of 9 respondents rather than 10.

It must be said that the results on this point are entirely unsatisfactory; they reveal that companies have only imprecise and vague knowledge about the subjective profile of the criminals who targeted them. One plausible explanation is that companies do not have the requisite information. Yet it is difficult to understand, for example, why they indicated the number of criminals involved – thus showing a certain acquaintance – but gave no information on the other related features of perpetrators, saying for example whether or not they were insiders.

The following analysis therefore considers only the questionnaires which were complete and reliable; the others will be considered only with reference to information of particular interest to this study.

Case 1: *Business risk consultancy*

Before entering into details, it should be specified that this company had not been victimised by a high number of crimes in the previous two years; as said, the crimes that did occur mainly affected human resources and information technologies.

According to the replies given, perpetrators were both insiders and outsiders: in the former case, they were mainly *employees*, in the latter they were *individuals*.

As regards sex, average age and educational level, the criminals were *female*, aged between *25 and 35*, and possessing *secondary school diplomas*.

It is interesting to note that the insiders had been working for the company *for between 1 and 3 years on average*.

One of the factors indicated by the interviewee as having the greatest impact on the occurrence of crimes was a *lack of internal control*.

Insiders were motivated by *profit*, while there was no indication as to the outsiders' motives.

Finally, the technology used in criminal cases recorded over the previous two years was *e-mail*.

Case 2: *Financial services*

As regards the amount of crimes, the questionnaire reports 175,000 cases of financial fraud over the previous two years.

Accordingly, the perpetrators were both *insiders* and *outsiders*; the former were *employees*, while the outsiders were *organised groups*. Unfortunately, there is no information about the profile of these perpetrators, although it is important to stress that the employees had been working for the company for *over 10 years*.

The factors with the greatest impact on the occurrence of crimes were:

- *management override of internal controls*;
- *high risk field of activity*,
- *factors external to the company*.

Brief discussion is required of the *high risk field of activity* as a factor which may have had a major impact on the occurrence of crimes. Is there, one may ask, a significant relationship between the economic sector in which the company operates and the types of crime to which it is exposed? A useful and authoritative source of information with which to answer this question is the *European Economic Crime Survey 2001* conducted by PricewaterhouseCoopers. [38]

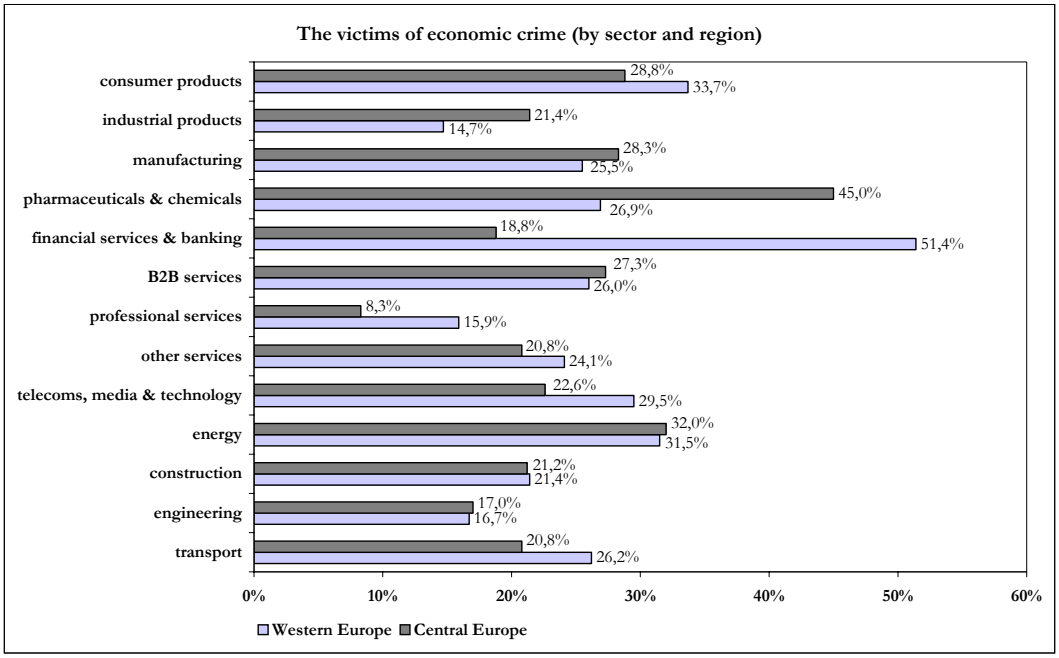
One of the most interesting parts of this survey deals with the relationship between victimisation and industrial sector. Although there are no significant differences, it should be stressed that financial services are the sector at greatest risk. The figure below shows victimisation according to industrial sector and geographical region.

That banks and financial services providers are significantly vulnerable to criminal risk does not depend solely on the fact that they 'manage' money and are therefore at '*greater inherent risk'.* The other important factor is that they operate in a closely regulated sector and for this reason have heightened awareness of the problem. The fact that they are strictly controlled also means that they (should) have developed a prevention and control system which enables them to detect and report a higher number of fraudulent activities. The financial industry should consequently have deeper knowledge of criminal dynamics and possible risks, and this should lead to their greater success in the fight against economic crime also reflected in the larger number of cases reported. This consideration cannot be generalized, however: it is well known that Western European companies are subject to stricter regulation and controls than Central European ones.

The reverse is the case of pharmaceuticals and chemicals. This economic sector is more exposed to economic crime in Central Europe than in Western Europe. The most frequent offences are corruption and infringements of intellectual property rights - product piracy and patent theft included.

[38] PricewaterhouseCoopers, *European Economic Crime Survey 2001*, 2001, p. 5.

Figure 4



Source: PricewaterhouseCoopers, *European Economic Crime Survey 2001*.

To return to the case-study analysis, the criminal motives indicated by the interviewee were the following:

insiders: *profit-making*. *High life style* was added by the compiler;

outsiders: the only reason indicated was *profit*.

There was no indication of the technologies used, if any.

Case 3: *manufacturing*

As already said, over the previous two years this company had experienced a high crime rate affecting all the assets specified: production line and products, human resources, information technologies, know-how and money/capital.

Although the questionnaire was carefully completed in all its parts, it is not possible to draw up a precise and unique profile of the perpetrators, because of the high number and heterogeneity of the crimes reported. However, this not to imply that the information was useless; on the contrary, this case is important because it is representative of the project's principal assumptions: namely that business crimes committed within companies are mostly *crimes of opportunity*, and that they are committed by a wide range of subjects, within and without the company, at all levels, according to the means available and opportunity. This issue will be analysed in detail later.

In confirmation of this, the replies to the questionnaire indicated that the insider perpetrators were *employees*, but also middle and senior managers. External perpetrators were both individuals and organised groups.

This case highlights another important feature: *collusion*. In fact, according to the information provided by the questionnaire, the number of perpetrators involved in the crimes detected was always *more than 3 persons*.

This confirms that the distinction between internal and external crimes is not clear-cut, and that it is mainly a classification criterion: the two categories are closely interconnected, especially because most fraud is collusive. There is therefore a third type of particular importance, what we may call *collusive* fraud.[39]

Collusion can be defined as an agreement between two or more people to commit a dishonest act. Within a company, it may take place from the inside towards the outside (between insiders and outsiders), as well as among insiders. Moreover, it can be organised at different levels and take different forms:

Collusion can be classified into two main levels:

- minimum collusion. Collusion is minimum when it does no more than provide the necessary opportunities, resources and/or skills for commission of the crime; this pattern usually involves links among perpetrators of high-skilled fraud: these kinds of crimes, in fact, usually involve only a limited number of people because they are so complex that only those with specific expertise can understand them. Moreover, they are based on as few contacts among the fraudsters as possible in order to protect them against the risk of discovery.
- maximum collusion. Collusion is maximum when the perpetrators share the proceeds of low-skill fraud among the maximum number of people, usually in order to ensure their silence. Low-skill fraud, in fact, usually involves a high number of co-workers, especially at low level, and it is mainly based on simple criminal conspiracies. This internal, horizontal collusion reduces the risk that one thief/fraudster will inform on another.

Collusion can be classified into the following types:

- passive. A person not involved in the fraud becomes aware of its occurrence but says nothing;
- negligent. A person realizes that his/her failure and/or omission has made it possible for a fraud to be committed but does or says nothing;
- supportive. A person knows that a fraud/crime is being committed in his/her area of responsibility but decides to do nothing;
- committed. A person takes active part in the fraud/crime.

The data on sex, age and educational level show that offenders were both *male* and *female*, aged mainly between *18 to 35* and covering almost all educational levels: *elementary school certificate*, *secondary school diploma* and *university degree*.

Insiders had been working for the company for an average of between 1 and 3 years.

---

[39] For detailed analysis of crime collusion in the business sector see Comer M. J., *cit.* 6, p. 30.

According to the questionnaire replies, the factors with the greatest impact on the occurrence of crimes were the following:

- *management override of internal controls;*
- *lack of managerial control over outsourced services;*
- *high field risk of activity;*
- *factors external to the company;*
- *employees and third party collusion;*
- *existence of parallel markets;*
- *socio-political situation (social instability, high crime rate)*.

As regards motives, the compiler ticked the following:

insiders: *profit*, *covering-up of possible mistakes or omissions*, *personal discontent*;

outsiders: *profit*.

In this case, too, *e-mail* was the technology most frequently used.

Case 4 - *Petroleum and petrochemicals; Chemicals*

Over the previous two years this company had most frequently experienced crimes against the production line and products, human resources and information technologies. In particular, vandalism by outsiders and the theft of money/personal effects and laptops were indicated as the most numerous.

Unfortunately, the questionnaire was not compiled in its entirety, so that it is not possible to reconstruct the subjective profile of the perpetrators.

The information provided concerns the factors with the greatest impact on the occurrence of crimes and the technologies used. As regards the former, the factors indicated were:

- *lack of managerial control over outsourced services*;
- *factors external to company*.

Interestingly, in this case the technologies used to commit the crimes were not only *e-mail* but also the *Web*, while the technique indicated was *file removal*.

Case 5 - *TLC*

Like case 3, this one is particularly significant because it concerns a company frequently victimised over the previous two years. The assets damaged were: production line and product, human resources, information technologies, know-how and money/capital.

Although the questionnaire did not give precise figures on the crimes experienced, the information about perpetrators was extremely detailed and consequently of great interest.

For example, the replies enabled a relationship to be established between the number of perpetrators and the types of assets damaged. The following chart schematises the findings.

	1	1-3	>3
manufacturing establishments		√	
facilities/equipment/plant		√	
Information Technologies			√
human resources	√		
process know-how	√		
image/reputation	√		
customer relations	√		
partnership with vendors	√		
money/capital		√	
raw materials	√		
semi-finished products	√		
finished products		√	

It is interesting that other questionnaires indicated crimes, abuses and attacks against information technologies as generally committed by more than three persons. However, a lack of precise information on specific cases makes it difficult to find a possible explanation for this phenomenon; nor is it possible to determine whether ICT crimes are actually committed by groups of people rather than by individuals, or whether it is a company perception based on the fact that these kinds of crime require a high level of expertise, so that it is more likely that they are perpetrated by more than one offender.

According to the questionnaire, when crimes were committed by insiders, the perpetrators were usually *employees*. When they were committed by outsiders, the perpetrators were individuals.

Moreover, the offenders were mostly *male*, *aged between 25 and 35*, with *elementary school certificates*.

As in case 3, the employees had usually had a long relationship with the company: in fact, on average, they had been working for it *for between 3 and 10 years*.

The factors with the greatest impact on the occurrence of crimes were the same as those in the previous cases:

- *lack of managerial control over outsourced services*;
- *high risk field of activity*;
- *factors external to the company*;
- *organised crime infiltration (company infiltrated by organised crime)*.

The last factor is of particularly importance, given that – as said – identification of the criminal dynamics involving organised crime in the business sector is one of the main objectives of this Project. It is accordingly important to specify that only two out of nine questionnaires (the second being case 6) indicated organised crime infiltration as a factor impacting on the occurrence of crimes experienced.

The completed questionnaire cited the following motives for the crimes committed against the company:

insiders: *profit* and *personal discontent*;

outsiders: *profit*.

The technological instruments used were mainly *e-mail* and the *Web*.

Case 6 – *Transport*

Over the previous two years this company had experienced a huge number of crimes, and targeted on the following assets in particular: production line and product, human resources, information technologies and money/capital. To be emphasised is the significant number of thefts – within and without the company – and frauds, especially financial.

According to the information provided by the questionnaire, *employees* were the most recurrent category of internal offender, while outsiders were mainly *organised groups*.

Perpetrators were mainly *male*, aged between *18 and 35*, with *elementary school certificates*.

As in some of the cases already analysed, they had been working for the company for between *3 and 10 years*.

The questionnaire indicated the following factors as exerting the greatest impact on the occurrence of crimes:

- *management override of internal controls*;
- *high risk field of activity*;
- *employees and third party collusion*;
- *organised crime infiltration (company infiltrated by organised crime)*.

The perpetrators' motives were:

insiders: *profit*;

outsiders: as well as *profit*, the interviewee added *political reasons*.

This detail warrants reflection. To sum up the principal information provided by the questionnaire, external perpetrators are mainly organised groups, often motivated not only by profit but also by ideology; their threat to corporate security and productivity must be serious, considering that organised crime infiltration is indicated as one of the factors with the greatest impact on the occurrence of the crimes experienced over the previous two years. However, traditionally, political goals are not among the main concerns of organised crime. It consequently seems likely that since the company operates world-wide, it is not victimised by traditional organised crime but by local groups seeking to gain visibility and political outcomes by attacking multinational companies.

The *Web* is the technology used.

Case 7 – *Recruitment services*

This case is of particular interest: although the company's crime rate over the previous two years had not been particularly high, according to the questionnaire the crimes experienced were all committed by insiders, and specifically by employees.

As regards the profile of perpetrators, they were mostly *male*, aged between *18 to 25*, but also *female* and aged between *25 and 35*. They all possessed *secondary diplomas* and had worked for the company for between *1 and 3 years*.

The factors with most impact on the occurrence of crimes were:

- *factors external to company*;
- *employees and third party collusion*.

According to the compiler, there was only one motive for crimes committed: *covering-up possible mistakes or omissions*, with computer technologies being mainly used to *remove files*.

Case 8 – *Textiles, clothing, cork, real estate, tourism, insurance, capital development.*
Not applicable

Case 9 – *TLC mobile*
Over the previous two years, this company had been the victim of crimes against the production line and products, human resources, information technologies and money/capital. The number of crimes was not stated by the completed questionnaire.
This case is particularly interesting because it furnishes information and details not present in the previous questionnaires, so that this company's situation is somewhat singular. On the basis of the information provided, one gains the impression that the company was the victim of an outright criminal conspiracy, whose perpetrators operated both within and without the company.
The profiles of the perpetrators are as follows: the insiders were mainly *employees* and *middle managers*, while the external subjects were *organised groups*.
They were both *males* and *females*, aged between *18 and 25*, with *secondary school diplomas*. As regards the employment relationship with the company, this is the only case where it was quite recent: in fact, the perpetrators had been working for the company for between *6 months and 1 year*.
Moreover, from the list of factors with greatest impact on the occurrence of crimes, the compiler indicated *collusion between top managers and employees* and *employees and third party collusion*.
The insiders damaged their employer for the following reasons: *personal discontent* and *gambling debts*. External subjects were motivated by *profit*.
As regards technology, most frequent use was made of *e-mail* but also the *LAN.*

Case 10 – *manufacturing*

As in the majority of the other cases, over the previous two years this company had experienced crimes against almost all the assets specified. This case is also quite interesting as regards the profile of the perpetrators, especially because the information is detailed.
According to the questionnaire, the offenders were mainly insiders, and specifically *employees*.
The following tables reconstruct the perpetrator profile according to sex, age and educational level.

age	male	female
under 18	0	
18 to 25	20%	
25 to 35	20%	
35 to 50	50%	
over 50	10%	

educational level	male	female
elementary school certificate	60%	
secondary school diploma	35%	
university degree	5%	
Master's degree	0	
other	0	

Interestingly, according to the questionnaire, these insiders had been working for the company for a short period of time: *less than six months*. However, this information seems unreliable, especially if compared to the data in the previous tables: considering that offenders were mostly people aged between 35 and over 50 and generally had elementary school certificates, and given that the company also engaged in work-based production line activity, it is difficult to consider these perpetrators as relatively recently hired employees.

The questionnaire singles out the company's *high risk field of activity* as the factor with greatest impact on the occurrence of crime, while the most frequent motive for committing a crime was *profit.*

In this case, too, the computer technologies most frequently used was *e-mail*.

On the basis of the findings already schematised, this analysis of the subjective profile of the offenders concludes with the following considerations.

- The replies given by the companies interviewed were not always convincing; they were very often contradictory or not exhaustive, so that the analysis of the findings was very difficult. This may have been due to the complexity of the questionnaire's structure, which was extremely detailed; but it was also probably due to the lack of precise information on these issues. However, it is important that companies should collect detailed information about both the subjective characteristics of offenders and their *modi operandi*. It will thus be possible for them to develop specific preventive measures which enable them to monitor and

protect corporate assets while reducing the risk of crime and the related damage.

- With regard to insiders, almost all companies indicated '*employee'* as the most recurrent profile. This result seemingly confirms the general rule that crimes committed by high-status employees, such as middle and senior managers, are extremely difficult to detect, although this does not mean that they are less numerous than those committed by employees. Management organization and role is therefore one of the key aspects to be taken into account by companies when they consider security and crime prevention. This is also confirmed by the finding that one of the factors with the greatest impact on the occurrence of the crimes experienced was management responsibilities (*management override on internal controls* and *lack of managerial control over outsourced services* were among the reasons most frequently cited).
- As regards insiders, a further important factor is how the company manages human resources. For example, almost all the compilers cited *profit* as the most frequent reason for the commission of crimes and abuses against the company. However, this seems to be an oversimplification. It is more likely that there are other causes besides greed, ones also related to or determined by the business environment. in fact, some of the interviewees indicated *personal discontent* or *gambling debts* as well. Moreover, *retaliation* and *revenge* should not be underestimated. Companies should therefore pay closer attention to the workplace climate and its internal dynamics, starting from the premise that fair and correct human resources management is as important as physical security measures like alarm systems.

S – Security measures

This section of the questionnaire collected information about the company security level, focusing on both the internal and external environment. This information was then enriched with the personal perceptions, observations and remarks of the interviewees collected by Part III of the questionnaire.

The findings of this section are of particular importance because they provide a general overview of how companies consider security-related issues and risks, and how they manage them in practice. In other words, having identified the crimes most frequently committed and – when possible – the profiles of their perpetrators, the focus is now on the company and on the environment in which it operates, the purpose being to clarify the most recurrent criminogenic factors and how companies react to them.

The first question is quite general but, as will be explained, is essential to the purpose of this research:

Does the 'security issue' in any way influence the organisational model of your company?

Yes	6 out of 10 questionnaires
No	4 out of 10 questionnaires

The purpose of this question was to determine the company's approach to security-related issues, starting from the assumption that security in general, and precise knowledge of existing security problems in particular, are essential and should pervade all business functions and departments. In other words, security is not merely a matter of risk management and assets protection; on the contrary, it should be a fundamental component of the entire business plan.

The fact that only 6 out of 10 respondents cited security as an issue influencing the company model confirms that companies have not yet understood and/or adopted this perspective; security is still considered to be one of the business functions (mainly of concern to the Security Division, when it exists), and, most of all, it is still handled by taking an emergency-coping approach: it does not prevent incidents; it only helps in handling the *ex post facto* situation.

As regards the presence of external factors impacting on the crime rate, 5 out of 9[40] respondents did not think that the social-political situation of the host country (or countries) affected the incidents reported. However, it is important to point out that the most frequent replies in the four other cases were the following:

- *political instability* and the presence of *organised crime* (respectively, 3 out of 4 respondents);
- *ordinary crime* and *rate of corruption* (respectively, 2 out of 4 respondents)

Moreover, at least one of these four respondents also indicated one of the following factors: *malfunctioning of institutions*, *strong pressure and political influence on the company*, *inefficient judicial system*, *social unrest*.

By contrast, as regards the possible impact of economic factors (affecting both the company and/or the host country) on the occurrence of crimes, there was general agreement that these were not relevant. Only one respondent disagreed and specifically cited the *recession of the country* and its *high unemployment rate* as significant factors.

Therefore, of external factors, criminality was generally viewed with particular concern by businesses.

The following findings concern the internal factors, and in particular the preventive measures, regularly implemented within companies. The replies are somewhat surprising: according to the information collected, in fact, the companies interviewed should be absolutely 'secure', given that they had already implemented almost all the security measures indicated in the questionnaire. On average, all the companies had implemented at least 10 to 15 of the 22 measures specified.

The following table lists these measures in decreasing order; multiple choice was possible. The number of companies implementing each measure is also stated.

[40] Case 8 did not report any crimes over the previous two years. Hence this question – as well as the next – were not applicable.

SECURITY MEASURES REGULARLY IMPLEMENTED IN THE COMPANY	NUMBER OF COMPANIES
corporate code of conduct strengthening of internal controls internal auditing adequate physical security systems	9 out of 10
corporate policy for the use of new technologies	8 out of 10
thorough internal controls reference checks and screening of new employees established anti-fraud policy	7 out of 10
anti-fraud training courses for personnel reference checks and screening of employees earmarked for particularly sensitive appointments codes of conduct for contractors and suppliers a horizontal control system (separation of responsibilities) a company department specialised in security problems	6 out of 10
information on customer solvency a database on crimes experienced	5 out of 10
checks on managers by the administration increased focus of senior management on the problem internal surveillance resources an anonymous system of incident reporting	4 out of 10
rotation of staff at risk	3 out of 10

To be emphasised is that only one company added *access control* to the list of security measures.

Moreover, the table confirms some of the previous observations. As regards, for example, the hypothesised lack of information about criminal risks and crimes suffered, the table confirms that a company department specialised in security problems was present only in 6 out of 10 companies, while only 5 companies had a database of information on crimes experienced.

In addition, crimes committed by managers went largely undetected because there was a general lack of controls over their work; indeed, only 4 out of 10 companies conducted checks on managers. Moreover, as regards the role of top management in security organization, 'increased focus of senior management on the problem' was chosen by only 4 out of 10 companies.

Considering that, as seen in previous sections, different types of crimes had affected the companies interviewed over the previous two years, the conclusion is that these measures are not infallible. Consequently, the next question was: *in the case of crimes you remember over the last two years, what precautionary actions could have prevented the illicit events from occurring?* Multiple choice was possible. The following table schematises the findings.

PRECAUTIONARY ACTIONS THAT COULD HAVE PREVENTED THE ILLICIT EVENTS FROM OCCURRING	NUMBER OF COMPANIES
awareness strategies (corporate code of conduct, internal policies, anti- fraud training courses for personnel)	5 out of 10
preventive measures at the point of engagement (reference checks and screening of new employees)	4 out of 10
physical security measures (alarm system, internal surveillance resources, investment in third party surveillance)	
early warning preventive strategies (thorough internal controls, an anonymous system of incident reporting, a database on crimes experienced, internal auditing)	3 out of 10
corporate governance measures (checks by the administration on managers, a system of horizontal control, separation of responsibilities, reference checks and screening of employees earmarked for particularly sensitive appointments)	2 out of 10
preventive measures applied to external commercial partners (information on the solvency of customers, code of conduct for contractors and suppliers) deterrent measures (established anti-fraud policy)	1 out of 10

5 out of 10 companies considered *awareness strategies* (corporate code of conduct, internal policies, anti-fraud training courses for personnel) to be measures that could have prevented the crimes experienced from occurring. Yet, considering that awareness strategies can work effectively only if they are based on realistic and precise knowledge of what is happening in the company environment, in a certain sense this reply confirms one of the most important premises of this research: that the business sector should collect more data and information on its vulnerabilities and develop specific analysis in order to implement adequate strategies for the prevention and control of crime.

Interestingly, together with awareness strategies, 4 out of 10 companies chose other two groups of measures as well: *preventive measures at the point of engagement* (reference checks and screening of new employees) and *physical security measures* (alarm system, internal surveillance resources, investment in third party surveillance).

Considering that *early warning preventive strategies* (thorough internal controls, an anonymous system of incident reporting, a database on crimes experienced, internal auditing) and *corporate governance measures* (checks by the administration on managers, a system of horizontal control, separation of responsibilities, reference checks and screening of employees earmarked for particularly sensitive appointments) are not given particular consideration, it can be concluded that companies still prefer traditional security measures and systems. In a certain sense, it seems that companies are aware of the possible criminal risks – also posed by insiders – but they do not want to consider them so dangerous to react in a direct and pervasive way. The fact that they consider policy, codes and training courses to be the most effective preventive measures, together with the strengthening of physical security measures, is symptomatic.

This interpretation of the findings is confirmed by the replies to the following questions: *which of the following preventive measures were implemented after the crime had occurred?* Multiple choice was possible.

SECURITY MEASURES IMPLEMENTED AFTER THE CRIME HAD OCCURRED, OVER THE PREVIOUS TWO YEARS	NUMBER OF COMPANIES
awareness strategy (corporate code of conduct, internal policies, anti- fraud training courses for the personnel)	5 out of 10
physical security measures (alarm system, internal surveillance resources, investment in third party surveillance)	4 out of 10
preventive measures at the point of engagement (reference checks and screening of new employees) preventive measures applied to external commercial partners (information on the solvency of customers, code of conduct for contractors and suppliers) early warning preventive strategies (thorough internal controls, an anonymous system of incident reporting, a database on crimes experienced, internal auditing)	3 out of 10
deterrent measures (established anti-fraud policy) corporate governance measures (checks by the administration on managers, a system of horizontal control, separation of responsibilities, reference checks and screening of employees earmarked for particularly sensitive appointments)	2 out of 10

Awareness strategies and physical security measures were the measures most frequently chosen, while corporate governance was still regarded as a marginal solution. Whereas the former require only general action, such as codes and/or occasional training, which remain at a superficial level while responding to a momentary need for intervention, the latter entails a totally different approach involving all the company's functions. Senior and middle managers should always treat security as an essential component of every decision-making process, even when the decision is not directly related to security problems. Moreover, corporate governance measures require a particular kind of internal organisation: human resources management – at all levels of the company hierarchy – should be designed with close attention paid to internal environment and should involve constant controls.

