University of Piraeus
Faculty of Digital Systems
Department of Security of Digital Systems

The state of IT Security from a confidentiality-focused perspective and the role of IT Risk Management

MASTER THESIS

Submitted to: Prof. Dr. Günther Pernul and Prof.Dr. Sokratis Katsikas
Mentoring: Michael Weber

Submitted on 26th of February 2015

Submitted by:
Myrsini Athinaiou
Dr.-Gessler-Straße 15b
93051 Regensburg (Germany)
matriculation number. 1718030

University of Regensburg
Faculty of Business, Economics and Management Information Systems
Department of Information Systems
Prof. Dr. Günther Pernul

The state of IT Security from a confidentiality-focused perspective and the role of IT Risk Management

MASTER THESIS

Submitted to: Prof. Dr. Günther Pernul
Mentoring: Michael Weber

Submitted on 26th of February 2015

Submitted by:
Myrsini Athinaiou
Dr.-Gessler-Straße 15b
93051 Regensburg (Germany)
matriculation number. 1718030

Abstract

Information security is important for corporations. Decisions regarding security involve uncertainties, complexities related to various scientific and technological disciplines, and adverse impacts on business prosperity and goals. Risk management methodologies are widely accepted and used to increase the efficiency and effectiveness of information security, according to the priorities and limited resources of each firm. The common belief is that risk management offers a framework which summarizes scientific judgment and can be used to support decisions regarding the security of information. Still, every year and even on a daily bases, enterprises worldwide are reporting lost or stolen data and also suffer the various consequences. Legal penalties, diminishing reputation, lost costumers, financial losses are some of the most referenced examples. As risk management is used in the field of information security, it has been considered not only as a strengthening element but also as an opening. Some scientists and affected parties perceive risk management as narrowly focused, non-scientifically quantitative, overly quantitative, theoretical, and biased. If information security is related with risk management, if information security is violated, if failures of security are the cause of corporate loses, then where risk management has flows? Is it a matter of application or lies to the core of the practices? Is the concept of risk management misunderstood or security is unreachable? Those are some of the questions that were examined. A literature review shows that information security risk management is a scientific field for each own. Regarding security violations the paper shows that, especially regarding confidentiality, incidents occur worldwide. The impact of data breaches cannot be ignored in monetary terms as they lead to losses. Finally, the paper identifies possible sources of information risk management weaknesses. Future work could examine the given answers from different angles, time periods, and sample selection criteria. The importance and criticality of the issue can also lead to a depth analysis of how improvements in risk management will raise the efficiency of information security. Furthermore, other factors that can advance risk management practices can be found. This research focuses on confidentiality, integrity and availability oriented studies can be also held. It’s a field of growing importance, its critical for corporate success and as the value and amount of information increases more research is necessary.

Acknowledgments

First and foremost I would to thank Dr. Prof. Pernul and my advisor Michael Weber. It has been an honor to be taught from them. I appreciate all their contributions of time, ideas and motivation. I am also thankful for the corrections and the excellent example they have provided me of how scientific methods are implemented with consistency. Also all the members of the department of management information systems I (Wirtschaftsinformatik I) have contributed immensely through attendance to lectures, where they presented the state-of-the-art. I would also like to acknowledge Dr. Prof. Katsikas for his advice to study in the University of Regensburg and his support during all this time, from the very beginning of my master studies.

I have appreciated the insides Prof. Sneed gave me through Software Engineering lessons in the IT business reality, highlighted also how priorities differ based on cultures, regions and people. Communication, as a term, took a different dimension for me after his presentations, from a managerial perspective. I gratefully acknowledge the funding sources that made my master work possible. I was funded be the ERASMUS program of the University of Piraeus. Lastly, I would like to thank my family, the hidden heroes, that make the impossible possible for my sake and they have been an endless source of love and encouragement.