In the light of the findings of this case-study analysis, the inevitable conclusion is that companies are not still ready to consider security in these terms. The replies to this question confirm that, as already said, security is based on an emergency-coping approach. Another finding which supports this interpretation is that after the occurrence of crimes, only 3 out of 10 companies implemented preventive measures at the point of engagement, preventive measures applied to external commercial partners, or early warning preventive strategies. Another surprising feature is the almost total lack of interest in deterrent measures, chosen by only 2 out of 10 companies.

This approach seems to only be used with reference to security related issues; in fact, almost all the companies had monitoring systems for other types of risk, such as financial risk (9 out of 10 companies), currency risk (8 out of 10 companies), but also computer and country risks (7 out of 10 companies, respectively).

Starting from the consideration that corporate governance is of major importance for the prevention of crime, the questionnaire sought to gather information on its implementation in the business environment, asking which of the measures listed were implemented in the company. The following table schematises the findings. Multiple choice was possible.

MEASURES OF CORPORATE GOVERNANCE IMPLEMENTED IN THE COMPANY	NUMBER OF COMPANIES
compiling of periodic internal statements of accounts	9 out of 10
system of periodic reporting to shareholders	8 out of 10
frequent and accurate social communication	7 out of 10
instruments measuring management performance incentives for employees to become company shareholders presence of an external firm of auditors	6 out of 10
balancing of powers measures discouraging unethical behaviour by directors and managers	4 out of 10

According to these results, companies believe that, unlike employees, senior and middle managers do not commit crimes; moreover, from a criminal point of view, the first three groups of measures are entirely ineffective in terms of crime prevention and deterrence.

- The great majority of documents, accounts and financial records in general can be easily forged and falsified; therefore, they are not reliable evidence.
- Moreover, these documents are generally trusted because they are mostly prepared by middle and senior managers who enjoy the respect of almost all superiors, who seldom mistrust them. The problem is that this is a conventional arrangement which misrepresents reality: according to the 1996 Report to the Nation on Occupational Fraud and Abuse, published by ACFE[41], 58% of the reported frauds and abuses were committed by non-managerial employees, 30% by managers and 12% by owner/executives. However, as explained by the analysts, the median losses caused by non-managerial employees were significantly lower than those caused by managers and executives. Specifically, losses related to managerial fraud were 16 times more numerous than those caused by non-managerial employees. This situation is reconfirmed by the 2002 Report to the Nation edition[42]: frauds by managers and executives cause median losses of $250,000, which is about 3,5 times as high as losses associated with frauds committed by rank and file employees. Apart from the trust relationship, the problem is that crimes by high-level employees are more difficult to detect

[41] ACFE, *1996 Report to the Nation on Occupational Fraud and Abuse*, 1996. The executive summary is available at the following URL: http://www.acfe.org.

[42] ACFE, *cit.* 8.

because they are generally more complex and sophisticated, due to the fact that these employees have a greater knowledge of, and closer control over, company assets.

- There are also cases of collusion between employees and managers; collusion is difficult for companies to prevent and discover because it involves precisely those persons who are expected to identify fraud among employees and to deter crime by means of their supervisory functions.[43]

It is clear from these considerations that the above-mentioned corporate governance measures have no concrete utility or impact on the prevention of crime. Likewise, the presence of external accounting firms does not seem to provide sufficient guarantees; the recent Elron and Worldcom scandals are symptomatic.

To be noted is that only one company added another measure of corporate governance to the list given, one that is extremely important: reporting on corporate security. This partly confirms that security related information does not circulate within companies, which reduces awareness among both management and employees.

The generic lack of controls evidenced by the findings applies not only to managers and executives but also to employee management, as confirmed by the replies to the question: *which of the following personnel management measures have been implemented in your company?* Multiple choice was possible.

As the following table shows, the great majority of the companies interviewed rely simply on general policies with specific regard to personnel recruitment and training. Surprisingly, policies to promote employee loyalty and those rewarding ethical behaviour are the least implemented.

PERSONNEL MANAGEMENT MEASURES IMPLEMENTED IN THE COMPANY	NUMBER OF COMPANIES
recruitment policies training policies	9 out of 10
career planning policies	8 out of 10
monitoring policies	7 out of 10
counselling policies	6 out of 10
policies promoting the loyalty of employees	5 out of 10
policies rewarding ethical behaviour	3 out of 10

In order to determine whether companies are aware of the fact that, in most cases, crimes are preceded by early warning signs which can be used to organise more effective preventive strategies, question number 38 asked: *in cases of crimes you remember have you ever recorded (also subsequently) elements or signals indicating the occurrence of the event?* Multiple choice was possible.

[43] As explained in the 2002 Report to the Nation on Occupational Fraud and Abuse edition "*when managers participate in fraud along with their employees, this serves to disrupt a major component of internal control and creates a much higher level of vulnerability for the victim organisation*". ACFE, *cit.*8, p. 14.

The following table reports all the early warning signs listed in the questionnaire, indicating the ones most frequently ticked and the number of preferences.

RECORDED EARLY WARNING SIGNS INDICATING THE OCCURRENCE OF CRIME	NUMBER OF COMPANIES
absenteeism	4 out of 10
small shortages of cash lifestyle in excess of pay mistakes or alterations in accounting recordings	3 out of 10
small shortages in inventory records alarm systems out of order false statements concerning topics of little importance	2 out of 10
employees with long periods of unused paid holidays atypical behaviour of employees	1 out of 10
lack of co-operation of employees questioned about their tasks/ duties	
sharp increase in rejects	
employees systematically coming into work before the established starting time and leaving long after closing time	
financial business operations with unclear competitive/income purposes	
release of information only after insistent requests	
frequent company changes	
employees with drug or alcohol related problems	
exaggerated employee mobility	
climate of discontent among employees	
unclear relationships between employees and vendors/ customers	
excessive careerism of some employees	

These findings are particularly interesting; unlike the replies to the previous questions, not all the companies interviewed could indicate the early warning signs of crimes. This confirms that there is a general lack of concern for, and direct controls over, internal human resources. In fact, as will be explained in detail in the following sections, early warning signs are generally not used in the business sector as vital components of an effective crime prevention strategy.

This is also confirmed by the replies to question number 39. When invited to consider possible ways to pick up early warning signs and/or anomalies, 6 of the 10 companies interviewed suggested *auditing and accounting reviews*, while 5 of them also suggested the *regular monitoring of duties*.

POSSIBLE WAYS TO PICK UP EARLY WARNING SIGNS	NUMBER OF COMPANIES
auditing and accounting reviews	6 out of 10
regular monitoring of duties	5 out of 10
system of anonymous reporting regular staff appraisals internal cross-checks	3 out of 10
periodic performance review in-depth inventories	1 out of 10

These replies do not depict profound understanding and awareness by management of the usefulness of early warnings; moreover, they confirm the existence of a detached and superficial attitude towards the (necessary) implementation of a set of regular control activities. In fact, as results from the previous table showing all the findings, only 3 out of 10 companies used specific methods with a direct impact on human resources management and crime prevention, such as: a system of anonymous reporting, regular staff appraisals and internal cross-checks.

This section of the questionnaire ended with questions on the *ex post facto* situation; specifically, the companies were asked to indicate how they detected crimes, how these crimes were handled, and whether they involved the law enforcement agencies.

The following table schematises the findings on how crimes were detected. Multiple choice was possible.

POSSIBLE WAYS TO PICK UP EARLY WARNING SIGNS	NUMBER OF COMPANIES
notification by employees internal audit review accidental	5 out of 10
information by customers routine internal checks	3 out of 10
checks by employees	2 out of 10
information by supplier deliberate third party checks external audit review notification by police deliberate checks by managers	1 out of 10

These results highlight that companies rely on good fortune where security is concerned, and they also confirm what this Report has repeated many times: security is still not conceived and treated with the requisite attention and the appropriate countermeasures. In fact, despite all the preventive measures that companies say they implement, they still largely rely on chance in the detection of internal fraud and crimes.

This behaviour is confirmed by other surveys and researches, also ones conducted at European level. According to the 2001 European Economic Crime Survey release by PricewaterhouseCoopers, for example, 'respondents suffering from economic crime in the last two years stated that accident had played a role in the detection of 58 per cent of cases'.[44] To provide more precise information, the following table shows how fraud is detected across Europe, according to PricewaterhouseCoopers.

HOW FRAUD IS DETECTED ACROSS EUROPE	
tip off	28%
risk management systems	30%
audit process	32%
change in management	53%
accident	58%

Source: PricewaterhouseCoopers, *2001 European economic crime survey*, 2001.

PricewaterhouseCoopers analysts comment on these findings as follows: 'in many companies, control systems are not geared to the detection of fraud: the risks are often underestimated or simply not recognized. Even where controls do exist, they may be rendered ineffective by management override or by collusion. Thus, it is not unusual for chance to play a role in uncovering wrongdoing'.[45]

We entirely agree with this analysis, for it accurately sums up the current corporate attitude towards security management and crime/fraud detection.

As regards how companies handle crimes once they are discovered, 7 out of 9 respondents cited *notification to the police*, while 6 out 9 also indicated *dismissal* and *internal investigation*. An interesting finding is the scant attention paid to *communication inside the company*: only 3 out of 9 companies decided to inform the workforce about the crimes experienced.

The real relationship between 'crimes experienced' and 'crimes reported' was 'measured' by question 42 of the questionnaire, which asked respondents to indicate which of the crimes listed had been experienced by their company over the previous two years, and which of them they had reported to the police. The interviewees were asked to give the figure.

Only a few respondents did as asked. All the others simply put a mark in the columns, without specifying whether they reported all or some of the crimes experienced. The following analysis therefore considers only the cases in which the respondent gave the figure requested.

Case 1 – *Business risk consultancy*

[44] PricewaterhouseCoopers, *cit.* 38, p. 9.

[45] *Ibid.*

This company had experienced the following crimes:

- theft of money/personal effects of employees;
- computer system penetration from outside;
- Denial of service (DoS) and distributed Denial of service (dDoS);
- damage to computer systems due to computer viruses sent from outside;
- employee abuse of Internet access;
- laptop thefts.

The company only reported the laptop thefts.

Case 2 – *Financial services*

As already said, over the previous two years, this company had experienced 175,000 cases of financial fraud. Of these, 150 were reported to the police.

Case 4 – *Petroleum and petrochemicals. Chemicals*

Considering that this company gave very detailed information, it is schematised in the following table, which reports the number of crimes experienced over the previous two years and the number of them reported to the police.

	crimes experienced	crimes reported
theft of company products in transit	1	1
vandalism by outsiders	20	20
theft of money/personal effects of employees	50	10
defacement of the web site home page	1	0
damages to computer systems due to computer viruses downloaded during internal surfing	1	0
laptop thefts	4	4

There are two interesting exceptions: ICT related crimes were the only types never reported to the law enforcement authorities, and only some thefts of money/personal effects of employees were reported. As regards the latter, the decision to involve the police may often depend – amongst other things – on the economic value of the stolen goods. According to victimisation surveys, people tend not to report thefts to the police if the stolen personal effects are not valuable.

By contrast, it is probable that thefts of company products in transit, vandalism and laptop thefts were all reported because they are usually covered by insurance.

Case 5 – *TLC*

This case is of particular interest because, although the respondent did not give the figures for crimes experienced and reported, s/he stated that none of the crimes experienced had been reported to the police.

However, as in the great majority of the sample, this company indicated 'reporting to the police' as one of the most frequently used measures to handle crimes.

Case 6 – *Transport*

In this case, too, a table helps clarify the information provided by respondents.

	experienced crimes	denounced crimes
theft of company property from warehouses	hundreds	
defacement of the web site home page	1	1
laptop thefts	90	0
financial fraud	hundreds	20

Case 7 - *Recruitment services*

This company had not experienced a significant number of serious crimes over the previous two years; specifically, it had been affected by financial fraud and embezzlement, and had reported only the latter to the police.

These cases evidence that although companies rely on the police, indicating 'reporting to the police' as the most common method to handle crimes, they in practice tended not to report them. The already mentioned PricewaterhouseCoopers survey itself highlights that 'depending on where an organisation is located in Europe, attitudes vary on how a fraud should be dealt with'.[46] Moreover, even organisations which have a policy to report all frauds did not proceed in every case.

PART III - RECORDING OF MANAGERS' PERCEPTION OF SECURITY

S - Security measures

As already explained, the questionnaire ended with questions on the managers' perceptions of business security, and their personal points of view on the risk of crime and possible ways to reduce it.

The fact that not all the interviewees were Security Managers is extremely positive, for it aids understanding of how security is generally perceived within the business sector, also by non-experts.

The findings will be analysed in the order of the questions.

The first question was no. 43: *do you think that investment in security can produce a competitive advantage?*

With only one exception,[47] the answers were unanimous: security investments do produce a competitive advantage.

Moreover, as confirmed by the findings for question no. 44 (*do you think that the security issue is tackled correctly in your company?*), almost all the interviewees (9 out of 10) thought that their company managed security-related issues correctly. Only one respondent indicated 'no'.

Considering that this is a case-study analysis, it is interesting that the only interviewee who *did not know* whether a company which invests in security can have a competitive advantage was the same person who *did not think* that his/her company was treating security issues appropriately, and this despite the fact that

[46] PricewaterhouseCoopers, *cit.* 38, p. 10.

[47] Only one of the interviewees, in fact, chose "*do not know*".

s/he was Head of Internal Audit. Moreover, this person *did not even know* whether the organization's personnel were aware of the real threat of fraud. But most surprising was the fact that when asked to indicate the best way(s) to tackle crime, s/he only answered: *Internal investigation* and *Observance of maximum discretion*.

This case is representative of a negative or confused attitude towards security, which is still considered to be an internal and confidential 'company issue'.

As regards the sense of safety in the company environment, most of the interviewees considered their workplaces to be generally safe. In fact, on a scale from 1 to 5, where 5 is the level of highest concern, 7 out of 10 respondents indicated 1. The other three cases require explanation:

Case 7 – the figure chosen was 2;

Case 8 – the figure chosen was 5; the reasons are explained in the following note by the respondents: 'we consider this issue [physical security] a very important concern for the Company, not because there is a lack of physical safety in any area of activity, but because it is our aim to improve continuously safety and hygiene conditions in all work points';

Case 9 – the figure chosen was 3. This reply is not easy to explain; in fact, none of the questionnaire findings can justify or clarify it. However, it is well known that the individual sense of security, as well as the fear of crime, are very often irrational and are largely independent of the existence of real and perceptible threats of crime. Moreover, they are closely related to a variety of factors which may be external and/or unrelated to the workplace features. In this case, the interviewee considered his/her company to be as risky as the place where s/he lived; therefore his/her sense of fear and/or insecurity was probably connected to elements external to the company.

In order to gain a clearer idea of the respondents' sense of security, the questionnaire asked them to indicate whether they considered their work environment to be more risky or less risky than where they lived, or whether it carried the same risks. The results were as follows :

- 4 out of 10 respondents: SAME;
- 3 out of 10 respondents: LESS;
- 3 out of 10 respondents: MORE.

The respondents were also asked to give their opinion about the most effective methods for the detection of business crimes. The replies as schematised in the following table were extremely interesting. Multiple choice was possible.

MOST EFFECTIVE METHODS TO DETECT CRIMES	NUMBER OF COMPANIES
reporting by employees	**10 out of 10**
review of internal auditor	8 out of 10
information by supplier notification by police routine internal controls	6 out of 10

review of external auditor deliberate checks by managers	5 out of 10
checks on employees information by customers accidental	4 out of 10
deliberate third party controls	1 out of 10
shortfall in company earnings	-

The fact that all respondents indicated *reporting by employees* as the most effective method to detect crime is significant; they all agreed that crime detection and prevention must be developed within their company, and mostly with the help of those who *lived* the company every day. The note added to this question by one of the respondents (case 3) is indicative: that a culture of awareness and concern can be extremely useful, given that 'security is everyone's responsibility'.

It is interesting that together with internal informal control, the company should also invest in formal control countermeasures like review by an internal auditor and routine internal controls.

None of the respondents cited a *shortfall in company earnings*. They obviously understood that this was not a way to detect the occurrence of crimes but just one of the damaging consequences that may arise once the crime has been committed. A consequence that must be prevented.

These answers should be considered jointly with those to the next question, which asked '*what do you think is the best way to tackle crimes?*'. Multiple choice was possible.

BEST WAYS TO TACKLE CRIMES	NUMBER OF COMPANIES
notification to the police civil action for the recovery of damages	8 out of 10
internal investigation	7 out of 10
dismissal disciplinary hearings	6 out of 10
internal communication	4 out of 10
observance of maximum discretion	1 out of 10
request for resignation	-

Like the company, also the respondents viewed the reporting of crimes to the police (together with civil action for the recovery of damages) as the best ways to tackle crime. However, according to the findings, they should be supported by company efforts in the form of internal investigation and severe treatment of perpetrators: when crimes are committed by insiders, the respondents considered dismissal and disciplinary hearings to be the most appropriate company reactions.

To be noted is that only one respondent (case 8) thought that the company's reaction should be proportionate to the type of crime committed.

As regards the corporate environment, the respondents were also asked to indicate if, in their perception, the personnel of their organizations were aware of the real threat of fraud.

The vast majority of them answered in the affirmative (8 out of 10), and one of them (case 3) stressed that the personnel did know that the company was exposed to criminal risks but this was a general perception not based on precise information. This observation can perhaps be extended to all the companies interviewed, given that a lack of information was one of the features shared by all the cases analysed.

The last question required the compilers to indicate, for each type of incident listed, the probability of occurrence and the severity of its impact on the company's assets, assigning an indicator from 1 to 5, where 5 was the maximum probability/severity. The results were as follows.

Before analysing the findings in detail, it is necessary to explain the methodology used to elaborate the figures given by the interviewees, seeing that some inferences were needed. In fact, while the questionnaire requested that an indicator from 1 to 5 (with being 5 the maximum probability/severity) be assigned to both probability and severity, some respondents inserted also the answers 'not applicable' and 0. According to the specific crime these answers were assigned to and, in general, to the company characteristics (e.g. the business/economic sector of reference and the typology of activity) emerging from the whole questionnaire, it was concluded that both 'not applicable' and 0 could indicate that the company is not exposed to that particular kind of crime.

Therefore, 'not applicable' is here considered as 0, that is the absence of criminal risks related to the specific crime; the range has thus been enlarged from 0 to 5, with 0 corresponding to 'no probability' and 'no severity'. The average has then been calculated with reference to the entire sample (10 questionnaires).

The choice to adopt this approach depends on two main considerations. First, on the fact that this is not a quantitative but a case-study analysis, and it is mainly based on qualitative reflections. Therefore, figures and values must not be taken as absolute values, but only as indicative of a general trend.

Secondly, these specific figures do not aim at *measuring reality* (e.g. the real incidence of the typologies of crimes listed in the questionnaire) but only to understand how the respondents *perceive* the criminal risks their company is exposed to. This means that what is relevant is not the precise figure but the general range that may result from these ten cases.

Thus stated, in order to have a general overview of the findings, the following two tables schematise, in increasing order, the average values assigned by the respondents, respectively, to the probability and the possible severity of the listed crimes.

	RANGE	PROBABILITY (AVERAGE VALUES, IN INCREASING ORDER)
False bankruptcy Insider trading	0 – 0,9	0,8
Patent infringements		0,9
Identity theft	1– –1,9	1
Sale of information by insiders		1,2
Counterfeiting Arson Extortion Disclosure and use of passwords by outsiders Active wiretapping Falsification of financial statement Business relations with companies involved in criminal activities/money laundering		1,3
Vandalism by insiders Industrial espionage		1,4
Transactions involving conflicts of interest		1,5
Theft of transaction information Cyber-terrorism Trademark counterfeiting Inflated expense accounts		1,6
Sabotage of plants Terrorist acts/diffusion of subversive materials Unfair competition due to key employees resigning (professional roaming) Theft of money/personal effects of employees Distributed denial of service (dDos) Unfair competition Embezzlement (misappropriation of cash/funds)		1,7
Corruption of employees Telecom fraud/eavesdropping Unauthorised dissemination of information by insiders Unintentional release of information/know how to competitors Administrative fraud		1,8
Vandalism by outsiders Computer systems penetration from outside Computer systems penetration from inside Defacement of the web site home page Theft of information by means of social engineering techniques		1,9
Theft of company goods/ products during the manufacturing activities Theft of company products from warehouses	2 – 2,9	2

Damage to computer systems due to computer viruses – downloaded during internal surfing		
Employee abuse of internet access		2,1
Denial of service (dos) Financial fraud Purchase of goods/services for personal use		2,2
Theft/damage/sabotage of information from databases Disclosure and use of passwords by insiders Theft of company time		2,4
Theft of company products in transit		2,6
Damage to computer systems due to computer viruses – sent from outside		2,7
Laptop thefts		2,9

As schematised in the table, the respondents have all individuated the probability of occurrence of the listed crimes according to a range of values included, more or less, between 1 and 3. It is interesting to note that there is a particular concern for all the crimes and illicit conducts related to **thefts** in general and to **ICT technologies**, which are considered the most probable crimes.

As regards to theft, the most expected crimes are embezzlement, theft of information through social engineering techniques, theft of company products during the manufacturing activities, from warehouses and, in particular, while in transit. Also theft of company time is considered as highly probable, while laptop theft is absolutely seen as the most probable crime.

As far as ICT technologies are concerned, the respondents look with particular concern at all the typologies of crime, targeting hardware and software components, as well as the company network and the data/information security. To be highlighted that the active role of *insiders*, as possible perpetrators, is seriously taken into consideration by the respondents: considering the range from 2 to 3, 7 out of 13 crimes are perpetrated (or can also be perpetrated) by people within the company: damage to computer system due to computer viruses – downloaded during internal surfing, employee abuses of Internet access, financial fraud, purchases of goods/services for personal use, disclosure and use of passwords from insiders, theft of company time and laptop thefts.

The following table schematises the perception of the severity level associated by the respondents to the occurrence of the crimes listed.

	RANGE	**SEVERITY (average values, in increasing order)**
False bankruptcy	1 – 1,9	1,7
Counterfeiting Inflated expense accounts		1,8
Identity theft		1,9

Theft of company products from warehouses Theft of money/personal effects of employees	2 – 2,9	2
Theft of company goods/ products during the manufacturing activities Industrial espionage Business relations with companies involved in criminal activities/money laundering		2,1
Telecom fraud/eavesdropping Trademark counterfeiting Purchase of goods/services for personal use		2,2
Insider trading		
Extortion		2,3
Active wiretapping		
Patent infringements Falsification of financial statement		
Transactions involving conflicts of interest		
Employee abuse of Internet access Theft of company time		2,4
Theft of company products in transit Disclosure and use of passwords by outsiders Unfair competition Administrative fraud		2,5
Corruption of employees Theft of transaction information		2,6
Sale of information by insiders Embezzlement (Misappropriation of cash/funds)		
Vandalism by outsiders Unfair competition due to key employees resigning (professional roaming) Defacement of the web site home page		2,7
Unintentional release of information/know how to competitors		
Theft of information by means of social engineering techniques Cyber-terrorism		2,8
Laptop thefts		2,9
Damage to computer systems due to computer viruses – downloaded during internal surfing	3 – 3,9	3
Vandalism by insiders Damage to computer systems due to computer viruses – sent from outside Disclosure and use of passwords by insiders		3,1
Unauthorised dissemination of information by insiders		3,2
Financial fraud		3,4
Denial of Service Distributed Denial of service		3,5
Computer system penetration from outside		3,9

Sabotage of plants Arson	4 – 4,9	4
Theft/damage/sabotages of plants		
Terrorist acts/diffusion of subversive materials		4,1
Computer system penetration from inside		4,2

Differently from the probability scale, the respondents have associated a higher level of risk to severity; the range approximately goes from 1 to 4,5.

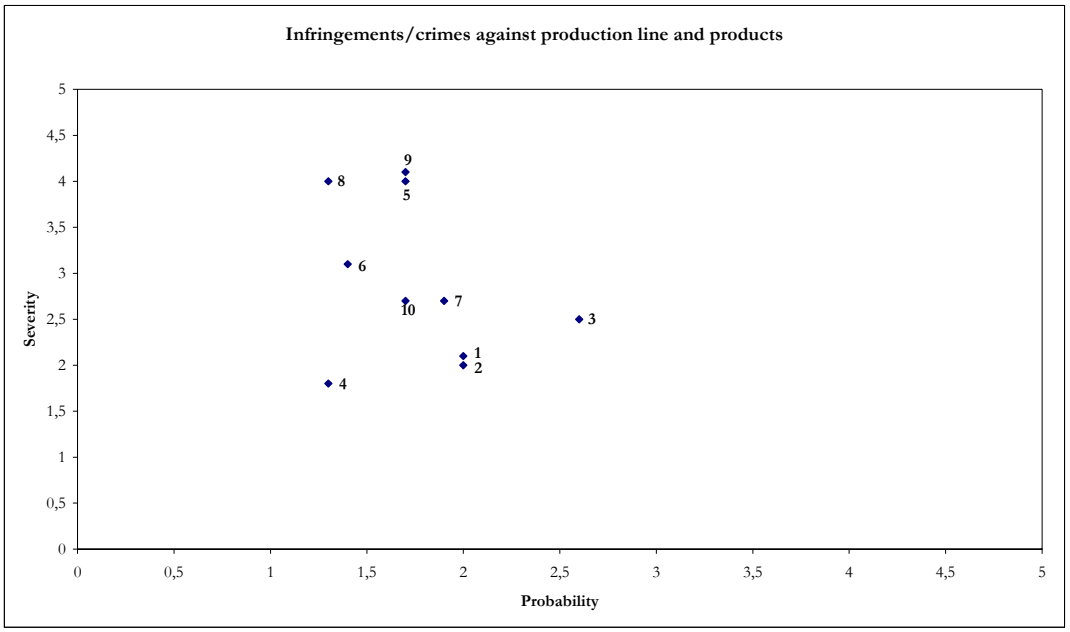
It is important to say that, according to the findings, the crimes which are considered to have a more serious impact on the company are mainly related to **ICT technologies**: considering the range is between 3 and 5, in fact, 7 out of 14 of the listed crimes concern damages to computer system, disclosure of passwords, denial of service (also distributed), computer system penetration from both outside and inside. It is curious to note that computer system penetration from inside is considered as the most *severe* crime, according to the impact it may have on company assets.

Together with ICT related crimes, there are also other groups of crimes that are considered particularly damaging: crimes against **production line and products**, in specific vandalism (to be noted that vandalism by insiders is associated to a higher level of severity – 3,1 – rather than vandalism by outsiders – 2,7), sabotage of plants and arson; within the crimes against capitals, a serious grade of severity is generally associated only to **financial fraud**.

As for probability, it must be underlined that the maximum level of severity is largely attributed to those crimes which are committed – or can be also committed – by employees. As regards to disclosure of passwords, for example, companies seem to be more concerned about possible disclosure on the part of insiders.

The following graphs clarify the relationship between probability and severity by representing it according to the different categories of infringements/crimes specified by the questionnaire. The tables also give the corresponding numerical values; the crime with the highest probability/severity ratio and the one with the lowest probability/severity correlation are highlighted.

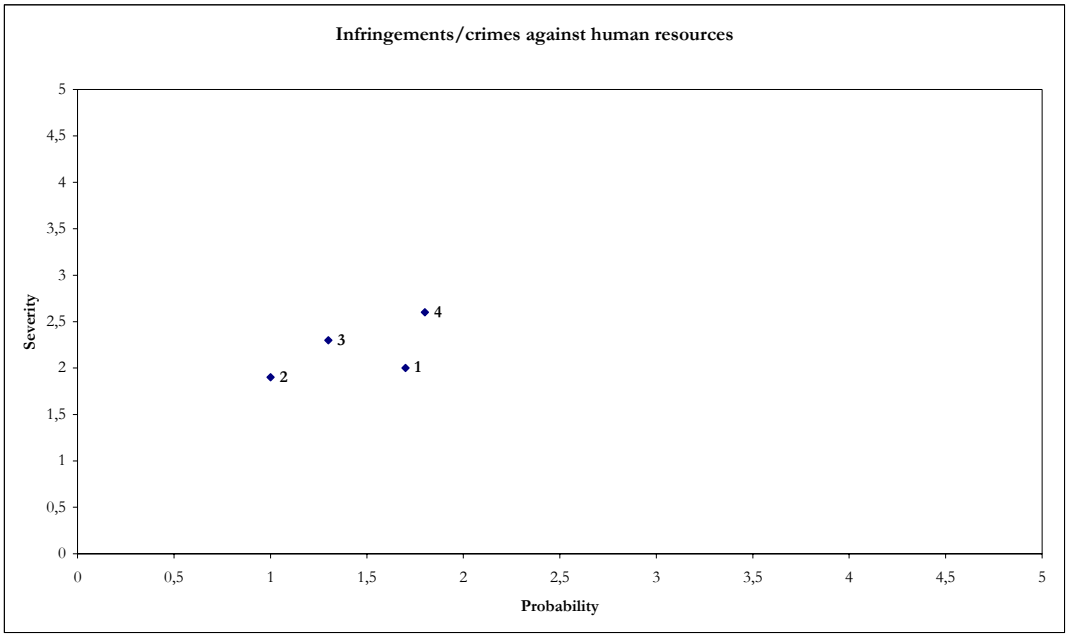
Infringements/crimes against production line and product



NUMBER	INFRINGEMENTS/CRIMES	SEVERITY	PROBABILITY
1	Theft of goods/products during the manufacturing process	2,1	2
2	Theft of company products from the warehouse	2	2
3	*Theft of company products in transit*	2,5	2,6
4	*Counterfeiting*	1,8	1,3
5	Sabotage of plants	4	1,7
6	Vandalism by insiders	3,1	1,4
7	Vandalism by outsiders	2,7	1,9
8	Arson	4	1,3
9	Terrorist acts/diffusion of subversive materials	4,1	1,7
10	Professional roaming	2,7	1,7

On average, respondents have associated the highest levels of both probability and severity to the theft of company products while in transit; on the contrary, counterfeiting is considered probable but not so severe.

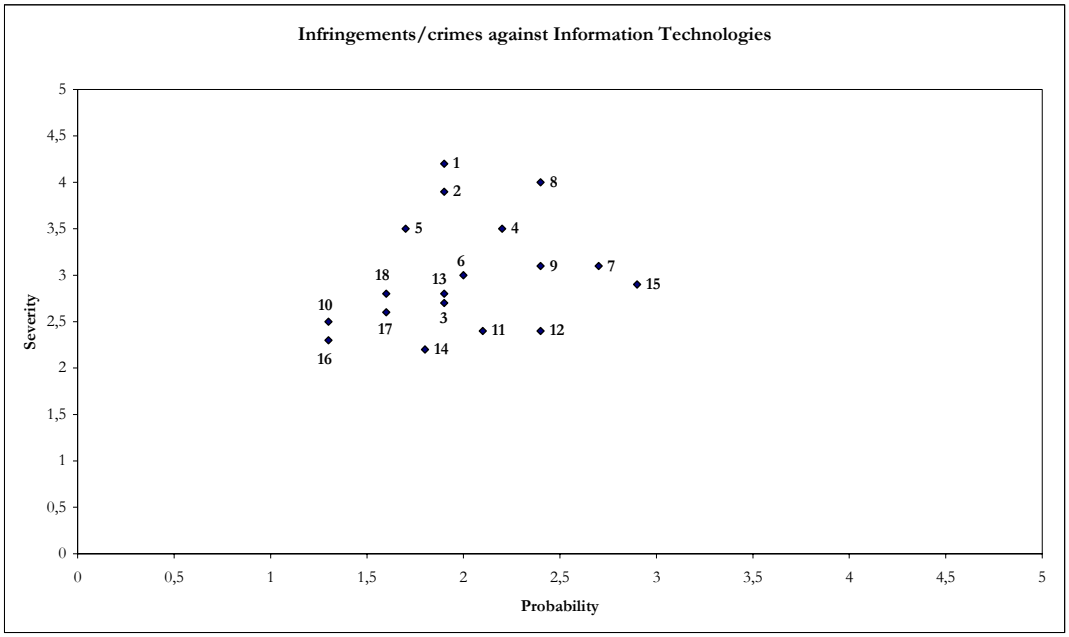
Infringements/crimes against human resources



NUMBER	INFRINGEMENTS/CRIMES	SEVERITY	PROBABILITY
1	Theft of money/personal effects	2	1,7
2	*Identity theft*	1,9	1
3	Extortion	2,3	1,3
4	*Corruption of employees*	2,6	1,8

As the graph shows, the respondents perceived corruption of employees as the most probable and severe of the crimes against human resources specified in the questionnaire, while identity theft seemed to generates little concern. Interestingly, although theft of money/personal effects of employees was considered to be highly probable, this type of crime was generally not associated with a high degree of severity.

Infringements/crimes against Information Technologies



NUMBER	INFRINGEMENTS/CRIMES	SEVERITY	PROBABILITY
1	Illicit computer system penetration from outside	3,9	1,9
2	Illicit computer system penetration from inside	4,2	1,9
3	Defacement of the home page of the web site	2,7	1,9
4	Denial of Service (DoS)	3,5	2,2
5	Distributed Denial of Service (DDoS)	3,5	1,7
6	Damages due to computer viruses downloaded during internal surfing	3	2
7	Damages due to computer viruses downloaded during external surfing	3,1	2,7
8	Theft/damages/sabotage of information from database	4	2,4
9	Disclosure of and use of password from insiders	3,1	2,4
10	Disclosure of and use of password from outsiders	2,5	1,3
11	Employee abuse of Internet access	2,4	2,1
12	Theft of company time	2,4	2,4
13	Theft of information through social engineering techniques	2,8	1,9
14	Telecom fraud/eavesdropping	2,2	1,8
15	*Laptop thefts*	2,9	2,9

16	*Active wiretapping*	2,3	1,3
17	Theft of transaction info	2,6	1,6
18	Cyber-terrorism	2,8	1,6

The respondents considered laptop thefts to be the most probable and most serious type of crimes against information technology. This result is not surprising: it probably depends on the fact that laptops are tangible assets which can be easily stolen and concealed. At the same time, they are usually valuable sources of information because they contain company records of particular importance, such as proprietary and commercial information.

It is interesting to note that crimes affecting computer systems, such as illicit computer system penetration from outside (1), illicit computer system penetration from inside (2) and denials of service (3,4) are considered to be particularly serious but are not perceived to be highly probable.

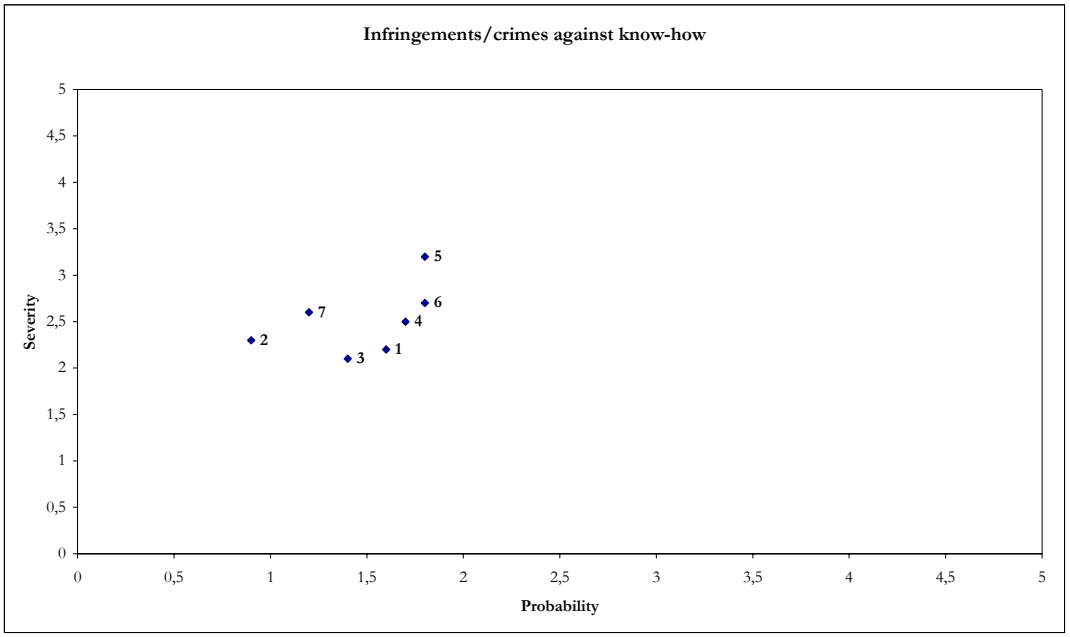
The only exceptions are theft, damage and sabotage of information from database (8), which are viewed with concern.

It may be that the respondents give differing degrees of importance to these crimes according to the assets that they might damage: information was perceived as being more important than computer system integrity, functionality and security, so that these display a balanced ratio between probability and severity.

Moreover, respondents may not have been completely aware of the modi operandi of perpetrators and the techniques used to attack company computer systems, with the consequence that they failed to perceive the real incidence and risks of these types of crimes but on the contrary realized that if they did occur, they could seriously damage the computer system.

The approach to cyber-terrorism is also of particular interest: it is not considered to be one of the most likely crimes against a company but it is associated with a quite high level of severity.

Infringements/crimes against know-how

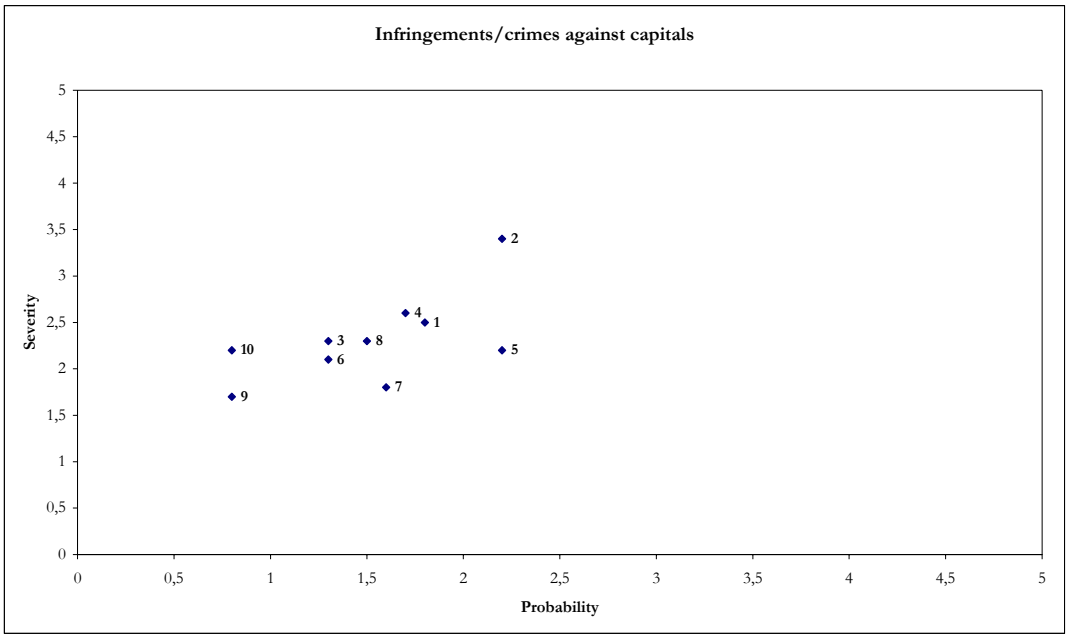


NUMBER	INFRINGEMENTS/CRIMES	SEVERITY	PROBABILITY
1	Trademark counterfeiting	2,2	1,6
2	*Patent infringements*	2,3	0,9
3	Industrial espionage	2,1	1,4
4	Unfair competition	2,5	1,7
5	*Unauthorized dissemination of information by insiders*	3,2	1,8
6	Unintentional release of information/know-how to competitors	2,7	1,8
7	Sale of information by insiders	2,6	1,2

The findings confirm that information receives particular attention in this group of crimes as well: the unauthorised dissemination of information by insiders (5), in fact, is perceived as the most probable and most serious crime/infringement. This is confirmed by the fact that also the unintentional release of information/know-how to competitors (6) is perceived as highly probable and damaging.

On the contrary, it seems that less attention is paid to industrial property infringements.

Infringements/crimes against capitals



NUMBER	INFRINGEMENTS/CRIMES	SEVERITY	PROBABILITY
1	Administrative fraud	2,5	1,8
2	*Financial fraud*	3,4	2,2
3	Falsification of financial statements	2,3	1,3
4	Embezzlement (misappropriation of cash/founds)	2,6	1,7
5	Purchase of goods/services for personal use	2,2	2,2
6	Business relations with companies involved in criminal activities/money laundering	2,1	1,3
7	Inflated expense accounts	1,8	1,6
8	Transactions involving a conflict of interest	2,3	1,5
9	*False bankruptcy*	1,7	0,8
10	Insider trading	2,2	0,8

The graph shows clearly that financial fraud is the crime that the respondents regarded as the most probable and the most serious. By contrast, they assigned both low probability and low severity to false bankruptcy, which is perhaps not generally perceived as pertinent to the company's philosophy.

PART III – EARLY WARNING SIGNS AND BUSINESS SECURITY

As already explained, this Falcone 2001 '*Business Crime Prevention in Europe: Implementing an Early Warning Strategy*' Study proposes a new approach to business security management. It starts from the idea that if the crimes committed most frequently within and without companies are identified and analysed, it will be possible to single out *early warning signs* able to alert managers and executives, as well as employees, when a specific company department or area is at threat of criminal penetration. On this view, early warnings are a specific preventive strategy which provide also methodological support for traditional risk analysis procedures.

In order to be successful, however, this approach needs information, data, and especially, profound knowledge of the given company environment. Moreover, from a scientific perspective, the possibility of drawing generalizations, conducting comparisons and devising best practices depends on the availability of case studies and experimentation. This is not the case of the business sector alone, for, as will be explained in the following sections, early warnings models are applicable to diverse contexts and for different purposes.

Their essence and importance are summed up by the following statement: 'early warning and conflict prevention are based on proactive responses to potential threats to national and/or human security'.[48]

At present, the different areas of application, and the relative lack of systematic analysis of early warnings, mean that a general definition of them is not possible. Nevertheless, the one proposed by the Forum for Early Warning and Early Response (FEWER) can be taken as a benchmark. As will be explained in the following sections, this definition refers to the specific research area of the prevention and management of conflicts, but it is sufficiently flexible for it to be adapted to other contexts as well.

According to FEWER, the early warnings approach consists of the systematic collection and analysis of information from areas of crises in order to:

1. anticipate the escalation of violent conflict;
2. develop strategic responses to these crises; and
3. present options to critical actors for the purposes of decision making.[49]

On the basis of this definition, but adopting a business-oriented perspective, the early warning approach is considered here to be the systematic collection and

[48] Leatherman J., Väyrynen R., "Structure, Culture, and Territory: Three Sets of Early Warning Indicators." Paper prepared for the *Panel on Early Warning and Conflict Prevention in Intrastate Conflicts, Annual Meeting of the International Studies Association*, Chicago, Illinois, 21 – 25 February 1995.

[49] This definition is proposed in Ampleford S., *Methodology Review*, prepared for the International Development Research Centre, July 2000, p. 4. The text is available at the following URL: http://www.reliefweb.int/library/documents/studmeth.pdf.

analysis of information within the corporate environment in order to develop more detailed knowledge of criminal dynamics within the company, to identify the causes, to intervene in internal opportunities, and to prevent crimes and abuses from occurring.

If crime prevention is the principal output of early warnings strategies, also the other related benefits are not to be underestimated; in fact, by developing greater awareness on the part of management, the early warning approach can help create a secure and well-organised workplace environment. These issues will be developed in detail by the analysis that follows.

10. EARLY WARNINGS THEORIES AND APPLICATIONS

Apart from certain exceptions analysed later, both the study and the application of early warning signs theory to the business sector are still in their beginnings. However, early warnings have been already tested and used in other contexts for different purposes.

In order to clarify the relevance of early warning signs, and to point out their utility and value, this section provides a general overview of the most important experiments to date and their results. As will be explained, most early warning projects have encountered difficulties that obstruct the achievement of positive results, as well as the study of new models and strategies. This does not mean, however, that early warning theories have failed; on the contrary, experts generally agree that these projects, together with pilot studies in new research areas, should be developed further, because there is already substantial evidence of the importance and the utility of this approach to different phenomena.

Before entering into details, we would point out that studies and programmes focused on the possibility of using an early warning strategy to solve and/or prevent certain incidents deal with a wide variety of phenomena: weather forecasting, clinical practice and early diagnosis, humanitarian crisis and political disaster management, juvenile delinquency and school safety, agriculture, insurance. Early warnings are used in the business environment to prevent workplace violence, for example, while there is growing interest in their use to prevent employee theft.

Some of these applications will be analysed in the following sections.

10.1 EARLY WARNING SIGNS AND *FOREIGN POLICY MANAGEMENT*: FROM CONFLICT ANALYSIS TO RESPONSE DEFINITION

The use of early warning signs in foreign policy management is mainly oriented towards the prevention of possible international conflicts by developing internal (political, social, economic) stability.

Various programmes and projects deal with this issue. One of the most authoritative and important of them is the *Country Indicators for Foreign Policy* (CIFP) developed by the Canadian Department of Foreign Affairs and International Trade (DFAIT) and the Norman Paterson School of International Affairs, in 1997.[50]

This project is an on-going effort to identify and assemble statistical information covering the key features of the political, economic, social and cultural environments of countries around the world. The resulting collection provides a core set of data for each country regarding demography, economics, social development, the environment, political climate and internal stability, military capability and risk-conflict potential.

The collection of trans-national data, generated through CIFP, is intended to be applied and used in different ways by government departments, NGOs and by the private sector. At the moment, this data set includes measures of domestic armed conflict, governance and political instability, militarization, religious and ethnic diversity demographic stress, economic performance, human development, environmental stress and international linkages. The CIFP database currently includes statistical data on these areas in the form of over one hundred performance indicators for 196 countries, covering 15 years (1985-2000) for most indicators.

The importance of this project is confirmed by its current implementation; together with the Canadian International Development Agency (CIDA), CIFP has started a pilot project in partnership with the Forum on Early Warning and Early Response (FEWER). Apart from operational aspects, to be highlighted is that the project intends to establish a framework for communications, information gathering and sharing, and to develop a conflict early warning system involving the various members of the FEWER network.

As regards the early warnings to be collected, these have been identified by means of both applied research (pilot early warning activities undertaken in the Great Lakes area and the Caucasus) and academic studies. In the light of the results obtained, early warnings require the use of a wide range of data, methods and sources including local analysis, the monitoring of newswire reports and structural data.

This initial, exploratory research has concluded that the outbreak of violent conflict is due to three main elements which escalate conflicts: structural factors, accelerators, and triggers.[51]

---

[50] For a detailed description of the project and the methodology used, see CIFP, *Risk Assessment Template*, August 2001. More information is available at the following URL: http://www.carleton.ca/cifp.

[51] CIFP, *cit.* 50, p. 4.

Structural/root factors comprise all the pre-conditions for crisis situations, such as systematic political exclusion, shifts in the demographic balance, economic inequalities, economic decline and environmental decay;

Accelerators, or also *precipitators*, are factors which increase the incidence and significance of already-existing root causes;

Triggers are unexpected and abrupt events that precipitate the conflict and/or the crisis: the assassination of a leader, for example, electoral fraud or a political scandal.

Although this classification is an operational simplification,[52] the assessment of indicators – even if general – is nevertheless necessary because crises and conflicts very often do not spring from a precise single cause; on the contrary, they may arise from numerous contributory ones which vary in importance and must be somehow classified.

From the theoretical point of view, an important feature of the CIFP Project is its approach to the relationship between early warnings and risk assessment, which it sees as complementary but distinct. This aspect is particular significant because it can be straightforwardly applied to other areas and environments, and at the same time to different issues and for different purposes. From the business-oriented perspective, this approach can be of extreme importance.

Gurr and Marshall explain the correlation between early warnings and risk assessment as follows:

'Risk assessment… identifies situations in which the conditions for a particular kind of conflict… are present. They are not predictions in the sense that is usually meant by the terms 'forecast' or 'early warning' because risks are assessed on the basis of background and intervening conditions— the conditions that establish the potential for conflict. Whether or not risks are realized depends on whether the preconditions remain unchanged and on the occurrence of accelerating or triggering events. Early warnings by contrast are derived from monitoring the flow of political events, with special attention to actions that are likely to precipitate the onset of conflict in high-risk situations. Risk assessments provide the context. Early warnings are interpretations that the outbreak of conflict in a high-risk situation is likely and imminent'.[53]

In practice, while risk assessment makes some sort of diagnosis of the situation, the early warnings approach seeks to develop appropriate and forward-looking preventive measures. Early warnings combine theoretical analysis with a more practical approach, which means that information gathering and early warnings analysis aim to prevent crises and other phenomena while also developing strategic responses to them, offering different options to the critical actors involved in the decision-making process.

---

[52] See also West Africa Network for Peace-Building, Centre for Conflict Research, Fewer, *Conflict Analysis and Response Definition – Abridged Methodology*, April 2001.

[53] Gurr T. R., Marshall M., "Assessing the Risks of Future Ethnic Wars", in Gurr T. R., *People versus States: Minorities at Risk in the New Century*, Washington DC, Institute of Peace Press, 2000.

The point is that analysts must find a time frame suitable to the issue with which they are dealing. Internal and foreign policy management and conflict prevention comprise various steps and stages which must be treated in different ways. A clear explanation of how early warnings work is provided by David Carment[54]: 'warnings must come several years in advance to respond strategically to structural problems (development, institution building, establishing infrastructure), but only months or less when escalation is imminent and when the tasks are to engage in preventive diplomacy, dialogue and mediation'.

This aspect is of great importance because it sums up the essence of early warnings theories. What has already been achieved in the sector of foreign policy management, therefore, is extremely valuable for both this specific problem and more generally for development of an early warnings methodology.

10.2 EARLY WARNING SIGNS AND *COMPLEX HUMANITARIAN CRISIS*

This issue is not entirely different from the one just examined. Complex humanitarian crisis (CHC) is the label used to denote mass phenomena deriving, in general, from serious political, social, economic, military and/or natural accidents. Many of these phenomena combine, for example, the usual problems of civil war with famine, refugee movements, large-scale violations of human rights, and a variety of levels of international intervention.[55]

The importance of early warning signs in this area – 'moribund for about a decade after substantial research in the late-1970s'[56] – has been rediscovered in recent years, and owing to three main factors:

1. since the end of the Cold War, sudden outbreaks of serious systematic violence, both international and inter-ethnic, have characterised the international system. Examples are Iraq's invasion of Kuwait, the conflict between Armenia and Azerbijan, the genocidal violence in Bosnia and Rwanda, and the violent internal conflicts in Somalia, Chechnya, Haiti, Algeria, and Liberia. Concern over these situations apart, from the methodological point of view there is an urgent need for new studies and approaches to the problem;

2. since the disappearance of the 'Communist threat', liberal, democratic, military powers like the United States, Great Britain and France have been generally less inclined to intervene directly in local or regional disputes. By contrast, at international level there is a certain inclination towards multilateral responses

---

[54] Carment D., "Assessing Country Risk: Creating an Index of Severity", May 2001, p. 2. The text is available at the following URL: http://www.carleton.ca/cifp/risk.htm.