Table of Contents

Page

Page

List of Figures

Page

List of Tables

Page

Abbreviations

AOL	America Online
APT	Advanced Persistent Threat
ARPA	Advanced Research Project Agency
B.C.E.	Before Common Era
BYOD	Bring Your Own Devices
CAPM	Capital Asset Pricing Model
CAR	Cumulative Abnormal Returns
C.E.	Common Era
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIA	Confidentiality Integrity Availability
COBIT	Control Objectives for Information and Related Technology
CRO	Chief Risk Officer
CSI	Computer Security Institute
CVE/CVE-ID	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial- of-Service
DES	Data Encryption Standard
DMAIC	Define-Measure-Analyze-Improve-Control
DoS	Denial of Service
DT	Data/Decision Tree
GDP	Gross Domestic Product
GHS	Greek Hacking Scene
HIPAA	Health Insurance Portability and Accountability
IEC	International Electrotechnical Commission
Info Sec	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITRS	Identity Theft Resource Center
Ltd.	Limited Company
MIS	Management of Information Security

MIT	Massachusetts Institute of Technology
MOTD	Message of the Day
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OPAC	Online Public Access Catalogue
PCDA	Plan-Do-Check-Act
PSN	PlayStation Network
RSA	Rivest, Shamir and Adleman
SDLC	System Development Life Cycle
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
UK	United Kingdom
US	United States
WoV	Window of Vulnerability
XSS	Cross-Site Scripting

1 Introduction

Companies if they want to be competent and remain in the market they become unavoidable cyber. As was declared in the Accenture Technology Vision 2013, nowadays “every business is a digital business”. Technology is not just a current state of doing business, but the new business form adjusted to an interconnected and interdependent world. Enterprises use new technologies not just as means to operate more efficiently, but also to evolve their activities [Accen14]. This is, also, true for middle and small companies [NSBA13], especially in the field of telecommunications and technology [BCG10]. From the above can be contacted that today companies need technology to conduct business.

Undoubtedly, the new technologies come with many benefits but also with weaknesses and vulnerabilities, affecting not only companies but also governments and critical infrastructures [DHS05]. Focusing to enterprises, those vulnerabilities can be identified in various corporate areas such as, hardware, software, networks, databases, security policies and personnel. The fact that vulnerabilities databases and classification [SeHo05] exists, proves the criticality of the issue and the increasing number of errors found [Meun07]. The existence of vulnerabilities standardization, such as the Common Vulnerabilities and Exposures (CVE/CVE-ID) and Common Vulnerability Scoring System (CVSS) are another proof of the existence of vulnerabilities. In that way is clear that technology comes with vulnerabilities that eventually are identified.

The vulnerabilities identification is made ether from attackers or testers and security experts. Nevertheless, the existence of vulnerabilities leave space for attackers to exploit them and generally threats can materialize through the use of the new, let alone old and not supported technologies. Every year, many security companies like Sophos Ltd. [Soph14], Symantec [Symn14], McAfee Labs [McAL13] and many others, but also governments such as the Australian Institute of Criminology [Hutc12], which seems to be one of the most active, publish their findings about attacks, make predictions of how they will evolve and inform the public about computer security threats that big, medium and small companies should expect to face, currently and in the near future. Even in the Strategic Trends Programme of the UK Ministry of Defence 4th [MOD10] and 5th [MOD14] edition is clearly stated that cyber-attacks are expected to increase in importance and power. Globalization is the factor that magnifies the results and exposes anyone in more influences.

Facing those threats information security is being used for protection of the assets of an organization. Benchmarks and standards are usually set in order to adequate achieve a security of a specific level. Such standards are the ISO, COBIT, and Sarbanes-Oxley Act [HKSAR08]. As the majority of scientific terms information security "means different things to different people". According to the United States law, section 3542, Chapter 35, title 44, information security is "*defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modifications, or destruction in order to provide integrity, confidentiality and availability*." In other words, information security (InfoSec) is usually defined as a three dimensions defense practice.

According to section 3542 of the US code, "*Confidentiality means preserving authorized restrictions an access and disclosure, including means for protecting personal privacy and proprietary information.*", "*Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity*." and "*Availability means ensuring timely and reliable access to and use of information*." Usually those three dimensions are symbolized in a triangle, like the following depicted in Figure 1.