[55] This issue is exhaustively discussed by Schrodt P. A. and Gerner D. J., "The Impact of Early Warning on Institutional Responses to Complex Humanitarian Crises", paper presented at the *Third Pan-European International Relations Conference and Joint Meeting with the International Studies Association*, Vienna, 16-19 September 1998.

[56] Schrodt P. A., Gerner D. J., *cit*. 55, p. 1.

organised by international organisations like NATO and the UN, or as *ad hoc* initiatives (e.g. Iraq – Kuwait, Bosnia, Albania). This situation enhances the attractiveness of early warnings in two respects. First, if discovered in their initial stages, conflict situations can be contained by using smaller amounts of force; second, multilateral responses take much more time to organise than individual or direct interventions. This means that early warnings are of crucial importance in preventing a pointless waste of time;

3. ICT development is rapidly changing the quantity and timeliness of the collection and circulation of information, so that there are increasing opportunities to develop early warnings systems. As Schrodt and Gerner point out: 'One recent estimate states that the amount of information available in electronic form has increased by a factor of 10 6 —one million times—since 1981. In addition, inexpensive desk-top computers now surpass in capacity most of the main-frame computers available to national intelligence agencies until the middle of the last decade'.[57]

From the empirical point of view, however, the identification, collection, analysis and use of early warnings in humanitarian crises is anything but simple. There are possible failures to be prevented, and obstacles like the intentional concealment of relevant signs, institutional ignorance, political or social hostility, and cognitive problems to be avoided. Anyway, in this sector, the development of early warnings is supposed to produce relevant, positive effects, so that obstacles must be removed.

However, researchers stress that early warnings of CHCs are likely to remain confined to academic, nongovernmental (NGO) and intergovernmental (IGO) projects. Yet, considering the increases in information availability, this decentralization does not necessarily preclude effective early warnings, which may in fact be enhanced. But as Schrodt and Gerner stress, it is necessary to augment the credibility, visibility, and efficacy of these efforts, as is now being done by such initiatives as the Forum for Early Warning and Emergency Response (FEWER) and the ReliefWeb. The latter is a project of the United Nations Office for the Coordination of Humanitarian Affairs (OCHA). As explained at its website[58], this project mainly responds to the information needs of the humanitarian relief community.

10.3 EARLY WARNINGS AND *ENVIRONMENTAL PROTECTION/ DISASTER REDUCTION*

One of the most interesting initiatives in the use of early warnings is the environmental protection project sponsored by the European Environment Agency,

[57] *Ibid*.

[58] See http://www.reliefweb.int/w/rwb.nsf.

the results of which are set out in its Report *Late Lessons from Early Warnings: The Precautionary Principle 1896-2000 – Environmental Issue Report No. 22*.[59]

The Report states that its concern is to gather information on the hazards raised by human economic activities and its use in taking action to improve protection of the environment and the health of the species and ecosystems dependent upon it. The study aims to furnish better and more accessible science-based information and to foster more effective stakeholder participation in the governance of economic activity so that environmental and health costs may be minimised and innovation maximised.

Like all the other experiments in the use of early warnings, this one too is based on a philosophical approach. In this case, the need to collect information with which to develop programmes to balance environmental protection with economic development derives from the so-called 'precautionary principle',[60] which the Report explains as follows[61]: 'being wise before it is too late is not easy, especially when the environmental or health impacts may be far into the future and the real, or perceived, costs of averting them are large and immediate. Forestalling disasters usually requires acting before there is strong proof of harm, particularly if the harm may be delayed and irreversible, an approach to scientific evidence and policy-making which is part of what is now called the precautionary principle'.

The precautionary principle is applied in various stages[62]:

research and monitoring for the early detection of hazards;

a general reduction of environmental burdens;

the promotion of 'clean production' and innovation;

the proportionality principle whereby the costs of actions to prevent hazards should not be disproportionate to the likely benefits;

a cooperative approach among stakeholders to solving common problems via integrated policy measures aimed at improving the environment, competitiveness and employment;

action to reduce risks before full 'proof' of harm is available if impacts could be serious or irreversible.

Since the 1970s, this approach has rapidly moved on to the political agenda in both Europe and internationally.[63]As regards Europe, for example, the European

---

[59] EEA, *Late Lessons from Early Warnings: The Precautionary Principle 1896-2000 – Environmental Issue Report No. 22*. The text is available at the following URL: http://reports.eea.eu.int/environmental_issue_report_2001_22/en. See also EEA, *Environmental Signals 2002. Benchmarking the Millennium – Environmental Assessment Report No. 9*. The text is available at the following URL: http://reports.eea.eu.int/environmental_assessment_report_2002_9/en/signals2002-intro.pdf.

[60] This approach was first applied to environmental hazards by environmental science in the 1970s, when German scientists and policy makers set out to deal with the so-called "forest death" and its possible causes.

[61] EEA, *cit*. 59, p. 13.

[62] *Ibid*.

Commission has supported its development with the Communication on the Precautionary Principle (2000), while it has also been considered by the Council of Ministers in its so-called Nice Decision (2000).

A great deal of work is also being undertaken by the United Nations, and specifically by its International Strategy for Disaster Reduction Division. Its mission is to enable all societies to become resilient to the effects of natural hazards and related technological and environmental disasters in order to reduce human, economic and social losses.[64] One objective is therefore to strengthen disaster reduction capacities through early warnings. To date, in accordance with the UN General Assembly mandate, the Secretariat has launched a number of initiatives in the area of early warnings, including the convening of six expert working groups to study geological hazards, hydrometeorological hazards, including droughts, fire and other environmental hazards, and technological hazards.

10.4 EARLY WARNINGS AND *CLIMATE DISASTERS*

This issue is closely related to environment protection, but also to community safety from natural and climate disasters.

Currently being developed by the United Nations, for example, is an early warnings system for areas threatened by climate-related natural disasters.[65]The United Nations Environment Programme comprises a specific Division on Early Warning and Assessment[66] whose aim is to provide the world community with improved access to meaningful environmental data and information and to help increase the capacity of governments to use environmental information for decision-making and action planning for sustainable human development.

Scientists divide the Earth into areas and show where the inhabitants are at risk of disaster, drawing up a *vulnerability index* which warns governments about the areas of the country that are disaster-prone. Experts are studying, for example, deforestation, coral reef destruction and other forms of environmental damage which make communities more vulnerable.

One of the first concrete results of this work, in terms of information circulation, is the activities of the GRID-Geneva Office. As a UNEP centre specialising in environmental data and assessment, this centre prepares and disseminates timely

---

[63] The EEA Report, *cit.* 59, contains also an interesting table schematising the presence and use of the "precautionary principle" in some international Treaties and agreements, such as the *Rio Declaration on Environment and Development* (1992), the *Treaty on European Union* (Maastricht Treaty, 1992) and the *Cartagena Protocol on Biosafety* (2000).

[64] See http://www.unisdr.org/unisdr/aboutisdr.htm.

[65] Kirby A., "UN's early warning of climate disaster", 4 February 2001, available at the following URL: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1150000/1150290.stm.

[66] See the United Nations Environment Programme (UNEP) website at the following URL: http://www.unep.org.

and understandable information in order to increase awareness and improve effective and efficient decision-making processes. The core tasks are grouped in five general areas[67]:

1. provision of early warning on emerging environmental problems and threats;
2. support to the UNEP's assessment process, including the Global Environment Outlook (GEO), a bi-annual review of the state of the world's environment;
3. implementation of capacity building projects to develop and strengthen the environmental information systems of partner organisations;
4. carrying out cases studies using GIS and remote sensing for the mapping, monitoring and sustainable use of natural resources;
5. provision of technical expertise for meta database and website design and creation.

Moreover, GRID-Geneva undertakes a wide range of projects in collaboration with UN agencies, also supporting the global/regional environmental conventions that help fulfil UNEP's mission.

10.5 EARLY WARNINGS AND *INVASIVE PLANTS MANAGEMENT*

In a certain sense, this is a practical implementation of the 'precautionary principle' discussed above; specifically, the use of early warnings against invasive plants is an example of how early warnings can be used in agriculture.

A clearer idea can be gained from a concrete example provided by the United States. The *Center for Invasive Plant Management*[68] is a coalition of agencies, organizations, and individuals interested in managing invasive plants and maintaining healthy ecosystems in western North America.

As explained by the Center, the main goals of the initiative are the following: enhancing land manager and public education, coordinating regional research, facilitating partnerships, increasing multidisciplinary communication, and implementing practical management programmes.

Of relevance to our research is how the Center uses early warnings: it collects information and alerts mostly from experts and public agencies, but also from individuals, warning of the presence of certain invasive plants and weeds in particular places and environments in western North America. It also advises on

[67] All the following information are available at the following URL: http://www.grid.unep.ch/activities/index.html.

[68] All the information set out in this Report can be found at the Center for Invasive Plant Management website at the following URL: http://www.weedcenter.org.

how to treat them in order to protect the land and to implement the most cost-effective method of invasive plant management. This information is public and is available on the Internet in a special section of the Center's website.

By using early warnings, the Center has fostered close communication among a wide range of public and private subjects. As explained in the *Center for Invasive Plant Management Annual Report 2001*[69], one of the most important results has been the creation and maintenance of an early-warning listserv for the Western Weed Coordinating Committee, connecting through email state and federal agencies, conservation organizations, and local land managers.

The use of early warnings is thus important because it allows the creation of a database of information collecting best practices and, above all, the organisation of concrete and specific preventive and incident handling countermeasures and initiatives.

10.6 EARLY WARNING SIGNS AND *JUVENILE DELINQUENCY PREVENTION*: THE SAFE SCHOOLS PROJECTS

Early warning signs have also been developed to prevent juvenile delinquency, especially in schools. In the United States, a huge number of programmes have been implemented thanks to the endeavour of staff, students, parents, and members of the community to create a safe school environment. These initiatives are based on the idea that schools must put strategies in place to deal with the needs of all children with behavioural disorders.

A distinctive approach is taken to early warnings, which are considered from a different perspective: they are not seen solely as the 'causes' in a cause-effect relationship where the cause is the signal and the effect is necessarily a crime or a deviant behaviour. That is, they are not necessarily predictors that a child is going to hurt himself or others, for example. It may be that even if the child displays problematic behaviour, this situation will not necessarily give rise to a criminal/violent conduct. As consequence, early warning signs are used to understand what is happening and to address problems before they escalate.

The approach is explained in numerous documents and guides: a useful example is the *Early Warning, Timely Response. A Guide to Safe Schools* published by the American Department of Education, Special Education and Rehabilitative Services.[70]

The following are the most important passages:[71]

---

[69] Center for Invasive Plant Management, *Center for Invasive Plant Management Annual Report 2001*, 2001. The text is available at the following URL http://www.weedcenter.org/about/2001annualreport2.pdf.

[70] The text is available at the following URL: http://www.ed.gov/offices/OSERS/OSEP/earlywrn.html.

[71] Italics is not used in the original text.

'There are early warning signs in most cases of violence to self and others -- certain behavioural and emotional signs that, when viewed in context, can signal a troubled child. *But early warning signs are just that -- indicators that a student may need help.*

Such signs may or may not indicate a serious problem -- *they do not necessarily mean that a child is prone to violence toward self or others*. Rather, early warning signs provide us with the impetus to check out our concerns and address the child's needs. *Early warning signs allow us to act responsibly by getting help for the child before problems escalate*.

Early warning signs can help frame concern for a child. However, it is important to avoid inappropriately labelling or stigmatising individual students because they appear to fit a specific profile or set of early warning indicators. *It's okay to be worried about a child, but it's not okay to overreact and jump to conclusions*'.

So that these signs are not misunderstood, the Guide also provides a list of principles that may be of help to those (relatives, practitioners) who recognize the signals and want to intervene; the following are examples: do no harm; understand violence and aggression within the context; avoid stereotypes; view warning signs within a developmental context; understand that children typically exhibit multiple warning signs.

The most indicative early warning signs derive from research which establishes that most children who become violent toward self or others feel rejected and psychologically victimized. In most cases, children exhibit aggressive behaviour early in life and, if support is not provided, will continue in a progressive developmental pattern toward severe aggression or violence. However, research also shows that when children have a positive, meaningful connection with an adult – whether at home, in school, or in the community – the potential for violence is significantly reduced. The use of early warnings must be harmonised with research findings if it is not to produce results that are much more negative than positive.

While reiterating that early warnings must not degenerate into stigmata, the Guide lists the following signals in particular:

- uncontrolled anger;
- patterns of impulsive and chronic hitting, intimidating, and bullying;
- history of discipline problems;
- past history of violent and aggressive behaviour;
- intolerance for differences and prejudicial attitudes;
- drug use and alcohol use; affiliation with gangs;
- inappropriate access to, possession of, and use of firearms;
- serious threats of violence.

While early warning signs must be 'handled with care', *imminent warning signs* indicate that a student is on the brink of behaving in a way that may be dangerous for him/herself and/or for others. An immediate response is thus necessary. According to studies on the matter, imminent signs are clearly recognisable by school staff as well as by the family. The following are examples:

- serious physical fighting with peers or family members;
- severe destruction of property;
- severe rage for seemingly minor reasons;

- detailed threats of lethal violence;
- possession and/or use of firearms and other weapons;
- other self-injurious behaviours or threats of suicide.

How should schools and relatives react to early warning signs once they recognize them?

Understanding early and imminent warning signs is an essential step in ensuring a safe school; to be effective, however, it must be followed by concrete support for the emotional and behavioural adjustment of the child.

The school should already have a procedure to be followed; as indicated by the Guide, there should be a support strategy, including:

'School board policies in place that support training and ongoing consultation. (The entire school community knows how to identify early warning signs, and understands the principles that support them);

School leaders who encourage others to raise concerns about observed early warning signs and to report all observations of imminent warning signs immediately. This is in addition to school district policies that sanction and promote the identification of early warning signs;

Easy access to a team of specialists trained in evaluating and addressing serious behavioural and academic concerns.

Each school community should develop a procedure that students and staff can follow when reporting their concerns about a child who exhibits early warning signs. For example, in many schools the principal is the first point of contact. In cases that do not pose imminent danger, the principal contacts a school psychologist or other qualified professional, who takes responsibility for addressing the concern immediately. If the concern is determined to be serious – but not to pose a threat of imminent danger – the child's family should be contacted. The family should be consulted before implementing any interventions with the child. In cases where school-based contextual factors are determined to be causing or exacerbating the child's troubling behaviour, the school should act quickly to modify them'.

It these are guidelines for the post-accident situation, the early warning signs approach is also used to forestall problematic behaviour by children. From a practical point of view, examples of effective early intervention include:

providing training and support to staff, students, and families in understanding factors that can set off and/or exacerbate aggressive outbursts;

teaching the child alternative, socially appropriate replacement responses-such as problem solving and anger control skills;

providing skill training, therapeutic assistance, and other support to the family through community-based services;

encouraging the family to make sure that firearms are out of the child's immediate reach. Law enforcement officers can provide families with information about safe firearm storage as well as guidelines for addressing children's access to and possession of firearms.

This abundance of information, programmes and initiatives concerning the use of early warning signs in the school environment is evidence of the concrete and important results that can be achieved when this approach is used. From the methodological point of view, however, the use of early warning signs is not a simple task: as evidenced by this case-study, understanding and using early warnings require constant efforts by a wide range of subjects and, most of all, multidisciplinary interaction.

10.7 EARLY WARNINGS AND '*PROBLEM POLICE OFFICERS*'

A project of great interest which is also based on early warnings deals with the phenomenon of 'problem officers'.[72] According to the information available, problem officers can be defined as those 'who are frequently the subject of complaints or who demonstrate identifiable patterns of inappropriate behaviour'.[73]

A growing body of evidence indicates that in any police department there will be a certain percentage of officers are who responsible for a disproportionate percentage of citizens' complaints. This is the case in the United States, where police chiefs are now aware that 10% of their police officers can cause 90% of the problems. Journalistic investigations have documented departments in which less than 2% of all officers are responsible for 50% of all citizens' complaints.

Abuses by law enforcement officers in the United States are among the most serious and divisive human rights violations in the country. The violations persist nation-wide, in rural, suburban, and urban areas of the country, and they are committed by a variety of law enforcement personnel including local and state police, sheriff's departments, and federal agents.[74] The problem is that while the number of repeatedly abusive officers on any force is generally limited, the authorities responsible — including law enforcement supervisors, as well as local and federal government leaders — often fail to act decisively to restrain or penalize such behaviour.

Human Rights Watch has intervened, conducting studies and surveys and reporting that all American cities share a lack of effective public accountability and transparency, a persistent failure to investigate and punish officers who commit human rights violations, and a variety of obstacles to achieving justice.

However, this situation is a not recent one; it was already made public by Herman Goldstein in 1970s, when he wrote that 'problem officers are well known to their

---

[72] All the information that follows are taken from Walker S., Alpert G. P., Kenney D. J., *Early Warning Systems: Responding to the Problem Police Officer*, National Institute of Justice, July 2001. The text is available at the following URL: http://www.ncjrs.org/pdffiles1/nij/188565.pdf

[73] U.S. Commission on Civil Rights, Who is guarding the Guardians?, Washington DC, 1981, p. 81.

[74] See http://www.hrw.org/about/initiatives/police.htm.

supervisors, to the top administrators, to their peers and to the residents of the areas in which they work but little is done to alter their conduct'.

To deal with the situation, in 1981 the U.S. Commission on Civil Rights suggested that all police departments should create an early warnings system to help supervisors identify problem officers and monitor their behaviour, intervening if necessary. This early warnings system is a data-based police management tool designed to identify officers whose conduct appears problematic and to warn about personal situations where intervention is required to correct problem behaviour, for example by means of counselling or training.

It is thus possible for the department to intervene before the situation degenerates and ends in disciplinary action.

It seems that this early warnings-based solution is becoming very popular; almost 30% of local law enforcement agencies serving populations of at least 50,000 already had early warning systems in 1999; another 12% were planning to adopt one.

Operationally, the early warnings systems used in this field divide into three main phases: selection, intervention, and post-intervention monitoring.

No common criteria and standards are provided as regards *selection*. However, there is general agreement that performance indicators should be citizens' complaints, firearm discharge and use of force reports, civil litigation, resisting-arrest incidents, high-speed pursuits and vehicular damage.

The second phase, *intervention*, combines deterrence and education. Deterrence takes two forms: simple and general. Simple deterrence assumes that officers subject to intervention will change their behaviour in response to the perceived risk of punishment. General deterrence presumes that all the other officers, who do not display deviant behaviour, will also take action to avoid punishment. Training is part of intervention because early warning systems start from the idea that they can help officers to improve their performance.

The last phase is *monitoring*; nearly 90% of the agencies with early warning systems continue to monitor problem officers after the initial intervention. This monitoring is mostly informal, and it is usually conducted by the officer's immediate supervisor. However, some agencies have also decided to implement a formal process of observation, assessment and reporting. The control period lasts for at least 36 months from the first intervention.

Unfortunately, there is still no research or survey work on the effectiveness of this early warnings approach; indeed, apart from some case studies and/or pilot studies, there is a lack of systematic analysis. Such studies should be conducted bearing in mind that the early warning system involves various subjects, so that evaluation studies should take account of its impact on citizens' complaints, on officers' performances, on supervisors, as well as on the other police departments.

To date, however, the general outcome is that the early warnings systems reduce the number of citizens' complaints.

10.8 EARLY WARNINGS AND *TERRORISM*

The relationship between early warnings and terrorism is difficult to describe because information is quite often reserved. However, since September 11 and the tragic attacks on the World Trade Centre and the Pentagon, terrorism and its threat to community safety have become a crucial issue world-wide. Part of the debate focuses on the fact that almost the recommendations made before September 11 went largely unheeded; recommendations which were mostly based on early warnings.[75]

For this reason, it seems important to briefly examine the possible role of the early warnings approach in this issue.

Apart from the specific case of September 11, the potential and utility of early warnings against terrorism are now generally accepted by the private and public institutions that deal with these issues. Indeed, the ability to identify and adapt to threats as and when they arise has become a critical component of the domestic and foreign policies of most countries. Moreover, the exploitation of new technologies in order to commit cyber-terrorist attacks requires especial effort, [76] since there are numerous critical infrastructures and computer networks that may be damaged or compromised, with severe repercussions on the community's safety.

Hence, if the aim is to prevent and/or develop the most appropriate incident handling methodology, early warnings are a crucial part of intelligence activity. In fact, counter-terrorism strategies require clear understanding of how terrorists are likely to attack, what targets they will choose, what weapons they will use and what tactics and methods they will employ to deliver the attacks.

As Devost and Pollard write, 'when terrorists take us by surprise (…) it is because we did not identify or understand the change in these areas, and adjust our strategies accordingly. Terrorists take advantage of this fact, not only to increase the immediate damage of their attacks, but to increase the longer-term psychological impact'.

With regard to this particular issue, early warnings must be treated not only as all the information deriving from intelligence activity but also as alert signals collected in different environments using different techniques and tools.

---

[75] The White House itself has recently been accused of knowing that terrorist attacks were likely to happen; eight months later, the White House admitted that it had indeed received early warnings. See Talbot D., "See no evil", 16 May 2002. The text is available at the following URL: http://www.salon.com/news/feature/2002/05/16/knew/index_np.html.

[76] Devost M. G., Pollard N. A., "Taking Cyberterrorism Seriously – Failing to Adapt to Emerging Threats Could Have Dire Consequences", 27 June 2002. The text is available at the following URL: http://www.terrorism.com.

Moreover, the ongoing war against terrorism should take serious consideration of the relationship between information warfare [77], cyberspace and terrorism, for it may be of valuable assistance in the detection of early warnings.

Terrorism seems to be closely related to the Internet; indeed, case studies confirm that the Net is used both against and by terrorists. It is therefore crucial to recognize that the increased threat of global terrorism is a real one.

By way of example, after the attacks on the World Trade Centre and the Pentagon, some of the most immediate retaliations were launched in cyberspace. The following are some cases:

- a hacker defaced thousands of websites in protest and re-routed all traffic to the attackers' website;[78]
- the Chaos Computer Club – a German hacker group – ironically condemned the use of the Internet 'as a battleground' because 'communication networks are essential for contributing to international understanding';
- 'crackerz' retaliated against the terrorist attacks by disabling ISPs in Palestine and seeking to destroy ISPs in Afghanistan. At the moment, they have more or less 1000 computers under their control and are apparently supported by crackerz around the world (UK, USA, Russia, Brazil, Mexico, China, Australia, Canada, India, Egypt, Germany, Holland and Denmark);
- in Canada, a Jewish group (B'nai B'rith) helped law enforcement officials to close down websites promoting or support Islamic terrorism;

On the other hand, also terrorists use the Internet. There follow the three main groups of possible harmful, dangerous actions:[79]

- defacement of electronic information sites (mostly in the United States and allied countries) and spreading (dis)information and propaganda. Terrorists, as well as dissidents and sympathisers, are aware that the Internet is an outstanding device with which to spread their organisations' messages and further their cause: it is the most widely used medium, uncontrolled, and with global reach. A huge number of organizations exploit Internet capabilities, examples being the Provisional Irish Republican Army (PIRA), the Euskadi Ta Askatasuna (ETA), the Mexican Zapatistas, and the Chechen rebels;[80]
- denial of service to legitimate computer users (in the United States and allied countries) through Denial of Service Attacks (DoS) and/or the use of worms and viruses, and the exploitation of inherent computer security vulnerabilities;
- unauthorized access to systems and networks (belonging to the United States and allied countries), potentially resulting in critical infrastructure outages and corruption of vital data.

---

[77] Information warfare is generally defined as the actions taken to achieve information superiority by affecting an adversary's information, information based processes, and information systems, while defending one's own information, information based processes, and information systems.

[78] Kovacich G. L., Jones A., "What InfoSec professionals should know about information warfare tactics by terrorist – Part I", in *Computers & Security*, Elsevier Science, vol. 21, No 1, p. 35-41.

[79] Institute for Security Technology Study at Dartmouth College, "Cyber Attacks during the War on Terrorism. A Predictive Analysis", 22 September 2001.

[80] Kovacich G. L., Jones A., "What InfoSec professionals should know about information warfare tactics by terrorist – Part II", in *Computers & Security*, Elsevier Science, vol. 21, No. 2, p. 113-119.

Case studies suggest that cyber attacks generally accompany physical attacks and political conflicts. There have been many recent cases of attacks against public and private institutions consequent on specific events. For example, Chinese hacker groups immediately reacted to the mid-air collision between an American surveillance plane and a Chinese fighter aircraft on 1 April 2001 by organising a massive week-long campaign of cyber attacks against American targets.[81] Moreover, top-level domain web defacements in India attributed to pro-Pakistan attackers have increased from 45 to over 250 in just three years.

Attacks are mainly directed against high-value electronic targets 'whose disruption would have symbolic, financial, political, or tactical consequences'.[82]

Particular concern is also generated by the subjective profiles of potential perpetrators; as said, offenders are not only terrorists but also a wide range of differently motivated subjects. American studies have identified the following categories:[83]

terrorist groups; it is still not possible to determine whether these are actually developing an information warfare and cyber-attacks strategy. To date, there have been no cases of terrorist groups using Internet and ICT as weapons, but terrorists are known to make extensive use of information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely;[84]

targeted nations/states; US sources report that various foreign nations [85] support terrorism and engage in espionage against Western countries using ICT infrastructures and cyber-attacks. Their targets are both public and private organisations. China, North Korea, Cuba and Russia are believed to be developing cyber warfare capabilities which could be also used for economic purposes;

terrorist sympathisers and anti-US hackers; cyber-attacks committed by these groups of people are far more likely than those perpetrated by terrorists themselves. As far as the business sector is concerned, the main threats are raised by anti-globalisation activist groups which applaud attacks against American capitalism. In some cases, their support for terrorist causes takes concrete form in direct attacks launched over the Internet (e.g. defacement and denial of service) against corporate computer systems;

thrill seekers; these are hackers and 'script-kiddies' who seek notoriety by getting involved in cyber-conflicts or trying to launch high profile attacks. Often, they are motivated not by political or ideological dogma but simply the desire to attract attention. These offenders do not cause particular concern because, generally, they had less expertise and do not seek to provoke serious damage. However, their potential should not be underestimated because they are capable of causing economic damage and disruption; for example, dDoS attacks against major

[81] Institute for Security Technology Study at Dartmouth College, *cit.* 79, p. 9.

[82] *Ibid.*

[83] Institute for Security Technology Study at Dartmouth College, *cit.* 79, p. 12-13.

[84] *Ibid.*

[85] Some examples are Afghanistan and the other U.S.-designated supporters of terrorism, such as Syria, Iraq, Iran, Sudan and Libya.

websites, such as those in February 2000 against CNN and Yahoo!, together with recent computer worms and viruses, were not politically or financially motivated but nevertheless had a significant economic and technical impact.

11. EARLY WARNINGS USE IN THE BUSINESS ENVIRONMENT

As said, early warnings have exceptionally been also applied to the business sector. Fortunately, the good news is that these exceptions generally fall in with efforts to prevent crime and violence. Notwithstanding general agreement on their importance – for example for the prevention of workplace violence – the bad news is that, at the moment, there are no general findings on, or analytical analysis of, their efficacy and effectiveness.

It thus seems useful to consider these initiatives, principally in order to initiate discussion on early warnings theories, in the hope that they will be given the attention that they deserve.

The next sections will analyse the use of early warnings in the following frameworks:

- workplace violence prevention;
- employee theft and dishonesty prevention;
- IT security management.

12. THE USE OF EARLY WARNING SIGNS IN THE PREVENTION OF WORKPLACE VIOLENCE

12.1 INTRODUCTION TO WORKPLACE VIOLENCE

The questionnaire prepared for this Study did not specifically ask whether the company had experienced cases of workplace violence over the previous two years. However, it is important to focus on this issue as well, because it is closely related to employee safety and business security. Moreover, as said, workplace violence is one of the few criminal phenomena to which early warning theory has already been applied.

Different definitions are given to workplace violence, but the most frequent are the two that follow:[86]

[86] Kaufer S., Mattman J., "Workplace Violence: An Employer's Guide'. The text is available at the following URL: http://noworkviolence.com/articles/employers_guide.htm.

1. the first closely relates to the mass media representation of the problem and refers to cases of violence by an armed, disgruntled employee or a customer who shoots employees, supervisors and managers selectively or indiscriminately;

2. the second is a closer match with reality: workplace violence is defined as any act against an employee which creates a hostile work environment and harms the employee, either physically or psychologically. These acts include all types of physical and/or verbal assault, threat, coercion, intimidation, and all forms of harassment.

The urgency of the issue is borne out by the huge amount of information available: for example, many public institutions have a website on which they publish reports and guidelines for recognizing and preventing physical and verbal violence in the workplace. Moreover, criminological studies have sought to determine why the phenomenon is so common; while public and private agencies organize training programmes on how to detect and defuse violence in the business environment.

However, that the great majority of these initiatives, as well as of qualitative and quantitative surveys, have been undertaken in America. In Europe, by contrast, there is a general lack of interest in the phenomenon, both within Member States and at the level of the European institutions.

Fortunately, there are exceptions. Some Member States have already updated their legislation and financed research and surveys on the phenomenon. By way of example, in Great Britain, during the 1980s and 1990s, violence at work was an issue that caused increasing concern.[87] The Health and Safety Executive, the government agency with responsibility for violence at work, produced guidelines on preventive strategies, while legislation was introduced which recognised violence at work as a health and safety issue. Since 1995, the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) have required employers to report to their enforcing authority (usually the HSE or Local Authority, depending on the type of premises) acts of physical violence which cause a fatality, a major injury, or absence from work for more than three days.

The need to focus on workplace violence is confirmed by the findings of available data analysis and reported cases: for example, an average of 20 workers are murdered each week in the United States, and the majority of these murders are robbery-related. In addition, one million workers are assaulted annually.[88] According to the Workplace Violence Headquarters, the U.S. Department of Justice considers the workplace to be the most dangerous place in America. The problem is so pervasive that the Centre for Disease Control classifies workplace violence as a national epidemic.

To provide some figures: in the United States, 1 in 4 workers are attacked, threatened or harassed each year; and the costs are estimated at:

- $13.5 billion in medical costs/year;

[87] Budd T., *Violence at Work: Findings from the British Crime Survey*, Home Office, October 1999.

[88] Department of Health and Human Services, *Understanding and Responding to Violence in the Workplace – Guidelines*, March 1997, p. 1.

- 500,000 employees miss 1,750,000 days work/year;
- 41% increase in stress level.

Obviously, these figures include incidents committed not only by insiders but also by outsiders; as regards the former, however, there is a lack of clear and more specific data on internal cases.

In Great Britain, for example, the Home Office research study '*Violence at Work: Findings from the British Crime Survey*'[89] defines violence at work as 'all assaults or threats which occurred while the victim was working and were perpetrated by members of the public'. Hence, they do not include cases of violence by co-workers. According to the study, they are not provided because the number of incidents of intra-colleague violence counted in the British Crime Survey (BCS) is too small to allow separate analysis. The 1998 BCS estimates that only 0.1% of working adults had been assaulted by a colleague while working in 1997, and 0.2% had been threatened by a colleague. However, if trends can be taken as indicative, workplace violence committed by both insiders and outsiders is on the increase.

As specifically regards co-workers delinquency, neither are American assessments homogeneous, owing to a lack of information and/or analytical studies; according to Workplace Violence Headquarters, 3% of perpetrators are former employees, while 20% are current employees.

In general, the prevailing underestimation of internal violence can be explained – perhaps – on the grounds that both small business owners and corporate executives believe that there is no need for training or crisis planning to deflect or eliminate violence. There are, in fact, two myths embraced by management[90]: the first is called the *Ostrich Syndrome* whereby almost all companies believe that violence will never happen in their environment; as a consequence, none of the cases that occur every day are reported by victims because of an evident lack of interest by management. The second myth can be summarised as '*it can't be prevented!*'; this popular belief is contradicted by the figures: in fact, there are clear warning signs for at least 85% of incidents.

This figure is of particular relevance to this Study. As explained, early warning strategies have yet to be implemented in the business environment, and the lack of information and of cases, as well as of best practices, greatly restrict opportunities to test the potential of these preventive measures. The following section will thus consider workplace violence issues as a case-study on how early warnings work and their role and value in the prevention of crime.

[89] Budd T., *cit.* 87.

[90] All this information is available at the following URL: http://www.workplace-violence-hq.com.

12.2 LEARNING THE WARNING SIGNS OF WORKPLACE VIOLENCE

The starting points for discussion on the implementation of early warnings to prevent workplace violence are the following *workplace violence perpetrators exhibit clear warning signs before committing a crime*; moreover, *potential or actual violence among employees typically escalates if it is not defused*. These considerations are completed by the observation that behind many workplace incidents there is a management and company failure to identify the danger early enough, or to prepare and respond appropriately.[91]

These two assumptions evidence the close parallelism between the use of early warning signs in the prevention of workplace violence and their implementation against the more general category of occupational crime. Also the latter, in fact, is very often anticipated by signals which, if recognised, can warn that different types of attacks and offences may occur.

To return to workplace violence, the 'early warning signs approach' has enabled experts to develop indicators with which to identify perpetrators before the crime occurs.

Anthony Baron,[92] for example, starts from the above two assumptions to identify three levels of violence, and the warning signs that generally occur at each of them. These levels are applicable specifically to co-workers and to the relationships between the clients and patients of medical services.

Level one (early warning signs)

The person:

- refuses to co-operate;
- spreads rumours and gossip to harm others;
- consistently argues with employees/clients;
- is belligerent toward employees/clients;
- constantly swears at others; and/or
- makes unwanted sexual comments.

Level two (escalation of the situation)

The person:

- increasingly argues with customers, vendors, employees and management;
- refuses to obey agency policies and procedures;
- sabotages equipment and steals property for revenge;
- verbalizes wishes to hurt employees and/or management;
- sends sexual or violent notes to employees and/or management;

---

[91] Kennish J. W., "Violence in the Workplace", 2000. The text is available at the following URL: http://www.kennish.com/workplaceviolence/.

[92] Baron A., *Violence in the Workp*lace, 1993.

- sees self as victimized by the Department (me against them).

Level three (further escalation, usually resulting in an emergency response)

The person frequently displays intense anger resulting in:

- recurrent suicidal threats;
- recurrent physical fights;
- destruction of property;
- utilization of weapons to harm others;
- commission of murder, rape and/or arson.

In addition to these indicators, there are others – so-called *performance indicators* – which signal whether the work environment is characterised by violence, or even if it is *at risk*. These signals may be exhibited by potential perpetrators, by those who feel that they are potential victims or have already been victimised, and by people in fear of being victims.

Although only one of the signals may be apparent, it is more likely that a pattern will be recognizable. Moreover, the occurrence of these signals does not necessarily mean that a violent act is going to occur, but they are certainly indicative of a change in the normal routine of the work environment, and thereby evidence the existence of other types of problem. Whatever the case may be, these signals are valuable for the understanding and prevention of internal problems and conflicts.

Examples of these performance indicators have been listed by Anthony Baron and reported by the American Department of Health and Human Services:

- attendance problems: excessive sick leave, excessive tardiness, leaving work early, improbable excuses for absence, higher than average absenteeism rate, high number of on-the-job incidents;
- impact on supervisor's/manager's time: supervisors spend an excessive amount of time trying to coach and/or assist and help with individual problems, re-doing the employee's work or dealing with his/her problems and concerns;
- decreased productivity: high number of mistakes, missed deadlines and wasting of work time and materials;
- inconsistent work patterns: alternating of periods of high and low productivity and quality of work;
- inappropriate reactions: overreactions to criticism, mood swings;
- concentration problems: distraction, difficulties in recalling instructions, project details and deadline requirements;
- safety issues: increasing number of accidents, disregard for personal safety as well as for the functionality and security of machinery and equipment;
- poor health and hygiene: evident changes in personal grooming habits;
- evidence of possible problems of alcohol use and abuse;
- evidence of serious stress and/or problems in the employee's private life: crying, higher number of personal phone calls, separation;
- continual excuses/blame: inability to accept responsibilities;
- unshakeable depression: low energy, little enthusiasm.

Although these indicators are quite precise, they are not the only means with which to understand and solve the problem of workplace violence. Early warnings should be supported by other countermeasures and initiatives.

The Workplace Violence Headquarters considers early warnings to be part of a more general pattern known as POSTAL.

POSTAL is the acronym for the following formula:

Profile + **O**bservable Warning Signs + **S**hotgun + **T**riggering Event = **A**lways **L**ethal

The chart that follows explains each of these terms and gives examples of what they refer to.

POSTAL			
Profile of potentially violent person	*Observable warning signs (often newly acquired negative traits)*	*Shotgun (it is not required for non-lethal violence)*	*Triggering event (no way out, no more options)*
previous history of violence, especially towards the vulnerable	violent and threatening behaviour (hostility, approval of the use of violence, direct or veiled threats of harm etc)	familiarity with weapons	being fired, laid off, suspended or passed over for promotion
loner, withdrawn, feels that no-one cares for him/her, views changes with fear	'strange' behaviour (becoming reclusive, deteriorating appearance/hygiene etc)	brings a weapon to the workplace or makes inappropriate references to gun and weapons use	disciplinary action, criticism from boss or co-workers
emotional problems (substance abuse, depression, low self-esteem)	emotional problems (drug, alcohol abuse, stress, depression etc)		bank or court action
career frustration (significant tenure in the same job, migratory job history)	performance problems (including, for example, problems with attendance)		benchmark date (for example: company anniversary, chronological age, other particular anniversaries)
antagonistic relationships with other people and especially co-workers	interpersonal problems (numerous conflicts, hyper-sensitivity, resentment, intimidating, belligerent, harassing, bullying or other inappropriate and violent behaviours etc)		failed or spurned romance; personal crisis
some type of obsession (weapons, violence-related hobbies, romantic/sexual, zealot)	'at the end of his rope' (indicators of impending suicide or has an unexpected plan to 'solve all problems'		

While the necessary starting point is awareness on the part of the company of the importance of ensuring a secure workplace environment, the next step is the development and implementation of concrete strategies and initiatives to guarantee security and crime/violence prevention in practice. Prevention can be obtained in two ways:

- as regards new employees, the hiring process should be conducted with particular attention to possible warning signs, such as those already seen. Careful interviews and background checks are thus essential;
- although internal human resources must be treated properly, they should be managed using, for example, the following measures: a zero-tolerance policy – effectively explained and implemented – combined with controls, employee training, counselling, security measures.

13. EARLY WARNINGS AND EMPLOYEE THEFT AND DISHONESTY PREVENTION

13.1 UNDERSTANDING WHY EMPLOYEES COMMIT INTERNAL CRIMES. A CRIMINOLOGICAL OVERVIEW

Discussion of why employees commit frauds and abuses tends to conclude that perpetrators have abnormal personalities or are not law-abiding. In other words, they are 'bad' people, far removed from the norm. This, however, is a misconception. The truth is that 'good' people, too, damage the companies for which they work, and they do so much more frequently than the general public, and also employers, generally believe.

Hence, at the moment, 'the biggest hurdle for most people to get over in terms of understanding occupational fraud is to realize that *anyone* can commit fraud'.[93]

Since internal crimes affect almost all companies and are committed by employees at levels – employees who cannot be generally categorised as deviant and/or *sick* – it is thus extremely important to leave misconceptions aside and examine why and how they occur.

The essential consideration is that occupational crimes do not spring from a single cause or factor; 'instead, there is a complex set of motivations that, when combined in the right environment, produce the impetus for an employee to begin committing fraud'.[94]

From a theoretical perspective, this matches the assumptions of so-called *opportunity theories*.

In practice, every employee –his/her attitudes towards crime notwithstanding – has *opportunities for crime* provided by the organizational environment in which s/he

[93] *Ibid*.

[94] *Ibid*.

works. These opportunities, as well as the decision to commit a crime, will differ according to the employee's position, and to the tasks and responsibilities assigned to him/her. Consequently, also the types of crime will differ from one department of an organization to another, and from one individual (or small group of individuals) to another.

Theoretically, it can therefore be assumed that, given suitable opportunities, employees at all levels will exploit and make use of such opportunities to commit every kind of occupational crime.

According to Case, in fact, it is the opportunity, not the need, to steal that is the primary cause of employee theft, By contrast, if an employee is in real need of money, before committing the crime, s/he also considers the presence of a suitable opportunity and then weighs the risks/consequences of his/her conduct. Moreover, as explained by Croall, 'employees at all levels of the occupational hierarchy have the opportunity to abuse or exploit aspects of their occupational roles, ranging from the seemingly trivial abuse of employers' telephones or computers, to more profitable and organized activities which are more readily definable as 'criminal''.[95]

According to surveys and studies, different types of internal perpetrators commit different types of crime and abuse: there those who intentionally move among jobs with the sole intention of stealing from and damaging the employers In general, however, occupational criminals are not career criminals: for example, the majority of internal crimes against small businesses are committed by long-term and trusted employees.[96]

Comer has well illustrated differential that characterises this opportunity approach with the following scheme: [97]

'all people are supposed to have the opportunity to commit fraud:

- against their employer
- against suppliers and customers of their employer
- against third parties
- against government department

opportunity is driven by four factors:

- the access the perpetrators has or can contrive to premises, accounts, assets and computer systems
- his skill in identifying the opportunity and exploiting it
- the time he has available to plan and successfully execute the fraud
- his rank or seniority: generally the more senior an employee becomes, the less restrictive the controls

these factors obviously differ from a person to another and from one time to another'.

---

[95] Croall H., *White Collar Crime*, Open University Press, 1992, p. 45.

[96] ACFE, *Small Business Fraud*, April 2002, p. 4.

[97] Comer M. J., *cit.*6, p.43.

Many authors on opportunity theories have sought to explain the relationship among insiders, internal opportunities, personal motivations/attitudes and the commission of occupational crimes. Despite a common point of departure, some of them have arrived at completely different conclusions.

Comer, for example, maintains that 'corporate frauds result from a combination of *motivational* and *situational* factors, in which the critical point is the presence of an *opportunity* and a *motivation*. It follows that if opportunity can be denied, either by preventative controls or the obvious threat of detection, one part of the equation is removed. Changing the motivation of criminals is an entirely different matter, although risks are significantly reduced when the organization follows the highest ethical standards and ensures everyone connected with it complies with them'.[98]

Cressey has developed of one of the most widely endorsed theories on the basis of empirical studies and analyses which combine opportunity with other elements. Starting from extensive research on more than 200 inmates at Midwest prisons incarcerated for embezzlement, Cressey first formulated the hypothesis set out in his study *Other People's Money: A Study in the Social Psychology of Embezzlement*: 'trusted persons become trust violators when they conceive of themselves as having a financial problem which is non shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalisations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds of property'.

Cressey uses a triangle to represent his theory, the so-called *fraud triangle theory*.

There are three main factors (each representing a side of the triangle) that, when combined, induce people to commit occupational fraud: one side corresponds to a *perceived non shareable financial need*, the secondto a *perceived opportunity,* and the third to the perpetrator's ability to *rationalize* the illegal conduct by finding a personal justification for his/her illicit conduct.

On generalising this scheme from embezzlement to occupational crimes in general, one may say that for a *trust violation*[99] to occur all three elements must coexist: *perceived motive*, *perceived opportunity* and the *ability to rationalize*.

As regards perceived motives, Cressey stresses that these should be perceived as non shareable financial problems; in other words, the (potential[100]) offender considers his/her problems to be a stigma, or even as shameful, so that s/he finds it impossible to talk about his/her personal situation with others. Possible examples are financial problems related to drug and/or alcohol addiction, gaming and gambling debts. Cressey identifies six basic categories of non shareable problems:

- violation of ascribed obligations: the subject starts thinking about the real possibility that s/he will not be able to repay his/her debts;

[98] Comer M. J., *cit.*6, p. 46.

[99] Trust violation is here used as synonym of occupational crimes.

[100] When the person perceives that he/she has a non shareable problem, he/she is still not a criminal.

- problems resulting from personal failure: the subject experiences problems – such as drug addiction – that result from personal judgement;
- business reversals: the subjects faces the possibility/probability of business failure;
- physical isolation: the subject is isolated (or rapidly departs) from people who could help him/her solve his/her problems;
- status gaining: the subject seeks to maintain a certain status but does not have the financial means to do so;
- employer-employee relations: the subject feels s/he has been mistreated by his/her employers.

As said, having a non shareable problem is only one part of the criminal pattern; the second is the perceived opportunity. The subject must be sure – or at least believe – that s/he will not be caught and that s/he can solve his/her problems in secret.[101] Perceiving the opportunity thus involves the belief that there is a way to deal with the problem rapidly without harmful consequences.

This second side of the triangle is of close relevance to the issues addressed by this Study: it indirectly refers to the company role and its possible responsibilities, given that opportunity reduction should be part of crime prevention strategies and policies. If opportunities are not eliminated, or at least controlled, the company will not be able to administer security issues properly. Put otherwise, if an employee perceives that there are no concrete risks related to given (perceived) opportunities, the company is not defending itself against crime. 'Generally employees only commit fraud when they perceive that there is a way to commit the crime in such a way that the company will not realize a fraud has occurred'.[102]

From the company perspective, if it implements an efficient and effective internal control system, letting employees know that that their behaviour is being supervised should induce them desist from crimes and abuses.

The last leg of Cressey's triangle is rationalization; the offender rationalises his/her conduct, so that – in his/her eyes – it becomes somehow legitimate, or at least justifiable.

But how can employees convince themselves that stealing is in some way acceptable or reasonable?

This issue has been examined by various criminologists, who draw different conclusions. One of the most accredited approaches consists of *anomie theory*. Without entering into the academic debate and into the literature, the principal feature of this approach to crime is that it is based on realism.[103] On this view – and

---

[101] Also Comer agrees that "*the most common reason why people commit fraud is very simple: they are greedy and they believe they will not get caught. They do not care a jot about the effect the fraud will have on their company, colleagues or managers*". Comer M. J., *cit.*6, p. 30.

[102] ACFE, *cit.* 96, p. 7.

[103] Unlike the previous theories, realism does not focus on one single element of the crime (the offender, the victim, the social reaction, the criminal behaviour itself); on the contrary, it considers every aspect of the criminal process; "*the central aim of realism is to be faithful to the reality of crime: to the fact that all crimes must, of necessity, involve rules and rule breakers, and offenders and victims. (…) realism intends to bring together all aspects of the process: in this its approach emphasizes synthesis rather than a simple dismissal of opposing theories*". Maguire M., Morgan R., Reiner R. (edited by), *The Oxford Handbook of Criminology*, 2nd ed., Clarendon Press, Oxford, 1997, p. 485.

differences among specific studies notwithstanding – anomie theory identifies the causes of crimes as consisting in the contradiction between the culture of meritocracy, which holds out the dream of equal opportunities, and the real class structure that prevents it.

If this approach is applied to the business sector, crime can be considered as bridging the gap between opportunities and aspirations: when aspirations cannot be fulfilled by using legitimate opportunities, unconventional methods will be found. Obviously, this situation does not arise whenever an individual feels that his/her aspirations are not matched by his/her opportunities and means. In fact, the decision not to commit a crime depends on other factors as well, such as personal beliefs and values, education, morality, and religion.

In a corporate environment, a conflicting anomic situation may arise from the existence of perceived artificial barriers and/or obstacles against aspirations raised by the company itself. These barriers will differ from one company to another according to the type of organization.[104] They may, for example, be related to race, sex, age and/or class.

The triangle has recently also been used by Felson, who argues that for any crime to occur there must be a coincidence of three basic elements: an *offender* (suitably motivated), a *target* (or victim) and the absence of a suitably capable *guardian* (which comprises both human and physical/technological controls).[105] This scheme is usually referred to as the *Felson triangle of crime*.

This model is part of the wider Routine Activity Approach used mainly to explain predatory crimes.[106] It accordingly assumes that for such crimes to occur there must coexist, in time and space, the following three elements: a *likely offender*, a *suitable target* and the *absence of capable guardians*. Given the likely offender, this approach focuses on the other elements: the guardian need not necessarily be a police officer or a security guard; s/he may be anybody whose presence obstructs or discourages the commission of a crime. As said, the other element is the target. The Routine Activity Approach uses this term instead of 'victim' because they are not always coincident: in fact, the victim may be absent from the crime scene.[107]

As well as a person, therefore, the target of crime may be an object whose position in time and space puts it at greater or lesser risk of criminal attack.

Under this approach there are four main factors which influence a target's risk of criminal attack:[108]

- value;

---

[104] Comer M. J., *cit.*6, p. 33.

[105] Sutton A., Tait D., McKenzie S., Bavinton F., "Internet Crime Prevention", paper presented at the *Conference Internet Crime*, Melbourne, 16-17 February 1998.

[106] Felson M., Clarke R. V., "Opportunity makes the Thief. Practical Theory for Crime Prevention", in *Police Research Series,* Paper 98, Home Office.

[107] The authors explain that "*the owner of a TV is normally away when a burglar takes it. The TV is the target and it is the absence of the owner and other guardians that makes the theft easier*". Felson M., Clarke R. V., *cit.*106, p. 5.

[108] *Ibid*.

- inertia;
- visibility;
- access.

Obviously, all these factors are seen from the offender's perspective. The result is that 'for the usual predatory crime to occur, a likely offender must find a suitable target in the absence of a capable guardian. This means that crime can increase without more offenders if there are more targets, or if offenders can get to target with no guardians present. This also mean that community life can change to produce more crime opportunities without any increase in criminal motivations'.[109]

This *triangular approach* may seem a simplistic or even gross oversimplification, but if applied to a workplace it is not too distant from reality. Where there is a lack of controls and implemented internal rules and policies there is also a lack of so-called *informal control* by co-workers. Moreover, when the workplace is characterised by indifference, or is unwelcoming, employees tend to adopt an individualistic approach and do not identify with their colleagues and/or, in general, with the company. This sense of being far ahead of one's own co-workers often creates situations suited to crimes, and in particular petty crimes like thefts of small amounts of money or personal effects. From a wider perspective, this kind of situation can also increase the number of crimes against the company itself; examples are provided by the replies to the questionnaires used for this Study: laptop thefts, different types of fraud (for instance, attempts to defraud the company by means of inflated expenses accounts), vandalism, sabotage of plant, abuses in the use of information technologies such as theft of company time for recreational surfing.

However, a company's perception of this *triangle* and of its possible consequences is often distorted. The following are examples of the misconceptions that reduce knowledge and awareness about the risks to which a company is exposed:

'well paid or adequately paid employees are less likely to steal';

'honest and loyal employees will report other employees who steal';

'recently engaged employees commit thefts while senior employees can be generally trusted'.