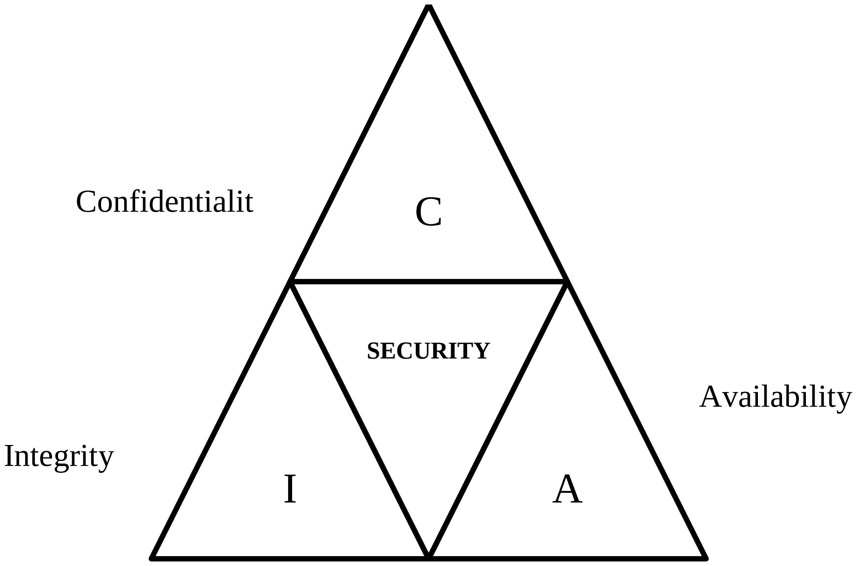

Figure 1: CIA Triad

1.1 Problem Description and Motivation

In the practice of information security, risk management plays an important role. Risk assessment, mitigation, evaluation and assessment processes are used to enable IT security decisions that optimize the benefits in correlation with the costs, supporting organization to achieve their mission [StGoFe02]. The main purposes of the use of risk management as an iterative and continually ongoing process, is to offer basis for security decisions based on evidences and control the impact of violations, enabling companies to achieve their goals [Hump02].

Highly distractive corporate cyber incidents, though, indicate that information security still fails to meet the security goals. Such incidents and well known are the case of in 2006 the AOL search data leak scandal, in 2007 the D.A. Davidson & Co failure to protect customer personal data, in 2008 the loss of blood donors data of Lifeblood, in 2009 the RockYou! password database breach, in 2010 the Ohio State University was hacked, in 2011 Sony experienced in their PlayStation Network a data breach, in 2012 the HSBC Bank USA National Association Names, Account numbers, account types, and phone, in 2013 Adobe Systems revealed that their corporate data base was hacked and in 2014 Home Depot suffered also a data breach. There even sites that report the data breaches of the year, such as the privacyrights.org or even of the day, for instance the databreachtoday.asia.

Such incidents pose many risks with serious consequences. Still in most cases there is no lasting damage. Nevertheless, when such incidents become publicly known, the impact for companies usually increases significantly [Pon13b]. In other words, data breaches come with costs, especially if individuals are informed about the potential source of the possible damage that may suffer [Pon12]. This is the main reason they cannot be neglected. Companies face the challenge to get even bankrupt as what they try to establish in years can be lost in the blink of the eyes. For a brief state of the situation Symantec [Pon13c] reported in 2013 that German and US companies had the most costly data breaches, \$199 and \$188 per record, respectively, with total cost for Germany at \$4.8 million and US at \$5.4 million.

From the various incidents that occur even though information security practices are followed, raises the question of where the weaknesses in the current state of measures are laid. As information security is usually implemented according and in relationship with risk management, a possible source of these breaches can exist in the risk management itself. In order to proof such a relationship, risk management should fail before information security and a way to verify that these incidents repeat in this sequence for a sustainable amount of cases, is necessary. If this causal relationship hypothesis can be proven, knowing what causes the information security failure, at an important percentage, would allow more effective predictions, influences and understanding.

The goal is to improve security practices focusing on the factors that create weaknesses. Even if the weaknesses may not be overcome, knowing the paths that lead the current attacks and technologies to violate the corporate and human rights, consists an important perspective of the situation. Assuming that the way risk management design and implementation is an important source of this misdirection of the security resources and forces, further examination is necessary. The most crucial factors that lead to risk management failure should be identified, studied, analyzed and if possible be measured and correlated. In this study emphasis will be given to the main factors that mislead risk management efficiency.

Having stated that, it should be added that the experience of the past is important, but the current technologies allow and more dynamic approaches, even real time, consequently a faster adjustment to the new threats it may be possible. As more intelligent attacks are expected, defense has also the means to advance. The aim is still related in terms of money and time. Security, seen as an important factor of success for corporations, is studied in relation to risk management flows, in order to allow a more focused analysis and dynamic development of solutions.

1.2 Structure and Objectives

In this research, after the comparison and contrast of information security and risk management, is examined if information security fails in terms of confidentiality, analyzing incidents in different geographical and time dimensions. In order to evaluate the importance of such security breaches, the cost of incident is taken from reviews. Also, estimation is attempted based on the number of records breached and the cost per record. This approach tries to show the impact of an incident for an organization. Finally, the factors that cause risk management to be less effective are identified and analyzed, to enable more focused future studies right in the core of the problem, if it lies where identified.