These statements are anything but true; companies are unaware of the fact that employee theft and dishonesty exist to the extent that management allows and budgets for them. Moreover, it seems that companies have not yet understood that effective internal management and controls will enable them to reduce losses.

Some criminologists working with the opportunity approach have focused on the company role and responsibilities, concluding that – in reality – occupational crimes depend principally on *workplace conditions*.

Hollinger and Clark, for example, point to job dissatisfaction as the prime cause of employee thefts; this being the main result of their research on over 9,000 American workers in three different sectors: retail, hospitals and manufacturing.[110]

---

[109] *Ibid*.

[110] Hollinger R. C., Clark J. P., *Theft by Employees*, Lexington, 1983.

They divided employee deviance into two main categories: 1) acts against property (e.g. theft, embezzlement); 2) acts infringing the norms regulating the minimal and/or acceptable levels of productivity (e.g. counterproductive behaviours).

As regards the first category, in all the three sectors examined, approximately one third of the employees interviewed admitted that they had committed some form of property crime. In the retail sector, for example, the most recurrent crimes were the misuse of discount privileges, store merchandise theft and the requested payment for more hours than worked. In the manufacturing sector, theft of raw materials used in production, as well as of company tools or equipment, and requests to for payment for more hours than had been worked, were the property crimes most frequently reported.

As regards production violations, almost 65% of the employees interviewed, in each sector, answered that they took excessive time for lunch breaks, came to work late or left earlier in the evening, and abused sick leave policy. These offences were much more common than property violations and infringements.

Hollinger and Clark then sought to identify the factors that influenced, contributed to and/or determined the commission of internal crimes. The following were the ones isolated:

- income

Since there is no proven relationship between personal income and deviance, the former cannot be considered a predictor of crime. However, a correlation can be hypothesised as follows: employers on low incomes will tend to be in greater need of extra money. The questionnaires used for this Study showed that in almost all cases of crimes experienced over the previous two years by the companies interviewed the main motivation had been *profit*.

- Age

Unlike income, it seems that there is a strong relationship between age and deviance. According to Hollinger and Clark's findings, younger employees are much more likely to steal. The authors concluded that this was related to the fact that younger employees are less involved in the company and are less committed and loyal to the organization.[111]

- Position

In this case, too, there is a strong relationship between the factor and employee deviance: constant contact with proprietary assets and goods can give rise to a greater propensity to crime due to the absence of concrete obstacles or difficulties. In a certain sense, this feature is an example of Cressey's perceived opportunity. However, Hollinger and Clark take another approach: although opportunities do exist, they are only a 'secondary factor'. Opportunities will only predict how employees will commit a crime. The point is that employees must be motivated by other factors: once a worker has decided to commit the crime, s/he will find an

[111] "*Societal rules and codes of conduct generally have less importance to young people than they do to older individuals*". ACFE, *cit.* 96, p. 13.

opportunity to do so. In this sense, opportunity is the second level of the decision by an employee to abuse his/her position in a company.

- job satisfaction

Regardless of age, all groups of employees (but especially young people) discontented with their jobs are more likely to commit crimes against their company. Very often, the sense of discontent and/or dissatisfaction is related to perceived unfair treatment.

- organizational controls

Can controls prevent crime from occurring because of their deterrent effect? And what attitude towards controls do employees generally have? Hollinger and Clark conclude that internal controls are able to reduce employee deviance but their effectiveness is nonetheless limited. The problem is that controls must be well balanced and organised; otherwise they will provoke a negative effect, rather than a positive one: for example, while a certain amount of control is valuable in preventing internal dishonesty, too much control may produce a negative reaction. The company must not create an atmosphere of suspicion and paranoia.

What is of greatest importance in crime prevention is the employees' *perceptions* of controls. The mere fact that employees perceive that management pays a certain degree of attention to crime prevention may have greater deterrent effect than any concrete controls put in place. According to Hollinger and Clark, 'the more people believed they would be caught, the less likely they were to steal, regardless how strong the actual controls were. This finding reinforces the notion that perception of detection is the key to preventing employee fraud'.[112]

Finally, one of the most interesting aspects of Hollinger and Clark's approach consists in two broad hypothesises which although intuitive and thus obvious are, like all simple things, extremely important. First, they hypothesize that efforts to reduce theft and internal dishonesty will be useless if the underlying causes are not reduced as well. Underlying causes are, for example, employee dissatisfaction, a lack of ethics, or perceived inequity. If these are not affected, they may cause what Hollinger and Clark call a *hydraulic effect*: tightening controls on property may provoke more serious deviance which affects corporate productivity. Secondly, they assume that increased management sensitivity to internal workforce reduces all forms of workplace deviance.

Specifically, according to Hollinger and Clark, management should pay attention to the following four elements: 1) a clear understanding of theft and dishonest behaviour; 2) continuous dissemination of positive information reflective of the company's policies; 3) enforcement of sanctions; 4) publicizing the sanctions.

Hollinger and Clark make one observation that is worth quoting in full, because it is extremely pertinent if the findings of our case-study analysis conducted on the returned questionnaires are considered as well:

'perhaps, the most important overall policy implication that can be drawn … is that theft and workplace deviance are in large part a reflection of how management at

[112] ACFE, *cit.* 96, p. 14.

all levels of the organization is perceived by the employee. Specifically, if the employee were permitted to conclude that his or her contribution to the workplace is not appreciated or that the organization does not seem to care about the theft of its property, one would expect to find greater involvement. In conclusion, a lowered prevalence of employee theft may be one valuable consequence of a management team that is responsive to the current perceptions and attitudes of its workforce'.

This issue will be analysed in the following section.

13.2 INTERNAL MANAGEMENT AND RELATIONSHIPS TO INTERNAL DEVIANCE

Many experts – who deal daily with business security and fraud prevention issues[113] – recognize that internal management style is crucial: 'there are some clear profiles and experience suggests that fraud risks and management style interact',[114] although is not possible to quantify this interaction precisely.

The role of management is thus vital, and managers must be made aware of this. In actual fact, they do not ignore their company's problems with crimes (internal and external), but they tackle them only partially or unscientifically.[115] Moreover, they have uncertain and sometimes ambiguous attitudes towards crime. Instead, they must make clear to employees what it is they expect of them, and at the same time they must set a good example. As Case emphasises,[116] 'as long as management embraces erroneous information about employee theft and fails to become educated to the facts, employee theft will remain a major drain of profits and employee morale'.

Starting from the premise that a clear workplace culture is extremely important, Challinger, too, underlines that 'a strong workplace culture will not develop from words alone. It is essential that management's own attitudes and behaviour reflect the desired culture. Negative behaviour by management or those in supervisory roles has a particularly damaging effect on workplace culture'.[117]

The positive results that may derive from this different approach to crime may be useful in other respects as well – as some researchers have sought to demonstrate. For example, Trevino and Victor[118] showed that when fast-food restaurant

---

[113] The most authoritative are usually Certified Fraud Examiners (CFE).

[114] Comer M. J., *cit.* 6, p. 39.

[115] Challinger D., "Will Crime prevention ever be a Business Priority?", in Felson M. and Clarke R. V. (edited by), *Business Crime Prevention*, Criminal Justice Press, 1997.

[116] Case J., "Over Employee Theft. The Profit Killer", 1999. The text is available at the following URL: http://www.employeetheft.com/casemain.htm.

[117] Challinger D., *cit.* 115, p. 51.

[118] Trevino L. K., Victor B., "Peer Reporting of Unethical Behaviour: a Social Context Perspective", in *Academy of Management Journal*, 35:38-64, 1993.

employees were specifically asked to report any cases of internal thefts that they witnessed, the number of these crimes dropped.

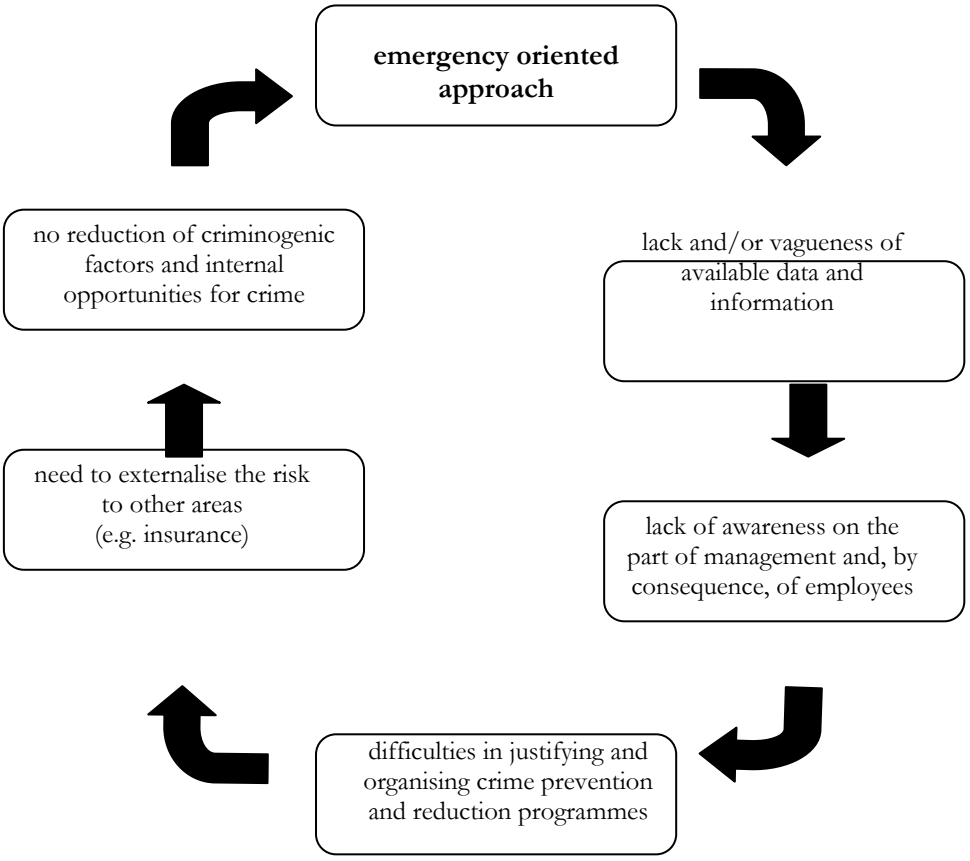
Also Shepard and Durston state that 'companies with the lowest incidence of employee theft are those with a clear commitment from top executives to line supervisors that theft will not be tolerated'.[119]

The collection of early warning signs should therefore also be oriented towards high-level employees and management, in order to implement strategies and initiatives that make them aware of the complexity of workplace relationships.

[119] Shepard I. M., Durston R., *Thieves at Work: An Employer's Guide to Combating Workplace Dishonesty*, Washington, The Bureau of National Affairs, 1988.

13.3 THE ROLE OF EARLY WARNINGS

According to the foregoing discussion, early warnings are valuable to all those businesses which agree that the private sector must change its attitude towards crime. In particular, businesses must break the vicious circle that characterises their emergency-oriented approach to crime, as schematised in the following figure.



Although businesses generally do take crime seriously, this emergency-oriented approach does not produce appropriate countermeasures, and it does not allow the correct down-management of losses. As schematised in the figure, one of the main causes of this vicious circle is the lack and/or vagueness of available data and information about the criminal risks faced by a company. Businesses are thus frequently ignorant of internal criminal dynamics and criminogenic factors, and above all they are unable to quantify losses clearly and precisely.

The problem is that until crimes become demonstrably major or visible, or even critical, management will not treat criminal phenomena appropriately. It also happens that businesses focus on crimes-related issues only when they must prevent negative customer reactions and/or image and reputation problems, ensure physical safety, and sometimes also improve staff morale.

However, this emergency-oriented approach is very often due also to an inevitable lack of knowledge (and consequently a lack of awareness) on the part of management; 'while it is quite realistic for business to acknowledge that it cannot avoid suffering some crime, why are its attempts to control or prevent those crimes the exceptions rather than the rule? There are numerous reasons, but I would argue that the main one is that understanding crime is not something about which business people learn. (…) The topic is not generally a major part of their professional education'.[120]

Inevitably, this situation produces no specific programmes or initiatives, given that these are difficult to justify without solid figures on losses. At the same time, the costs and the losses themselves must be externalised while the criminogenic factors remain unaffected.

Businesses do not intentionally underestimate the criminal risks to which they are exposed, or the opportunities that they provide for crimes; rather, owing to their lack of information and to their emergency-oriented approach, they fail to manage security rationally and effectively. As result, they are exposed to occupational crimes and abuses committed by insiders, but also to criminal threats by external subjects, sometimes in collusion with employees.

Therefore, what should be induced within the business sector is necessarily a set of changes involving all company departments and subjects. Specifically, top management performs a crucial role in ensuring that the company in its entirety is involved.

Considering this private sector scenario, early warning signs are a key element of business security. They position themselves at the very beginning of the chain of the emergency-oriented approach, and they are potentially able to break the vicious circle that derives from it. Firstly, they respond to the lack of information which is one of the main obstacles against getting management's to understand that *crime prevention* also means *profit enhancement*. Secondly, the development of specific and efficient preventive and control initiatives depends on the availability of precise data and information.

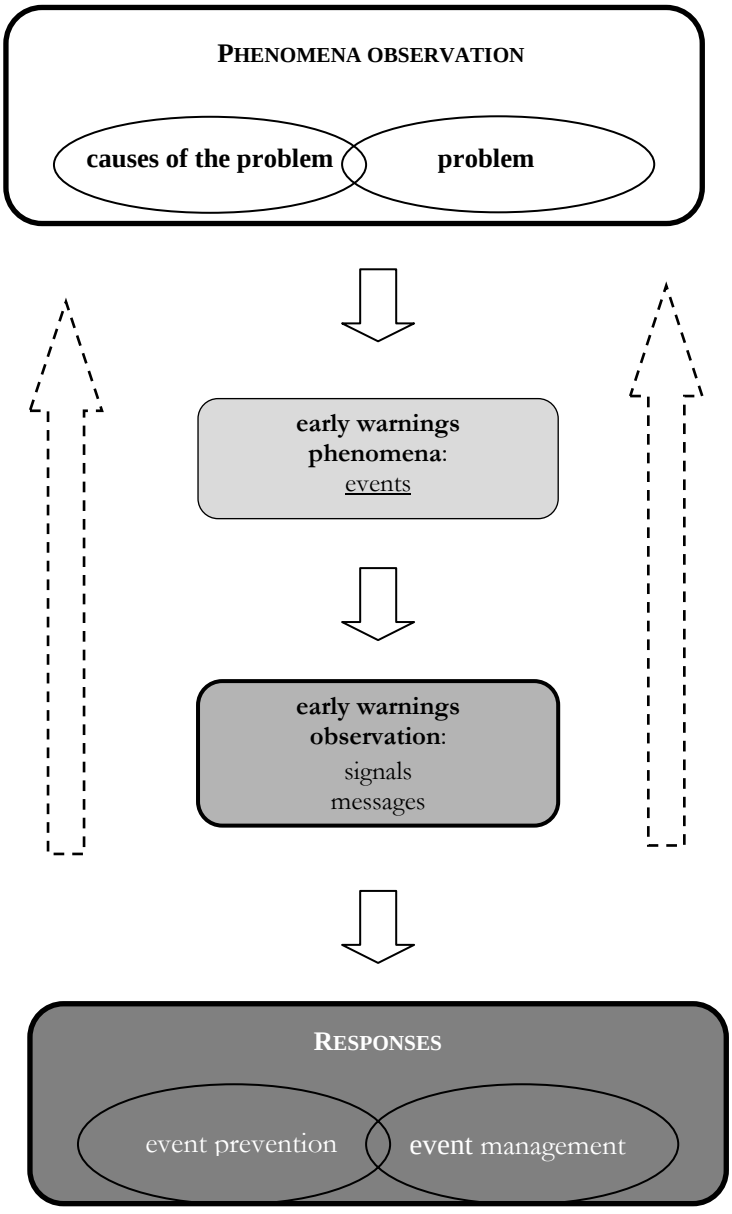
As already repeatedly said in the course of this Report, looking for early warnings means collecting useful information and indirectly increasing a company's attention to what is happening in its departments. The necessary premise is that – as already explained – crimes derive from opportunities and motivations, and these are not controlled by management. Managements also ignore the warning signs of theft and dishonesty; an attitude to be criticized because the list of these signs is literally endless.[121] The problem is that managers often assume that certain incidents or situations in the workplace are the result of carelessness, incompetence or inexperience on the part of employees. On the contrary, they are signs of theft in progress deriving from a precise criminal strategy.

[120] Challinger D., *cit*. 115, p. 36.

[121] Case J., *cit*. 116.

Hence, as Croall points out, 'detecting and preventing fraud is often simply a question of paying attention to detail and questioning deviations and exceptions'.[122]

The following scheme illustrates how the early warnings system works.[123]



[122] Comer M. J., *cit.* 6, p. 45.

[123] An early warnings schema is provided also by Nikander I. O., "Early warnings. A Phenomenon in Project Management", 2002. The text is available at the following URL: http://lib.hut.fi/Diss/2002/isbn9512258889/.

The most important feature to emerge from this schema is that it is possible to act on problems and their causes before the relative negative events and outcomes occur. Thanks to early warnings observation and analysis, in fact, it is possible to plan the management of events once they have occurred, but above all it is possible to prevent them by removing the already-known causes. Therefore, as schematised in the figure, early warnings – if implemented by a receptive and careful management – can play a central role in devising successful and effective preventive strategies while also improving also workplace safety and living conditions. In fact, as already said, early warnings strategies are largely useless if they are not implemented together with rational and respectful human resources management. The workplace climate, as well as the correct behaviour of managers and executives, are extremely important if internal trust relationships are to be developed.

The analysis has thus far focused on internal dishonesty and criminality. This is not to imply, however, that early warnings can be used only to detect and prevent occupational crimes. On the contrary, an early warnings system can be developed for the management of external relationships with, for example, customers, suppliers or partners. As explained, it is a highly versatile methodology which works properly if it is based on a proper information recovery system.

To return to occupational crimes, a concrete example of how early warnings work can be provided by answering the following two questions. What are the 'red flags' of internal fraud? Are there any recurrent signs of deviance which may be indicative of distortion in normal patterns?

Unfortunately, the lack of studies and scientific literature on this issue also hampers the development of a basic – but always updateable – list of signs. Nevertheless there are some *symptoms* which can be identified according to two broad categories: the personal and domestic profiles of the offender. The former also involves possible signs relating to the spending patterns of the offender.

The following are possible items that may be used as terms of reference. They have been collected by wide-ranging research using different sources of information and conducted in different research areas. Given that not all of them are scientific, the list should be considered generic and as merely indicative.

We would stress that they are not all early warning signs in the literal sense; some of them are distinctive details that, together with real alert signs, contribute to proper understanding of an ambiguous or complex individual profile.

Profile of the offender

- makes allusions to unexplained wealth or shortages of money;
- presents unexplained and/or unexpected changes in life-style (e.g. the subject appears to be living beyond his/her means);
- presents unexplained changes in personal behaviour;
- (heavy) use of alcohol and/or drugs;
- has problems of gambling and/or serious speculations;
- is permanently short of money;
- spends excessively on cars, home/clothes;

- makes unexplained absences from work (or is an absentee) or hours of attendance;
- has previous involvement(s) with issues of dishonesty;
- avoids taking vacations or sick leave;
- insists on performing tasks that could be and should be performed by others;
- feels that his/her pay is not commensurate with responsibility;
- is demoted, starts receiving disciplinary actions or believes his/her job is in jeopardy;
- has a wheeler-dealer attitude;
- is dissatisfied at work;
- seeks gratifications and acknowledgements;
- does not answer questions;
- has no respect for superiors and colleagues;
- claims false educational and other qualifications;
- presents different private and business personalities;
- complicates simple things;
- is arrogant and egoistical;
- is envious and resentful of others' successes;
- has interests in other businesses.

domestic profile[124]

- criminal associates and family;
- very successful parents, brothers and sisters;
- high-flying wife or girlfriend;
- flaky husband or boyfriend;
- serious marital, domestic problems;
- divorce or familiar problems.

Some recurrent and reliable red flags which may also alert to the occurrence of internal crimes are the following:

- file removal in the company system;
- documents and inventory counts alteration;
- (small) inventory or cash shortages which cannot be explained;
- alarm systems and physical measures out of order;
- financial business operations with unclear competitive/ income purposes;
- release of information only after insistent requests;
- false statements concerning topics of little relevance;
- unclear relationships between employees and vendors/ customers.

Some of the features listed may seem extravagant or even useless, but they are not. Their relevance is clarified by the most common reasons adduced by employees to justify their illicit behaviour; and sometimes they are so particular that they can be interpreted only if personal motivations are taken into consideration.[125]

[124] The following voices are taken from Comer M. J., *cit.* 6, p. 37.

[125] The following list is provided by Case, *cit.* 116.

- 'I was passed over for a raise or a promotion and the company owed it to me';
- 'the company expects some loss/shrinkages – besides it is insured';
- 'management doesn't care – they never said anything about it';
- 'management steals – why can't we?';
- 'the company cheated me out of some overtime and I got it back';
- 'I am worth a lot more than the company is paying me and I made up the difference';
- the company makes a ton of money and doesn't share the profits with us, so I created my own plan';
- 'things (controls, procedures, rules) were so lax that they made it easy to steal';
- 'the company angered me and this is how I got even'.

Another area of interest for the application of early warnings is IT protection. IT misuses and abuses are among the most thoroughly studied issues in this area, and continuously increasing attention to the phenomenon is generating a huge amount of important data and information.

14. EARLY WARNINGS AND IT MISUSE BY INSIDERS

This Report has repeatedly emphasised that IT security is becoming ever more crucial; at the same time, it has stressed the central role that insiders can play and the high probability that misuses and abuses will occur also within a company. However, despite the well-documented insider threats to information and communication systems,[126] the great majority of efforts and preventive/repressive initiatives are oriented towards outsiders.

The result is a lack of countermeasures against legitimate user misuse, and more opportunities for insiders to commit crimes and/or violate internal policies.

Concern over the increasing number of crimes committed by insiders has multiplied attempts to draw up staff personality profiles. For example, in 1997 the American

[126] Experts question recent findings that seemingly gainsay the conventional wisdom that insiders constitute the primary threat to enterprise security. Authoritative surveys report unexpected drop in insider attacks, in fact. However, there are contradictions between what companies say and what they then report to analysts. In the Department for Trade and Industry's annual Information Security Breaches report, released at Info Sec at London's Olympia, for example, 48% of large companies blamed their worst security incident on employees. By contrast, the 2001 edition of the survey shows that 75% of those questioned cited external attacks by hackers and criminals as the biggest threat to security. See Ward M., "Employees seen as computer saboteurs", 29 April 2002, available at the following URL: http://www.news.bbc.uk/english/sci(tech/newsid_1946000/1946368.stm.

A possible explanation is that, experts point out, insider threats to security may be harder to detect. As Robert Wright, a computer security expert at FBI's National Infrastructure Protection Centre writes, "*insiders are not just employees anymore. New technologies make insiders more dangerous than ever. The most effective insiders are often "keyholders", those who have access to internal system based on contract or partnership arrangements with an organization*". See Verton D., "Insider threat to security may be harder to detect, experts say", 12 April 2002, available at the following URL: http://www.computerworld.com/storyba/0,4125,NAV65-663_STO70112,00.html.

Department of Defence decided to sponsor a project by Eric D. Shaw, Jerrold M. Post and Keven G. Ruby[127] to construct psychological profiles of insider computer-crime perpetrators: that is to say, all those persons (e.g. employees, contractors, consultants, etc) with trusted access to a corporate computer system. From a wider perspective, it is of interest to determine the reasons that induce insiders to commit crimes and infringements, also in order to prepare adequate countermeasures.

Shaw at al. have found that one recurrent trait displayed by ICT employees is introversion. Six personal characteristics with direct implications for risks were identified. They are presented below:

- *frustration*. The case-analysis conducted for the survey showed many of the subjects had significant family and social problems and frustrations. This often resulted in negative attitudes toward authority. Some sub-groups were identified as displaying the so called 'revenge syndrome': their members were angry, alienated from authority, less socially skilled than their peers and isolated from them;
- *computer dependency*. The case-analysis pointed out that on-line activities strongly influenced the lifestyles and habits of perpetrators, interfering with and sometimes replacing social and professional relationships. One potential threat to business security may be the vulnerability of these individuals to on-line manipulation by criminals who target disgruntled employees for financial gain or espionage. These observations may also apply to employees in general. Recent studies have shown that computers may have the same kind of impact on the private and public lives of individuals who are not necessarily computer professionals. People who use computers and Internet at work may suffer from 'Internet addiction disorders' taking the form of more or less serious dependence on use of the Net and ranging from gambling to sexual or drug addictions. This is a problem that should not be underestimated, given that Internet is becoming an indispensable office asset, with employees increasingly likely to spend working hours browsing in anonymous chat rooms or other virtual communities. Although they may be in good faith and only want to engage in some recreational surfing, the risk is that they may be 'contacted' by external subjects who seek to 'extort' sensitive proprietary information;
- *ethical flexibility*. The survey stresses that many computer-crime perpetrators did not see their conduct as unethical, illicit or criminal. Some of them even considered their behaviour to be justified under the circumstances. The main finding was a general lack of moral inhibitions: computer professionals consider it acceptable for computer systems to be attacked if they are not made sufficiently secure by the company. In their view, it is the company itself that tolerates hacking and cracking, espionage and/or sabotage, because it does not develop and implement forceful countermeasures;
- *reduced loyalty*. It seems that insiders who commit computer crimes identify more closely with their profession and colleagues than with their employers. They take a personal attitude towards loyalty and respect;
- *entitlement*. This term denotes a sense that one is special and as deserving recognition, privileges or exceptions. This was one of the most common features that the survey identified in ICT offenders, and it was sometimes a

[127] Shaw E. D., Post J. M., Ruby K. G., "Inside the Mind of the Insider". The text is available at the following URL: http://www.securitymanagement.com/library/000762.html.

characteristic valued even by employers themselves. However, changes in the employer's attitude, in addition to the subjective characteristics already mentioned, may make the employee increasingly disgruntled;
- *lack of empathy*. The offender is indifferent to the possible impact and consequences of his/her conduct on the company, on the employers, or on other people.