After a brief review of the related work in Chapters 2 and 3, the main body of this study begins with the analysis of the two milestones for this research: information security and risk management. In Chapter 5 the examination of studies of incidents where information security existed and failed, in terms of confidentiality and presents proof which shows that information security has still weaknesses and consequently space for improvement. In Chapter 6 review of cost estimations and a cost analysis by the author based on Ponemon institute data, indicate that weaknesses in information security cannot be neglected from companies as they are accompanied with costs. The factors, that possible consist the main limitations of the current risk management practices, are examined in Chapter 7 to conclude that risk management is not the problem itself. The critical factor is the way it is understood and applied. An analysis of the results and indications for future work are given in Chapter 8 along with the main conclusions and limitations. In the Appendixes section more information directly related with this study and especially the experiments conducted by the writer can be found.

2 Methodology

The research methods differ from each of the stages of the investigation, mainly in the part of analysis. Still the main pattern which is followed is that they are based on evidences already published. In other words the data processed in the ways that will be described soon in more detail, come from various credible sources but they are not data that have been proprietary collected from the author.

There are two main reasons for this research decision. First, the time limit for a master thesis and conducting it in a country which the market is unknown for the writer was the first obstacles that unavoidable led to a literature review approach. Secondly, the diversification and credibility of various sources in an international level are already available data that can produce valuable information, seen and analyzed from deferent ankles. Instead of seen the above as obstacles, is attempted to turn them into opportunities and give useful results for the community.

Because the research consists of a series of different approaches, it is considered as more appropriate each one of them to be reported more analytically separately in its relevant chapter, as a section. In the introductory section of each chapter the theoretical frameworks and methodology will be explained in more detail. Consequently, this chapter contains a high-level, general, description of the methodology that high lightens the reasons those choices where maid and what each approach tries to achieve.

For the part where case studies are analyzed three databases of reported data were used as proprietary sources, examining incidents from 2005 up to 2014. The time frame examined varies based on the experiment healed. The source databases are the privacyrights.org and the databreachtoday.asia. The purpose was to collect the most characteristic incidents for different market sectors, method of leakage, geographic and chronological period. The basic criteria for the collection of the incidents were the size of the damage caused in a combination with the above factors of type of operation, location, year of the incident and the source of the incident. This attempt tries to highlight the ongoing and long-term failure of information security.

In the cost analysis, a monetary approach was made. Data from 2006 up to 2014 about the number of data records breached were collected. An average incident cause loses among 5,000 and 100,000 records. Based on that, a further selection of data has been made. The remaining incidents were correlated with the estimated cost per record as estimated from the Ponemon Institute. Furthermore, throughout the above researches, a detailed literature review is presented alongside. The goal is to show a more thorough and representative picture of how reality may be. The calculations made and the reviews of other studies are important as it can be seen easily that security has lot of information available, compared to the past.

A structured literature review was conducted in order for the factors that affect possible negatively or at least eliminate the real potentials of risk management to be identified by the development of an initial pool of items to compare, present and construct. The goal is to collect and integrate the most important, that will be the most referenced. The attempt is to summarize, analyze and correlate these items in a neutral perspective. However, it is not possible to remain neutral. A broad coverage was attempted, but it is limited to those sources available to the public and those publications that are understood in terms of language. The results are organized and arranged conceptually, so that works relating to the same items appear together.

The following subsections describe the selection of sources and keywords with which we required the databases. A) Selection of Scientific Databases: For our collection of relevant publications, we used the following databases which taken together that allow searching security and IT-related journals, articles and papers. Those were mainly Google scholar, OPAC of University of Regensburg. This selection of scientific databases allowed searching the abstracts of Management Information Systems (MIS) journals and allowed accessing the full text the majority of them. It was chosen to query whole scientific databases without restricting the searches to specific journals or proceedings in order to gain high coverage of all relevant sources, to be as exhaustive as possible and to find more techniques and defensive tactics.

For the same reason, the queries were not restricted to a fixed time frame. We searched all covered years and did not exclude older papers. B) Selection of Keywords: we were looking for papers in English languages whose titles indicated that the publication is about IT security and especially risk management. Out of those, we were looking for papers that mention incidents or risk-related terms in either the title or the abstract, with an orientation to failure. The keywords were selected from domains of IT security and IT risk management. To assure the quality of the keywords, the selection was done iteratively by sending test queries to the databases and by adding multiple synonyms and plural forms. For the terms related to IT security, we added commonly mentioned attack models, and according acronyms.