The second part of the study by Shaw et al. describes the main motivational categories into which different forms of illicit conduct can be distributed:

- *explorers*. These tend to be driven by curiosity as they wander into poorly designated or relatively unprotected company areas. Generally, they do not deliberately cause damage and are therefore only rarely punished. Insofar as the computer system is attacked by explorers, this serves to evidence a lack of adequate defences and/or company policies;
- *good Samaritans*. These strongly believe that their crimes result from concrete efforts to perform legitimate duties more effectively and efficiently. In most cases they are unaware of the illicit nature of their behaviour;
- *hackers*. This is a term widely used, but also widely confused because of its multiple meanings. In the traditional sense of the term, a hacker is someone who sees breaking into a computer system as essentially a personal challenge: he/she wants to bolster his/her self-esteem. Hackers challenge authorities as well as their peers, and they do not regard themselves as criminals because they mean no harm. They do not cause damage and mostly perform an important service by making companies, public agencies and institutions aware of the fact that their computer networks are not secure;
- *Machiavellians*. The study identifies Machiavellians with insiders who unscrupulously use corporate systems to achieve their personal and career goals. They are usually also disgruntled employees, but there are exceptions. The general rule is that their attacks are well organised and the damages/effects are well calculated. Their actions are entirely self-serving, but there are also cases in which they have accomplices. The fact they are usually leaders who can easily convince and motivate others makes them dangerous because of their ability to involve other possible disgruntled employees;
- *exceptions*. These regard themselves as having completely different status with nothing in common with other employees. For this reason they are allowed to do what is denied to others, and they always perceive their conduct as legitimate;
- *avengers*. They attack or cause damage in reaction to specific setbacks, disappointments and/or frustrations, not because of general disgruntlement. The most recurrent causes are, for example, termination, transfer, demotion or failure to receive an expected reward. These people perceive this situation as mistreatment, and this makes them particularly dangerous. As far as computer crimes are concerned, the most frequent attacks take the form of sabotage, espionage, theft, fraud and extortion;
- *career thieves*. These 'thieves' enter a company with a predetermined plan: they exploit their presence within the company to commit a moneymaking crime (e.g. embezzlement, fraud, theft). Computers are only tools with which to acquire funds. They organize well calculated criminal schemes and are not in any way motivated by internal mistreatment;
- *moles*. These also enter a company with criminal intent, but they have a more specific mission to fulfil: joining the company in order to spy for a competitor, or even a public agency. By contrast, career thieves work purely for themselves.

It is thus intuitive that early warning signs are extremely important, especially when associated with preliminary methods for predicting misconduct. At the moment, however, efforts to develop knowledge and the implementation of effective programmes and initiatives are still conducted mainly at academic and/or research level.

However, an example of the early warnings approach/philosophy against internal cyber-attacks is the Insider Threat Prediction Tool (ITPT) developed by G. B. Magklaras and S. M. Furnell.[128] This is based on the detecting of signs indicative of a particular misuse. It is thus primarily a threat *predicting* tool, rather than a merely threat *detecting* one.

The assumption behind this experiment can be summed up with the following statement of the authors: 'every form of insider IT abuse (or attempt to abuse) leaves certain traces in basic components of the IT infrastructures'.[129] From the preventive perspective, these traces are early warning signs which, if correctly handled, can be of valuable help in the avoidance and deterrence of crimes, abuses and misuses.

Without going into technological details, it seems at least helpful to depict how this tool works, as in the following figure:

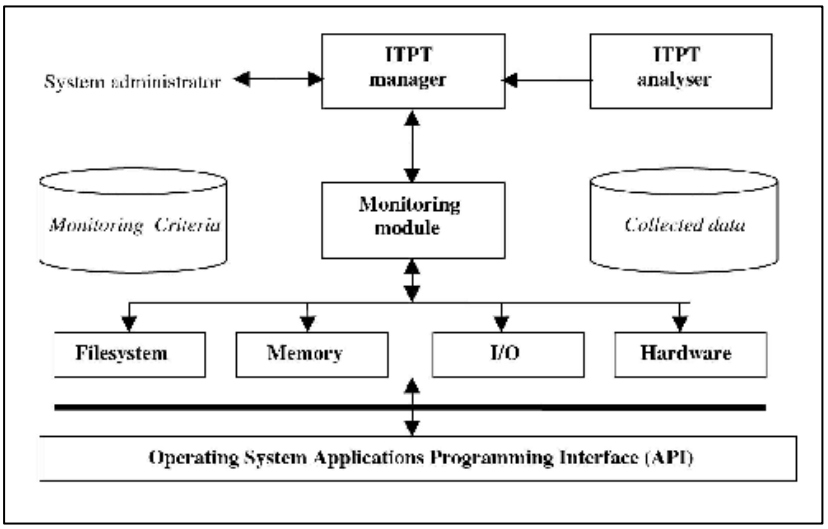


Figure 5: High-level architecture of the ITPT system[130]

By contrast, the output from this system should be clarified in detail. It consists in the possibility to classify conducts according to threat profiles on the basis of four main categories:

[128] Magklaras G. B., Furnell S. M., "Insider Threat Prediction Tool: Evaluating the probability of IT misuse", in *Computers & Security*, vol. 21, No. 1, pp. 62 – 73, 2002.

[129] Magklaras G. B., Furnell S. M., *cit* 128, p. 66.

[130] Magklaras G. B., Furnell S. M., *cit*. 128, p. 68.

1. *possible intentional threat*: the system can find evidence that it is very likely that a particular user will initiate a specific misuse action;

2. *potential accident threat*: the system can detect evidence that a user is about to perform a particular type of misuse, by accident;

3. *suspicious*: the system can also detect a set of ambiguous/suspicious user activities that indicate potential misuses and/or abuses;

4. *harmless*: the system collects no evidence at all of undesirable actions by users.

On the basis of the information collected, the system administrator or the designated person will be able to evaluate each individual profile, understand how misuses are committed, and be informed and updated about possible incidents/violations. In turn, this means being able to *prevent* them.

It is important to stress that this tool is built upon a taxonomy which is *human centric* in that it is people who use and abuse technologies. This classification takes three main elements into consideration:

- system role: the actual role of each individual according to his/her use of the given computer system (workstation, server, telecommunication system). The role is determined on the basis of the type and level of system knowledge that the person has. As regards insiders there are three main categories: system masters (e.g. system heads and network administrators), advanced users (who possess a substantial knowledge of the system internals) and application users (all the other legitimate users who utilize only given applications);
- reason(s) for misuse: there are two large groups of reasons: intentional and accidental. They are considered equally important because they both can cause serious damage;
- the way a misuse act is manifested at a system level.

The last element is particularly important because it is closely related to how early warnings signs must be evaluated once they have been collected. Although insider threats can be assessed in many different ways, it makes sense to organise them so that they can be easily detected, in this case by the software.

RESEARCH IMPLICATIONS

This final part of the Report consists of concluding discussion on the research findings, the aim being to propose a new approach to business security at both the theoretical and practical levels.

In specific, a new classification model has been developed in order to create a *business crime incident scheme*. This singles out the features most recurrent in cases of crime/abuse against the private sector and also outlines how they interact.

15. A NEW THEORETICAL APPROACH: INTRODUCTION TO THE *BUSINESS SECURITY INCIDENT* (BSI) MODEL

The research conducted to compile the FALCONE 2001 – BUSINESS SECURITY Study has led to the conclusion that a critical shortcoming is the lack of common definitions and scientific studies in the field of business security; on the contrary, however, there are numerous research studies that focus on Info Security related issues. Attempts have been made in the literature to draw up a complete taxonomy of computer and network attacks or incidents. After establishing principles of classification, the authors concerned have tried to create a common language enabling the gathering, exchange and comparison of information. This so-called 'approximation of reality'[131] is necessary in any field of study because it is essential for closer understanding. Like every approximation, however, it may be unsatisfactory, especially when data are imprecise, uncertain or still confused because they relate to recent phenomena. This is the case, for example, of business crimes and ICT related issues in general. Nevertheless, categorizations are necessary and they are indispensable for systematic study of a particular occurrence.

Starting from this consideration and from the premise that business security knowledge urgently needs improvement, it seemed important to develop a model which could schematise the main components of criminal threats to the private sector. The result has been a general and flexible model which can be called the *Business Security Incident* (BSI).

The model has been constructed laying no claim that it is a definitive, exhaustive and ultimate scheme; on the contrary, its value consists in the fact that it can be continually updated as and when information and data become available.

This is possible because the BSI Model has been conceived and designed as a *taxonomy*: that is, a classification scheme that partitions a body of knowledge and defines the relationships among the items. *Classification* is the process of using a taxonomy for separating and ordering.

---

[131] Howard J. D., *An Analysis Of Security Incidents On The Internet. 1989 – 1995*, 7 April 1997. Chapter 6, p. 1. The text is available at the following URL: http://www.cert.org/research/JHThesis/Start.html.

Before entering into details about the BSI methodology and contents, however, we must define some basic concepts and how they interact with each other.

16. WORKING DEFINITIONS: BUSINESS SECURITY, INFO SECURITY AND CPTED

As already explained during this Report, the aim of *business security* is to protect the people, assets, intellectual property and information technology within a company. Therefore, apart from the play on words, business security is that specific business function which guarantees security in general.

From a practical perspective, however, its functions can be classified into two specific sub-categories:

Info Security: the branch of security which deals with ICT vulnerabilities; put otherwise, within a company business security department, Info Security examines theories and seeks out instruments with which to protect intangible/immaterial assets against all the possible kinds of criminal threat and misuse/abuse;

Physical Security: the branch of security which deals with workplace security, protecting all other company assets; specifically, physical security measures are (or should be) based on strategies and measures which form the *Crime Prevention through Environmental Design (CPTED)*.

CPTED is a particular theoretical approach to crime prevention based on the construction of a safe workplace and business environment by reducing the opportunities for crimes to occur. It is mainly oriented towards tangible and physical assets protection.[132]

It should be emphasised that the *summa divisio* between Info Security and CPTED is not rigid. In some cases, it is necessary to go beyond this classification and accept that there are *grey zones*; for example, a laptop is a tangible asset (e.g. its hardware components) in which a huge amount of intangible assets (e.g. software, information and data) are stored. Hence its protection requires both Info Security measures and CPTED programmes.

Because of its flexibility, the BSI scheme encompasses these kinds of hybrid case as well.

[132] The distinction between immaterial and material assets mainly depends on their form: the former are intangible and expressed in a bit format, while the latter are tangible and, at any given time, occupy a specific portion of space which can not be occupied by other object.

17. THE BUSINESS SECURITY INCIDENT MODEL (BSI)

The BSI Model is largely based and partly reproduces the Computer Security Incident (CSI) scheme elaborated in the Sandia Report, 'A Common Language for Computer Security Incidents', written by John D. Howard and Thomas A. Longstaff, for Sandia National Laboratories.[133]

All the technical definitions used in the following sections are those drawn up by the Institute of Electrical and Electronics Engineers. [134]

As explained by Howard and Longstaff, their research does not seek to provide a comprehensive dictionary of terms used in the field of computer security; instead, it aims at 'developing a minimum set of high-level terms, along with a structure indicating their relationship (a taxonomy), which can be used to classify and understand computer security incident information'.[135]

Completely sharing this methodological approach, the BSI Model extends this computer incidents related scheme to the more general field of business security, including both Info Security and CPTED related issues.

Before entering into detail, we would repeat that, as already explained at the beginning of this Report, the term 'crime' is not considered from a legal perspective here, and hence refers to all crimes and offences committed against businesses.

Moreover, as said, the BSI Model is the result of the research conducted for the FALCONE 2001 - BUSINESS SECURITY Study and is specifically based on the findings of the case-study analysis. It has therefore been designed around the five categories listed in the questionnaire of infringements and crime against:

- production line and products;
- human resources;
- ICT;
- know-how; and
- capital.

---

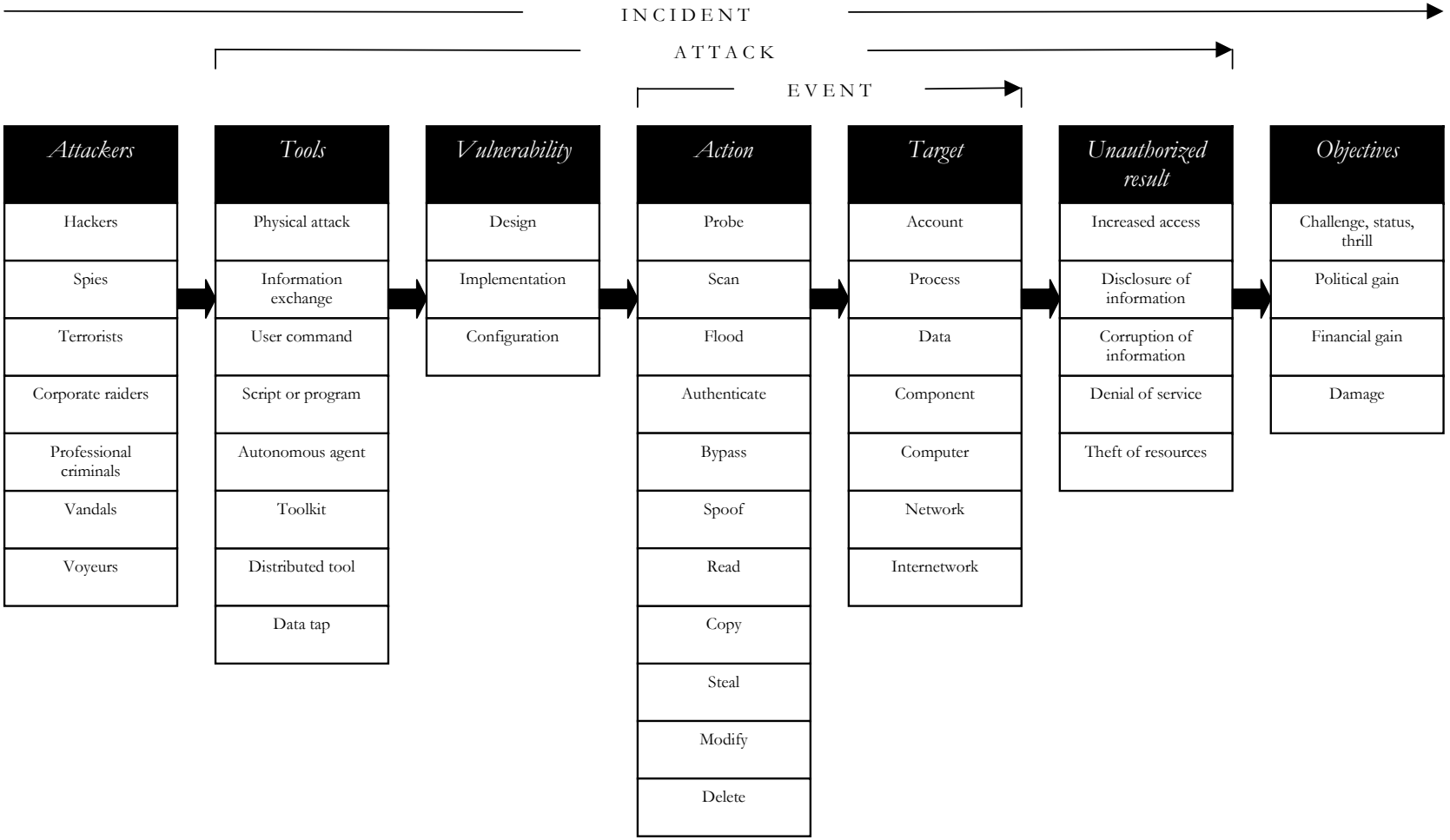
[133] Howard J. D., Longstaff T. A., "A Common Language for Computer Security Incidents", Sandia National Laboratories, October 1998. The text is available at the following URL: http://www.cert.org/research/taxonomy_988667.pdf.

[134] Institute of Electrical and Electronics Engineers, Inc., New York. See IEEE, *The IEEE Standard Dictionary of Electrical and Electronics Terms*, 6th ed., John Radatz Editor, 1996.

[135] Howard J. D., Longstaff T. A., *cit.* 133, p. iii.

From the case analysis perspective, therefore, the BSI Model lays absolutely no claim to exhausting the range of infringements/crimes considered. However as already pointed out, it is constructed in such a way that it can be easily integrated with other crimes and abuses not considered in this Study.

The methodology used, together with similarities and differences with respect to the Sandia scheme, will be explained step by step, as clearly as possible. In this way, also explained will be how the CSI is used by the BSI Model to involve both Info Security and CPTED. The Sandia Computer Security Incident Model is as follows.



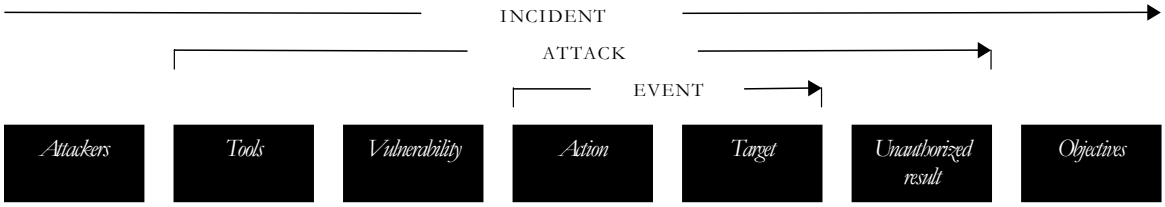
Computer Security Incident Scheme

On the basis of this scheme, the analysis of the CSI, and consequently of the BSI, will be developed by starting from the basic components and then explaining the representation as a whole. The main steps will be the following:

- *event*, which consists of *action* and *target;*

- *attack*, which consists of *event* but also *tools*, *vulnerability* and *unauthorised result*;

- *incident* which consists of *event* and *attack*, but also *attackers* and *objectives*.



As schematised in the figures, the CSI is based on the relationship between three main concepts: *event*, *action* and *target*:

- *event* is defined as an *action* directed at a *target* which is intended to result in a change of state (status) of the target [IEEE, 1996].
  Accordingly, the event creates a link between an action and a specific target;

- *action* is a step taken by a user or process in order to achieve a result [IEEE, 1996]. According to the Sandia CSI, it corresponds to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify or delete:[136]
  probe: access a target in order to determine its characteristics;
  scan: access a set of targets sequentially in order to identify which targets have a specific characteristic;
  flood: access a target repeatedly in order to overload the target's capacity;
  authenticate: present an identity of someone to a process and, if required, verify that identity in order to access a target;
  spoof: masquerade by assuming the appearance of a different entity in network communications;
  read: obtain the content of data in a storage device, or other data medium;
  copy: reproduce a target leaving the original target unchanged;
  steal: take possession of a target without leaving a copy in the original location;
  modify: change the content or characteristics of a target;
  delete: remove a target, or render it irretrievable.
- *target* is defined as a computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).

These definitions have evidently been formulated in response to specific Info Security needs. Therefore, while some of them are quite general, the majority specifically concern the protection of computer systems and networks. From the business security viewpoint, however, some of them must be redefined if they are also to be applied to 'physical' behaviours and CPTED.

Of the basic concepts of event, action and target, only the definition of *event* can be used directly, with no modifications.

As regards *action*, however, it is necessary to both re-define some concepts and supplement the list of the behaviours identified, adding further steps which represent business security issues more completely.

To re-define certain steps, from the business security perspective, *stealing* can for example be considered as directed against both intangible and tangible assets. It can consequently be used to denote all behaviours falling under the general heading of 'theft'. It is thus possible to use this category to comprise not only 'taking possession of a target without leaving a copy in the original location' but also the theft of tangible assets (e.g. theft of company goods during the manufacturing process, from warehouses or in transit) as well as specific illicit behaviour like embezzlement, that is, the misappropriation of cash/funds by employees.

The same 'generalization process' can be applied to other terms as well, such as *modify* and *delete*. Although these terms can be referred to the computer security area, they can also be used to indicate behaviour which involves 'physical' action. For example, *modify*, defined as changing the content or characteristics of a target, can be easily extended to cover physical behaviour as well, for instance when a

[136] The following definitions are taken from the Howard J. D., Longstaff T. A., *cit*. 133, p. 10.

company's accounts are altered in order to commit an administrative or financial fraud.

The steps that should be added to the CSI list include, for example, *counterfeit* and *falsify*, together with *modify*, in fact, these are both more pertinent to behaviour which targets mostly physical assets. Moreover, *destroy* must be included to complete the use of *delete* by encompassing behaviour which affects physical assets more directly.

As regards the BSI, the list of behaviours which fall under the heading of *action* must be completed with another general category: *physical action*. This encompasses a series of different forms of behaviour which cannot be related to the others. The physical action of setting fire to a company asset in a case of arson, or the breaking of a window in order to enter a company warehouse and steal the goods stored therein, are examples. Also kidnapping – which is extremely common in the private sector, especially in South America – can be labelled as physical action.

The second, fundamental component of the CSI scheme, and specifically of the *event* category, is the *target*. The CSI conceptualises *actions* as referring to seven categories of *targets*: *account, process* and *data* – which are defined as *computer or network logical entities* – *component, computer, network* and *internetwork* – which are defined as *physical entities*.

- account: a domain of user access on a computer or network which is controlled according to a record of information which contains the user's account name, password and use restriction;
- process: a program in execution, consisting of the executable program, the program's data and stack, its program counter, stack pointer and other registers and all other information needed to execute the program;
- data: representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. Data can be in the form of files in a computer's volatile or non-volatile memory, or in a data storage device, or in the form of data in transit across a transmission medium;
- computer: a device that consists of one or more associated components, including processing units and peripheral units, that is controlled by internally stored programs, and that can perform substantial computations, including numerous arithmetic operations, or logic operations, without human intervention during execution;
- component: one of the parts that make up a computer network;
- network: an interconnected or interrelated group of host computers, switching elements and interconnecting branches;
- internetwork: a network of networks.

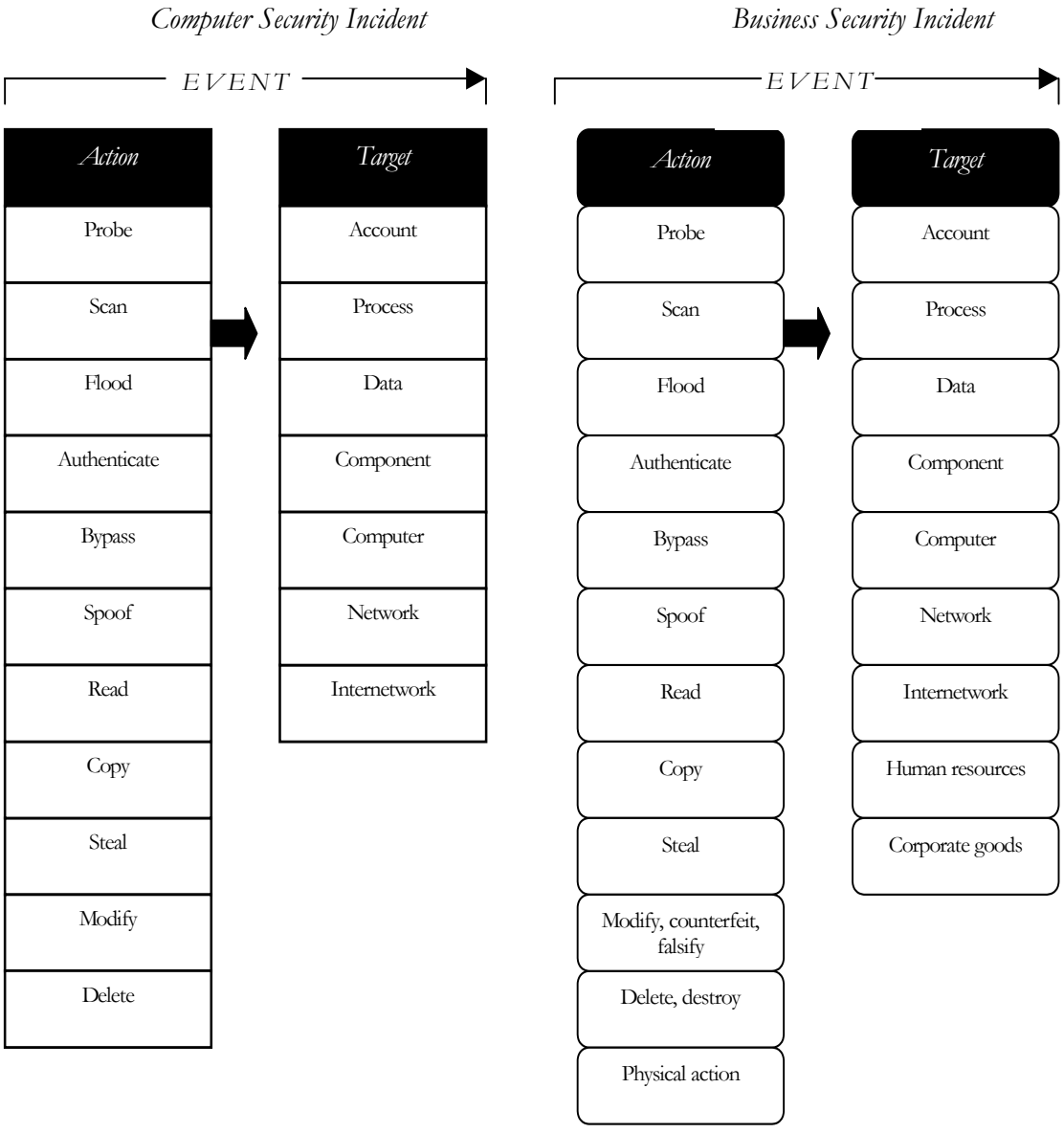
In this case, too, some definitions must be adapted before they are also applicable to the more general area of business security. For example, the notion of *data* must be extended to comprise the representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means, *the way in which they are expressed notwithstanding*.

Moreover, the list of possible targets must be supplemented with the further general categories of *human resources* and *company goods*.

Human resources is a broad label which denotes the company's entire workforce, at all levels. It includes external subjects who may have different kinds of relationship with the company itself, such as suppliers, customers, agents.

Company goods are all corporate assets, both physical and immaterial. Material goods include not only the company's products but also all its belongings: from machinery and equipment to stationery; in the same way, intangible assets consist of all company-related information: from suppliers' addresses to proprietary/confidential information such as, for example, know-how or trade secrets.

Now that the concepts of action and target have been defined, the two schemes, the CSI and the BSI, can be compared to bring out the similarities and differences between the two incident models.



The second level of analysis is the passage from *event* to *attack*.

The CSI Model defines attack as *a series of steps taken by an attacker to achieve an unauthorised result*. Attacks comprises five parts representing the logical steps that an attacker must follow. In practice, an attacker uses a *tool* to exploit a *vulnerability* to perform an *action* on a *target* in order to achieve an *unauthorised result*. To be successful, the combination of all these elements must be simultaneous or repeated.[137]

As for the event, this category too is divided into subcategories, which are now briefly analysed to show how they can be used in the BSI Model.[138]

The first element to be defined is *tool*: a means of exploiting a computer or network vulnerability. This encompasses the following sub-categories:

physical attack – a means of physically stealing or damaging a computer, network, its components, or its supporting systems (such as air conditioning, electric power, etc.);

information exchange – a means of obtaining information either from other attackers (such as through an electronic bulletin board), or from the people being attacked (commonly called social engineering);

user command – a means of exploiting a vulnerability by entering commands to a process through direct user input at the process interface. An example is entering Unix commands through a telnet connection, or commands at an SMTP port;

script or program – a means of exploiting a vulnerability by entering commands to a process through the execution of a file of commands (script) or a program at the process interface. Examples are a shell script to exploit a software bug, a Trojan horse login program, or a password cracking program.

autonomous agent – a means of exploiting a vulnerability by using a program, or program fragment, which operates independently from the user. Examples are computer viruses or worms;

toolkit – a software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities.

distributed tool – a tool that can be distributed to multiple hosts, which can then be coordinated to anonymously perform an attack on the target host simultaneously after some time delay.

data tap – a means of monitoring the electromagnetic radiation emanating from a computer or network using an external device.

Obviously, from the business security incident perspective, all these subcategories concern only the Info Security sector. Considering that, as explained, the BSI also includes the CPTED, a further subcategory must be added: *physical tools*. This encompasses all the material objects which may be used to commit a crime/abuse:

---

[137] Howard J. D., Longstaff T. A., *cit*. 133, p. 12.

[138] All the following information and definitions are taken by Howard J. D., Longstaff T. A., *cit*. 133, p. 12-15.

for example, a photocopying machine and/or a camera to copy documents, explosive material or a simple hammer. Given the wide variety of possible behaviours using material tools, it is well-nigh impossible to list all of them; therefore, this sub-category is a catch-all category.

As explained, in the CSI scheme, a tool is used to exploit a computer or network *vulnerability*, which is scientifically defined as a weakness in a system allowing unauthorised action.[139]

As regards Info Security, vulnerabilities are divided into three sub-categories:

design vulnerability – a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability.

implementation vulnerability – a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.

configuration vulnerability – a vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having 'world write' permission for new files, or having vulnerable services enabled.

From the BSI perspective, these definitions may be adapted to physical vulnerabilities as well. For example, an alarm system may suffer from the same vulnerabilities as a computer system: a design vulnerability may consist in the wrong positioning of the sensors, while an implementation vulnerability may be an alarm warning siren which does not function when the alarm system is set off. Configuration vulnerability may be due to a lack of *tolerance* in the system organization, so that the alarm is triggered even when it is not necessary.

The *event* category has already been analysed. The last logical step to be analysed is therefore *unauthorised result*. The CSI defined this as an authorised consequence of an event. If successful, an attack will result in one of the following:

increased access – an unauthorized increase in the domain of access on a computer or network.

disclosure of information – dissemination of information to anyone who is not authorized to access that information.

corruption of information – unauthorized alteration of data on a computer or network.

denial of service – intentional degradation or blocking of computer or network resources.

theft of resources – unauthorized use of computer or network resources.

Also this category has been modified on the basis of the BSI scheme's requirements; first, it was renamed *illicit result*, in order to encompass not only the unauthorised results but also all the criminal/illicit acts considered by this Project and, in particular, by the questionnaire. Moreover, the sub-category 'theft of

[139] *Ibid*.

resources' was considered to contain not only high-tech resources but also other valuable company resources like so-called *company time* and financial resources. For instance, Internet abuse in the workplace (e.g. *recreational* surfing) not only affects the computer and/or network system but also causes economic losses due to the employee's productivity shrinkage. Another example of theft of resources is the purchase of goods/services by employees for their personal use.

Therefore, in the BSI scheme, the *illicit result* category encompasses:

Theft of corporate goods – this affects the sub-category *corporate goods* subsumed by the category *target*;

Unfair competition;

Extortion;

Administrative and financial fraud;

Corruption;

Sabotage;

Vandalism;

Counterfeiting;

Industrial property infringements;

Industrial espionage;

Insider trading;

False bankruptcy;

Falsification of financial statement;

Money laundering;

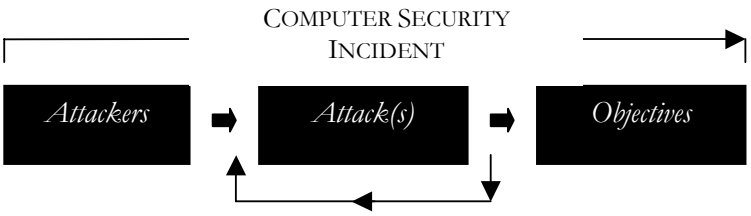
Transactions involving conflict of interest;

Business relations with criminal companies.

Once again, we would stress that the list of sub-categories identified is not to be considered exhaustive; on the contrary, it is merely a provisional list open to further analysis and integration. In reality, what really matters is the position of this category in the BSI sequence and how it interacts with the others.

This interaction will become clear after analysis of the last category: *incident*.

In the CSI scheme, *incident* is defined as a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing. It divides into three main parts:



Accordingly, an incident may consists of one single attack or it may be made up of multiple attacks, as shown by the return loop in the figure.

As with the previous sections of the CSI, these three categories break down into sub-categories. Starting from *attacker* (an individual who attempts one or more attacks in order to achieve an objective), it comprises six main profiles according to the *objectives* (the purpose or end goal of an incident):

hackers – attackers who attack computers for a challenge, to gain status or for the thrill of obtaining access;

spies – attackers who attack computers for information to be used for political gain;

terrorists – attackers who attack computers to cause fear for political gain;

corporate raiders –employees (attackers) who attack competitors' computers for financial gain;

professional criminals – attackers who attack computers for personal financial gain;

vandals – attackers who attack computers to cause damage;

voyeur – attackers who attack computers for the thrill of obtaining sensitive information.

From the BSI perspective, it should be specified that these categories of attackers represent several subjective profiles of perpetrators; in fact, spies, terrorists, professional criminals and vandals, especially, may target not only computer systems and networks but also material goods and/or intangible assets. For example, a terrorist may deface a web site or hamper its functioning, but he may also attack the company headquarters using explosives. In the same way, a vandal may be an outright *cracker* who definitively compromises a company website or the computer network's performance, but he may also be someone who simply draws graffiti on external company boundaries.

Therefore the sub-category of vandals, for instance, can be subdivided into two further groups: *virtual vandals* and *physical vandals*.

Again from the BSI perspective, other sub-categories must be added to the above list:

thief – in general, the person who steal proprietary goods/assets;

kidnapper – the person who unlawfully takes and carries away a human being by force and against his will;

criminal – a general category which encompasses all profiles not included in the previous sub-categories.

Finally, as regards *objectives*, the CSI singles out four main sub-categories, all of them very general:

challenge, status, thrill – these labels denote the various personal and psychological motivations that induce an offender/attacker to target a company;

political gain – this includes all possible political reasons;

financial gain – this includes all economic and financial aims, from pure and simple personal profit to particular reasons for committing a crime such as gambling debts or drug/alcohol addictions;

damage – this includes all cases in which the principal objective is to damage the company.

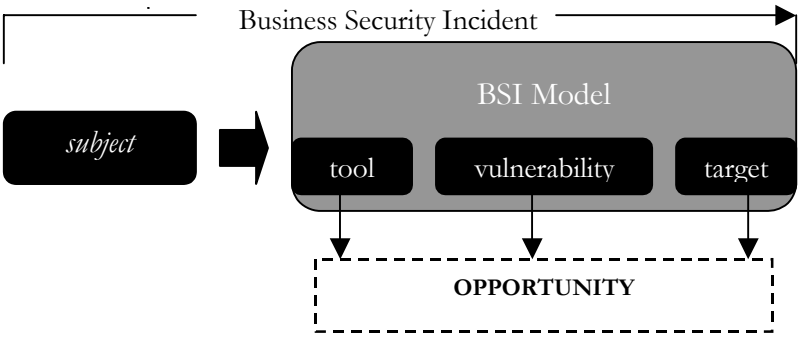
As said, all the categories analysed so far are those used in the CSI, and they have been interpreted so that they can be adapted to the BSI scheme. However, a Business Security Incident differs from a Computer Security Incident by virtue of an additional category specifically regarding the status of the subjects who commit an incident. Specifically, the BSI displays another category, called *subject*, which is divided into two further categories:

insiders – offenders who have contractual relationships with the company:

outsiders – offenders who have no relationships with the company.

This distinction is extremely important, especially from the crime prevention and opportunities reduction point of view; in fact, the countermeasures (should) differ according to the addressees and their role/position within the company.

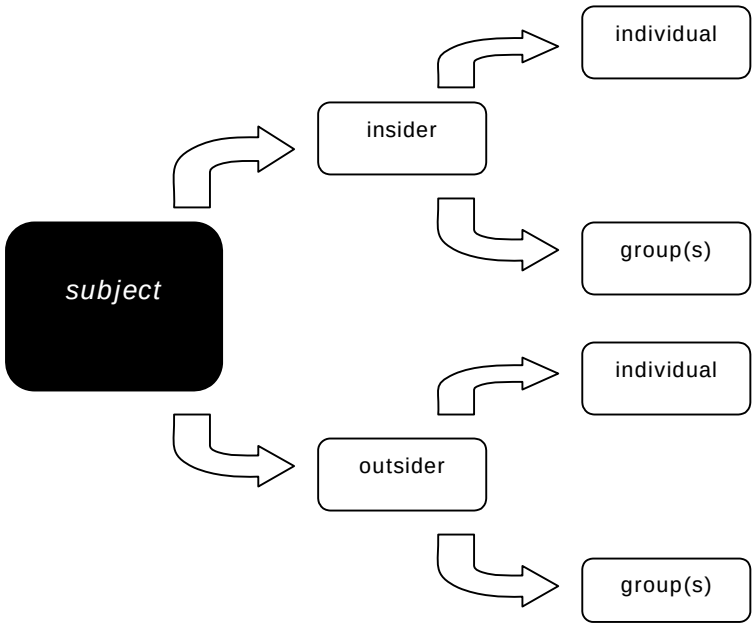
The following figure schematises the BSI philosophy.



Thus stated, it is necessary to define who an attacker is according to the BSI perspective of analysis. In particular, it is necessary to specify the relationship between this category and that of subject.

In the BSI scheme, the perpetrator who commits an incident is not the attacker but the subject: the fact of being an attacker is only a particular feature of the subject while s/he commits the crime/abuse. This explains why the category subject precedes the category attacker in the BSI scheme.

Besides the distinction between insider and outsider, subjects may have a further characteristic: they may be individuals or groups. The latter engage in different types and levels of collusion: they may all be insiders working at the same or different levels, or they may all be outsiders. Collusion may also take place between insiders and outsiders.



Now that each step, category and sub-category has been explained, the BSI can be depicted as follows.

Some examples of how the scheme works follow. They are taken from the five categories of infringement/crime specified, as said, for the FALCONE 2001 – BUSINESS SECURITY questionnaire.

Example 1 – *infringement/crime against product and production line*. The case is arson. An insider (step 1), who can be defined a vandal (step 2), performs the physical action of arson (step 3) to profit from a vulnerability in the alarm system (step 4) and destroys (step 5) a company asset/good (step 6) in order to sabotage the company (step 7)and thereby achieve a political objective (step 8).

Example 2 – *infringement/crime against human resources*. The case is extortion. An insider (step 1), who can be defined a kidnapper (step 2), performs the physical action of kidnapping (step 3) to profit from a vulnerability in the protection

programme (e.g. the lack of bodyguards) (step 4) by kidnapping (step 5) a manager (step 6) in order to extort (step 7) money (step 8).

Example 3 – *infringement/crime against ICT*. The case is unauthorised disclosure of information. An outsider (step 1), acting as a hacker (step 2), uses a script (step 3)to profit from a vulnerability in the internal company computer system and network (step 4) by reading (step 5) secret proprietary information (step 6) and gains unauthorised access to the computer system (step 7) merely as a personal challenge (step 8).

Example 4 – *infringement/crime against know-how*. The case is unfair competition. An outsider (step 1), acting as a spy (step 2), uses data interception (step 3) to profit from a incorrect computer system configuration (step 4) and steals/copies (step 5) secret information (step 6) in order to sell it to a competitor (step 7) for personal profit (step 8).

Example 5 – *infringement/crime against capital*. The case is administrative fraud. An insider (step 1), acting as a professional criminal (step 2), performs a physical action (step 3)to profit from a vulnerability in the auditing system (step 4) by modifying (step 5) company financial statements (step 6) in order to defraud the company (step 7) and gain personal profit (step 8).

BIBLIOGRAPHICAL REFERENCES

ACFE, *1996 Report to the Nation on Occupational Fraud and Abuse*, 1996. The executive summary is available at the following URL: http://www.acfe.org.

ACFE, *2002 Report to the Nation on Occupational Fraud and Abuse*, 2002. The text is available at the following URL: http://www.acfe.org.

ACFE, *Small Business Fraud*, April 2002.

Adamoli S., Di Nicola A., Savona E. U., Zoffi P., *Organised Crime around the World*, report prepared by Transcrime – University of Trento for HEUNI – United Nations, HEUNI Publication Series n. 31, Helsinki, 1998.

Ampleford S., 'Methodology Review', prepared for the International Development Research Centre, July 2000, p. 4. The text is available at the following URL: http://www.reliefweb.int/library/documents/studmeth.pdf.

Baron A., *Violence in the Workplace*, 1993.

Broder J F., *Risk Analysis and the Security Survey*, 2nd ed., Butterworth Heinemann, Boston, 2000.

Budd T., *Violence at Work: Findings from the British Crime Survey*, Home Office, October 1999.

Carment D., 'Assessing Country Risk: Creating an Index of Severity', May 2001. The text is available at the following URL: http://www.carleton.ca/cifp/risk.htm.

Case J., 'Over Employee Theft. The Profit Killer', 1999. The text is available at the following URL: http://www.employeetheft.com/casemain.htm.

Center for Invasive Plant Management, *Center for Invasive Plant Management Annual Report 2001*, 2001. The text is available at the following URL http://www.weedcenter.org/about/2001annualreport2.pdf.

CERT, *Trends in Denial of Service Attack Technology*, October 2001.

Challinger D., 'Will Crime prevention ever be a Business Priority?', in Felson M. and Clarke R. V. (edited by), *Business and Crime Prevention*, Criminal Justice Press, New York, 1997.

CIFP, *Risk Assessment Template*, August 2001.

Comer M. J., *Corporate Fraud*, Gower, Network Security Management LTD, 3rd ed., 1998.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions 'Network and Information Security: Proposal for a European Policy Approach' of 6 June 2001. COM (2001) 298 final.

Croall H., *White Collar Crime*, Open University Press, 1992.

CSI/FBI, *2002 CSI/FBI Computer Crime and Security Survey*, 2002.

Department of Health and Human Services, *Understanding and Responding to Violence in the Workplace – Guidelines*, March 1997.

Devost M. G., Pollard N. A., 'Taking Cyberterrorism Seriously – Failing to Adapt to Emerging Threats Could Have Dire Consequences', 27 June 2002. The text is available at the following URL: http://www.terrorism.com.

Dilworth G., 'The Economic Espionage Act of 1996: an Overview', 2001. The text is available at the following URL: http://www.cybercrime.gov/usamay2001_6.htm.

EEA, *Environmental Signals 2002. Benchmarking the Millennium – Environmental Assessment Report No. 9*. The text is available at the following URL: http://reports.eea.eu.int/environmental_assessment_report_2002_9/en/signals2002-intro.pdf.

EEA, *Late Lessons from Early Warnings: The Precautionary Principle 1896-2000 – Environmental Issue Report No. 22*. The text is available at the following URL: http://reports.eea.eu.int/environmental_issue_report_2001_22/en.

European Commission, 'Proposal for a Council Framework Decision on Attacks against Information Systems', Brussels, 19 April 2002, COM(2002) 173 final, 2002/0086 (CNS).

European Commission, Directorate General 'Justice and Home Affairs', 'Discussion paper on the role of the private sector in the prevention of crime – a European perspective', First meeting of the *EU Forum on the prevention of organised crime*, 17-18 May 2001.

European Council, 'Prevention and Control of Organised Crime: a Strategy of the European Union for the Next Millennium', 27 March 2000.

Europol, *EU Organised Crime Situation Report*, The Hague, February 2000.

Farrington D. P. (edited by), *Psychological Explanation of Crime*, Dartmouth, Adelshort, 1994.

Felson M., Clarke R. V., 'Opportunity makes the Thief. Practical Theory for Crime Prevention', *Police Research Series*, Paper 98, Home Office.

Ferreira B. R., 'Situational Crime Prevention and Displacement: The Implications for Business, Industrial and Private Security Management', *Security Journal,* 6 (1995).

Geis G., Meier R. F. (edited by), *White-collar crime*, Free Press, New York, 1977.

Gill M. (edited by), *Crime at work*. *Increasing the risk for offenders*, vol. II, Perpetuity Press, 1998.

Gill M., Hearnshaw S., Turbin V., 'Violence in Schools. Quantifying and Responding to the Problem', *Educational Management Administration*, vol. 26, No. 4, October 1998.

Gomm R., Hammersley M., Foster P. (edited by), *Case Study Method*, Sage Publications Ltd, 2000.

Grabosky P., Smith R. G., Dempsey G., *Electronic Theft. Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge, 2001.

Gurr T. R., Marshall M., 'Assessing the Risks of Future Ethnic Wars', in Gurr T. R., *People versus States: Minorities at Risk in the New Century*, Washington DC, Institute of Peace Press, 2000.

Hagan F. E., *Research Methods in Criminal Justice and Criminology*, 4th ed., Allyn and Bacon, 1997.

Head G. L., *Essentials of Risk Control*, 3rd ed. (vol. II), Insurance Institute of America, Chapter 11, 1995.

Hollinger R. C., Clark J. P., *Theft by Employees*, Lexington, 1983.

Howard J. D., An Analysis Of Security Incidents On The Internet. 1989 – 1995, 7 April 1997. Chapter 6. The text is available at the following URL: http://www.cert.org/research/JHThesis/Start.html.

Howard J. D., Longstaff T. A., 'A Common Language for Computer Security Incidents', Sandia National Laboratories, October 1998. The text is available at the following URL: http://www.cert.org/research/taxonomy_988667.pdf.

ICAC – Hong Kong, Survey on Business Ethics, March 1994.

Institute for Security Technology Study at Dartmouth College, 'Cyber Attacks during the War on Terrorism. A Predictive Analysis', 22 September 2001.

Institute of Electrical and Electronics Engineers, Inc., New York. See IEEE, *The IEEE Standard Dictionary of Electrical and Electronics Terms,* 6th ed., John Radatz Editor, 1996.

Janal D.S., *Risky Business*, John Wiley & Sons, Inc., New York, 1998.

Kaufer S., Mattman J., 'Workplace Violence: An Employer's Guide'. The text is available at the following URL: http://noworkviolence.com/articles/employers_guide.htm.

Kennish J. W., 'Violence in the Workplace', 2000. The text is available at the following URL: http://www.kennish.com/workplaceviolence/.

Kirby A., 'UN's early warning of climate disaster', 4 February 2001, available at the following URL: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1150000/1150290.stm.

Kovacich G. L., Jones A. (2002), 'What InfoSec professionals should know about information warfare tactics by terrorist – Part I', *Computers & Security*, Elsevier Science, vol. 21, No 1.

Kovacich G. L., Jones A. (2002), 'What InfoSec professionals should know about information warfare tactics by terrorist – Part II', *Computers & Security*, Elsevier Science, vol. 21, No. 2.

Laitinen A., Olgiati V. (edited by), *Crime-Risk-Security*, University of Turku, Publications of the Faculty of Law, Joint Studies Publications B, Series No. 8, 1999.

Leatherman J., Väyrynen R., 'Structure, Culture, and Territory: Three Sets of Early Warning Indicators.' Paper prepared for the Panel on Early Warning and Conflict Prevention in Intrastate Conflicts, *Annual Meeting of the International Studies Association*, Chicago, Illinois, 21 – 25 February 1995.

Leyden J., 'Curious employees are the biggest security risk', *The Register*, 4h March 2002. The text is available at the following URL: http://www.theregister.co.uk/content/55/24282.html.

Lyttle R., 'Computer Crime in 2002. An insider's Opinion', 25 January 2002.

Magklaras G. B., Furnell S. M. (2002), 'Insider Threat Prediction Tool: Evaluating the probability of IT misuse', *Computers & Security*, vol. 21, No. 1.

Maguire M., Morgan R., Reiner R. (edited by), *The Oxford Handbook of Criminology*, 2nd ed., Clarendon Press, Oxford, 1997.

National Integrity Systems, *The TI Source Book. Part B: Applying the Framework. Chapter 13: the Private-Corporate-Sector*. The text is available at the following URL: http://www.transparency.org/documents/source-book/b/Chapter_13/index.html.

Nikander I. O., 'Early warnings. A Phenomenon in Project Management', 2002. The text is available at the following URL: http://lib.hut.fi/Diss/2002/isbn9512258889/.

Ozenne T., 'The Economics of Bank Robbery', in Journal of Legal Studies, Vol. 3, 1974.

PricewaterhouseCoopers, *European Economic Crime Survey 2001*, 2001.

Schrodt P. A. and Gerner D. J., 'The Impact of Early Warning on Institutional Responses to Complex Humanitarian Crises', paper presented at the *Third Pan-European International Relations Conference and Joint Meeting with the International Studies Association*, Vienna, 16-19 September 1998.

Shaw E. D., Post J. M., Ruby K. G., 'Inside the Mind of the Insider'. The text is available at the following URL: http://www.securitymanagement.com/library/000762.html.

Shepard I. M., Durston R., *Thieves at Work: An Employer's Guide to Combating Workplace Dishonesty*, Washington, The Bureau of National Affairs, 1988.

Shimeall T., Williams P., Dunlevy C., 'Countering cyber war', *NATO review*, winter 2001/2002.

Smith R. G., 'Criminal Exploitation of New Technologies', *Trends and Issues in Crime and Criminal Justice*, n. 93, July, 1998.

Sussman M. A., 'The critical challenges from international high-tech and computer related crime at the millennium', *Duke Journal of Comparative and International Law*, vol. 9.

Sutherland E. H., *The professional thief*, University of Chicago Press, Chicago, 1937.

Sutton A., Tait D., McKenzie S., Bavinton F., 'Internet Crime Prevention', paper presented at the Conference *Internet Crime*, Melbourne, 16-17 February 1998.

Talbot D., 'See no evil', 16 May 2002. The text is available at the following URL: http://www.salon.com/news/feature/2002/05/16/knew/index_np.html.

Trevino L. K., Victor B., 'Peer Reporting of Unethical Behaviour: a Social Context Perspective', in *Academy of Management Journal*, 35:38-64, 1993.

U.S. Commission on Civil Rights, *Who is guarding the Guardians?*, Washington DC, 1981.

Verton D., 'Insider threat to security may be harder to detect, experts say', 12 April 2002, available at the following URL: http://www.computerworld.com/storyba/0,4125,NAV65-663_STO70112,00.html.

Walker S., Alpert G. P., Kenney D. J., 'Early Warning Systems: Responding to the Problem Police Officer', National Institute of Justice, July 2001. The text is available at the following URL: http://www.ncjrs.org/pdffiles1/nij/188565.pdf

Ward M., 'Employees seen as computer saboteurs', 29 April 2002, available at the following URL: http://www.news.bbc.uk/english/sci(tech/newsid_1946000/1946368.stm.

West Africa Network for Peace-Building, Centre for Conflict Research, Fewer, 'Conflict Analysis and Response Definition – Abridged Methodology', April 2001.

Williams C. A., Smith M. L., Young P. C., *Risk Management and Insurance*, 8th ed., McGraw-Hill Inc., 1998.

Zuckerman M. M., 'Moving towards a Holistic Approach to Risk Management Education – Teaching Business Security Management', *Security Journal*, 11 (1998).

ISSN 1824-274X
ISBN 978-88-8443-161-5