Also, we queried the databases to search for papers with a title related to IT security and security-related terms, as well as risk manage weaknesses in title. We used further filters, such as searching for journals and proceedings only, papers with full text available as well as exclusion of psychology and chemistry journals. Application of these further search filters excluded papers and thus, reduced the set of relevant papers. The resulting papers identified by keywords search have subsequently been evaluated, based on their titles and other metadata, and later based on their abstracts in order to assess their relevance for this study.

Some papers were out of scope and were therefore excluded. Out of the remaining papers, access to a sustainable number was granted. These have been evaluated based on a review of the whole content. This step resulted in exclusion of another few more papers which were out of scope. Content analysis of the final papers resulted in this thesis. The high number of initial sources items required to reduce the number of items to a manageable set given the time and defuse mode of this research. More demonstrations of the way the methods chosen are fit with each one of the research questions. Also, how the data was collected, recorded and analyzed is described more clearly in each chapter, as well as, the rationale for sampling and the choice of representative cases.

3 Review of Previous Work and Terminology

Many studies have been already made in the field of security. In this section the main concept is the review of studies and the progress made in the field, especially related with what is being considered as the state-of-the-art. The main focus of the study is how to improve security, in terms of confidentiality, in the area of information and through the revision of risk management. For that reason, the studies that will display and discusses are those that mainly contribute to this study and where the credit should be given. If these works weren't already published, this paper wouldn't be able to be produced. Also, in every chapter the references will show with more accuracy what has been taken from whom or what idea has inspired a series of thoughts.

In this part, beginning from the term security and progressing to information security, an attempt to cover basic terms is made. The analysis of risk management and information risk management works, studies, polices and standardizations will be also presented, along with the related literature. This attempts to offer the description and explanation of basic terms in order for the main body of the study to be easier to understand for the reader, based on the same interpretations of the terminology. Furthermore, is important to mention from the beginning that a common glossary, easy to access is used and more specifically the revised glossary of NIST [NIST13]. This is based on a thought that even though the same language and words are used, the meaning sometimes differ, consequently a common reference was though as necessary for better understanding and more effective communication of the main ideas.

3.1 Information Security related Terminology

Security has been defined as *"a form of protection where a separation is created between the assets and the threat."* [Herz03] Generally, is applied to any tangible and intangible asset that is considered as valuable. But with the globalization and the connectivity to progress with light spread, security still remains limited in borders and funds. Balady and Lehman [BeLe72] referring to the five laws of software evolution stated the law of restricted growth. This is not the case for security; even if it is dependent on many parts with limits to evolve security can adjust based on logic and innovation, which is an only limited to human ability. But science may be possible to overcome this obstacle by creating even more intelligent humans [Yong13] or machines to take the place of personnel. As Kenneth Geers [Geer11] observe, security has evolved from a technical discipline to a strategic concept.

A common question is about the truthfulness or even the existence of security. Many scientists state that security is a mirage and if someone wants to define it should eliminate it in time, source of threat and cost [Schn99]. It exist though and another perspective that "*security is both a reality and a feeling*" [Schn07]. It seems that what is interpreted as the reality of security is what can be monitored, measured, predict and plan. On the other hand, security is related the individual psychological believes, ideas, actions and reactions to risks, threats, weaknesses, vulnerabilities, assessments, audits, rules, processes, procedures, standards and security measures. To put it simple how people behave and are manipulated from rewards and punishment.

The subjectivity is difficult to eliminate in security. The same is true for controls used. The term 'perceived security' is usually widely used in literature [MeHu12] [Räm11] to express this phenomenon. The interference of perception in security is critical as can turn the focus in the opposite direction from which the real threat is preying. That could be also the result when the existence of security measures give the illusion of security, whereas controls are not security and one measure may eliminate another and they may create new weaknesses. As it is commonly said 'every solution to a problem creates new problems' to deal with.

Another important term related to the perception of security is the term 'security theater' [Galt10]. What this term indicates is that security is deployed in order to make people feel secure. That also comes with the possibility of feeling insecure at a higher level than the real one. The sensitivity of its individual differs and lies to many factors, but in the context of security 'theater' is best used when leads people closer to the real picture [Schn07]. Of course, the level of 'theater' should not reach the extremes because those will unavoidable expose the valuable assets into more dangers and in a more brutal way as in a state of surprise they will be taken by force. That again will lead to the loop of misgauging the same source of danger in the future.

The broad field of security contains a series of terms, used in different scientific areas like in technology, finance, political studies and many others. Here those terms will be interpreted to cover the technological needs. For the presentation of the terminology many resources could have been used. Based on the acceptance definitions from standards were preferred as more accurate and complete. Also they form the main source of relevant definitions. Thus, the NIST glossary is the main source of the following brief terminology review.

Security derives from the need of assurance. From various sources such as SP 800-27, SP 800-37, SP 800-53A, CNSSI-4009, SP 800-39 and SP 800-63, assurance is defined as the ground or measure of confidence that the security goals are met, in terms of functionality, performance and polices. Sufficient protection is necessary to be used not only for sufficient resistance against intentional penetrations and by-passes, but also against unintentional errors. Those safeguards or countermeasures or controls are commonly considered according to SP 800-53, SP 800-37 and FIPS 200 as "actions, devices, procedures, techniques, or other measures" that aim to decrease the information systems' vulnerabilities.

Those countermeasures are the milestones of **defense**. The term 'defense' is usually followed from the term 'in breadth' or the term 'in depth'. In the first case defense is perceived as a set of multidisciplinary activities systematically planed and conducted through a system and its life-cycle [UMB12]. When security is applied in various levels of an organization in a corporate wide strategic plan which integrates technology, processes and personnel, defense is characterized as in depth. Today, an interesting term in defense is the characterization 'invisible'. It refers to the application of the latest discoveries in fields such as "*quantum mechanics, neuroscience and human consciousness*" with the goal to 'defuse tensions' and eliminate hostility. Targeting the root of hostility strives for peace, currently it is mainly related with national security [IDT] but it has a global potential by design.

Risk, for information security, derives mainly from the loss confidentiality, integrity and availability that will impact an organization. The risk is usually perceived through the likelihood and the consequences. At the one angle is the probability with which a danger may materialize, simply an exploit to be made or a vulnerability to be triggered. Secondly, the losses that may occur are part of the risk. FIPS 200 defines risk as "*the level of impact on organizational operations* *(including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring*."

Uncertainty is usually confused with risk. It implies that lack of certainty, as there is limited knowledge related either with the existing state or the final outcome. A common definition of uncertainty is the so called knightian uncertainty. Frank Knight at 1921 in his work entitled Risk, Uncertainty and Profit, identified the distinguish between risk and uncertainty. More specifically "*Uncertainty must be taken in a sense radically distinct from the familiar notion of risk, from which it has never been properly separated.... The essential fact is that 'risk' means in some cases a quantity susceptible of measurement, while at other times it is something distinctly not of this character; and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is really present and operating.... It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all.*" [Knig21].

In the common vocabulary of security also belong the terms vulnerability, weakness and exploit. The effects of hostility when they cannot be withstood are usually referred as vulnerability. According to SP 800-53, SP 800-53A, SP 800-37, SP 800-60, SP 800-115 and FIPS 200 **vulnerability** is the "*weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*." Another usually encountered term related to vulnerabilities is the **window of vulnerability** a.k.a. WoV and is used to define the time frame in which defense loses ground or is not existent [ArFiMc00].

In contrast to security comes the **insecurity**. A possibility that an incident has been investigated, evaluated and possesses a threat that may jeopardize the information that needs to be protected is a way to define it [GeKa02]. Any source of risk is a form of insecurity. Before we move to the analysis of information security the term classified information will be clarified. The information that is considered as sensitive requires, usually by low, to be protected in terms of confidentiality, integrity and availability. Access rights should be in place and any type of penetration is penalized. Usually clearance is needed from a separate body for the possession and processing of classified data. The information can be separated in levels of criticality and relevant security measures to be established accordingly.

In this context information security is defined as any practice and measure applied in order to protect against unauthorized access, processing, modification, disclosure or destruction (44 U.S.C. § 3542(b)(1)). Information Technology security or computer security is the set of measures, processes, tools and skills applied to protect against threats. They attempt to assure that data are protected when incidents of different types arise. Corporations pose in most of the cases a great volume of confidential information about their personnel, clients, products, patents, research and development projects, production, strategic plans, economic data and many others. This information is, in most of the cases, in electronic form. As a result, an unavoidable concern for organizations is how to balance the costs for security measures in relevance with the potential damage they may suffer in case of an incident.

Information security having evolved covers many technical aspects and it possesses also an interdisciplinary character. Risk management practices are used and the field of information security management system (ISMS) [Kers12] has evolved. Polices, processes and systems should be in place and manage risk. ISO/IEC 27001:2005 is based on the approach of the Deming cycle of Plan-Do-Check-Act, abbreviated and as PCDA, for the risk management process [Hump11]. The revised ISO/IEC 27001:2013 can be also used with different management processes, such as Six Sigmas and DMAIC. There are many more practices, for instance COBIT, the German IT baseline protection, the Japanese and Korean ISMS and others, for the risk management application in information systems. Also many studies have been made that analyze them and contrast them [ENISA06], [Str11], [ShWa07].

Four are the main components of the information security landscape: assets, threats, vulnerabilities and controls. In the context of security, asset is anything that has value for the owner and as a result needs to be under protection. The digital assets though, are in the intangible assets which imply that are invisible and also they can be relatively easily duplicated. The reason information security has emerged to a today's trend, lies in the existence of vulnerabilities. The term 'vulnerability' can be defined as a weakness in a digital system which can be exploited [WeSaRo09]. Among others common software vulnerabilities are when the user inputs software without confirming its validity, as well as when uploads files without ensuring the specifications of the file if are proper for the software, cross-site scripting, which occurs when the user’s input is used without verification from other users, buffer overflow when more data are in a storage location than it can hold and as a result other data are overwritten, missing authorization in parts of programs where the credentials of users are not required and unencrypted data, saved or transmitted over networks.

It is important to state hear that encryption sometimes is considered as panacea, but except from the fact that the safety offered is a matter of cost and time, sometimes there are other ways to attack without to have the need to deal with the obstacle of encryption. In other words, encryption should be tackled with caution, as any other security measure.

Penetration testing and **vulnerability assessment** are two common processes that sometimes are confused. Vulnerability testing emphasizes to the discovery and identification of areas where are vulnerable to computer attacks, whereas penetration testing focuses to the gain of access as much as possible and within the contract agreement [SANS06]. The basic steps in penetration testing are the planning and preparation, the information gathering and analysis, the vulnerability detection, the penetration attempt, the analysis and reporting and finally the cleaning up [SANS02]. In other words, the tester tries to learn the most possible about the target. After the software used can be assumed, common vulnerabilities are found and a verification of the software assumption can be made. In stealthy penetration test these processes will repeat before an attack is lanced, in vulnerability assessment though the attack will not be launched and if the vulnerability was exploitable or not won’t be found [SANS06].

Two are the main procedural vulnerabilities according to bibliography, the password procedures and the training procedures. The term ‘threat’ is referred to the methods, motives, skills and knowledge attackers possess and can use in order to take advantage of somebody else’s digital assets and retrieve from them what they need or want or put them under their command. The treats are uncountable as undetected are the vulnerabilities. Viruses, worms, malware, DOS and DDOS, phishing, Rootkits, Zero-day exploits, Zombies, packet sniffing, password cracking, social engineering, drive by download, are some of the most popular in the past and now. The role of security is to eliminate attacks, discourage attackers, minimize vulnerabilities and recover from damages. In order to avoid mistakes and best practices to be followed various controls are established. In many cases special guidelines deriving from protocols are applied. Controls are usually categorized in physical, non-technical methods of preventing damages and technical, which tend to be embedded in procedures and systems measures of prevention. [SANS02]

On the other hand, those measures that are well structured, like best practices, are well known and can be studied until an opening is found. At the same time, if security experts find the weakness first, then security is improving because of that exposure. Also, an attack that has been conducted can as well reveal the weakness or weaknesses existing in a system (like Pen Testing, but in those cases illegal). Furthermore, some advanced organizations have adopted very complicated IT control systems, which are difficult to understand, but they also train their people properly and many goals are efficiently achieved in that way, while at the same time an attacker easily realizes the risks and the consequences of attacking such corporations. But as many criminologists claim, lows and dangers are for those who won’t commit the crime. [SANS06]

Attackers are also categorized in various types. All of them have common characteristics. They don’t want to be caught; they search for access and communicate the weaknesses or information gained. Their behavior resembles in that way as they attempt to conceal themselves, escalate after access and earn money or recognition. The categorization of attackers is made based on various criteria. Some common criteria are their skill level, the resources usable to attackers, their motives and intentions as well as the possibility of a particular system to be attacked from a type of attacker [Heck05].

Attackers can also be classified to internal or external from a network perspective, passive or active based on their ability to change the status of the network and adaptive or static when after the attack has started can or can’t change their resources and continue to build their capabilities [Raym00]. Many stereotypes though interfere between the attackers’ profiles and the actual capabilities and views that they have [AtCa11]. Consequently, they should be taken as a base for further analysis; also many different methodologies can be used for more accurate results. Usually, each organization develops their own profile and categories of attackers.

As the majority of scientific terms **information security** “means different things to different people”. According to the United States law, section 3542, Chapter 35, title 44, information security is “defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modifications, or destruction in order to provide integrity, confidentiality and availability.”

- Confidentiality: According to section 3542 of the US code, “Confidentiality means preserving authorized restrictions an access and disclosure, including means for protecting personal privacy and proprietary information.”
- Integrity: “Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.”
- Availability: “Availability means ensuring timely and reliable access to and use of information.”

In the corporate environment competition is a common term. Security is an essential part, as technology is advanced but still imperfect. Any adversary will look for the competitors Achilles heel. The corporate systems are thus a very attractive and prominent target. The cyberspace is an arena where most companies face asymmetric threats compared to the means they can invest. At the same time, from a business perspective, whatever is an obstacle is also an opportunity. Each company’s IT system that becomes a target holds the field advantage. The attacked companies can make changes to their hardware and software at will. Predictable defenses are doomed to fail, as attacks evolve rapidly. What corporate competition in the cyber field shows, is that unique environments, unfriendly and unseen to attackers, before, can prove important for defenders. Security, in this dimension, is essential to be implemented based on imagination, creativity and the use of deception. [Geer11]

No organization can ignore security. Cyber threats jeopardize any company’s short and long term profitability and survival [Jam13]. Due to the intensiveness and aggressiveness of the cyber competition among not only companies, the term ‘cyber war’ has emerged. This term make any electronic device a target and a weapon. Synonymous to cyber war are the terms *“speed, surprise, economy of force and asymmetry”* [Geer11]. In the bibliography is identified that once a system becomes important for the user, attacks emerge. They are followed by defense mechanisms and discovering techniques. Then more advanced attacks are lunched and improved more sophisticated defense emerge. In other words an ‘arms race’ is taking place where attackers and defenders compete [YaYu13]. Cyber war makes also possible its existence to be only known from the direct participants. Thus, any observation based on data published has a limited truthfulness and relation to the reality.

3.2 Corporations and Risk Management

From a corporate point of view, source of threat can be many different groups and people. Criminals with intent to make money through fraud, operating usually in groups, industrial competitors and foreign intelligent services that search to learn the competitive advantage, hackers challenged to penetrate a system and disrupt operations and hactivists moved by ideologies and political reasons are some of the outsiders that a company is threatened. Inside the company also the company’s own employees pose a threat, with malicious intents or unintended mistakes. The goals of the attackers, when targeting a company, can also vary. Intellectual property, commercial sensitive data, disruption of operations, exploitation of weakness targeting partners, subsidiaries and suppliers are some of the common targets. [UKG12]

Every danger, no matter the source or the motive, is understood as risk. The word risk it seems to derive from the old French world *risqué*, which means “danger, in which there is an element of chance” [Litt63]. Another term commonly used in risk management is the word hazard, which comes from a game of chance invented at a castle named Hasart, in Palestine, while it was under siege [OxEnDic89]. Games of chance and gambling were depicted in Egyptian tomb paintings from 3500 B.C.E., but a “scientific” or statistical basis for gambling was presented during the Renaissance. This was because the Hindu-Arabic numbering system appeared in Europe between 1000–1200 C.E. allowing calculations beyond simple addition and subtraction to be performed. However, it wasn’t until the Renaissance that the ten digits 0-9 replaced fully the Roman numerals[Litt63].

During the Renaissance, Girolamo Cardano, a sixteenth-century physician, gambler, and mathematician wrote a book titled, *Liber de Ludo Aleae* (“Book on Games of Chance”) that seems to be the first study of probability in cards, dice throwing, and gambling. Also, Galileo, in about 1630, wrote a brief essay, *Sopra le Scoperte dei Dadi* (“On Playing Dice”), in part to please Cosimo II, the Grand

Duke of Tuscany. According to Bernstein, other great thinkers contributed to the growing body of literature on the subject. Mathematicians and those organizing large bodies of data such as birth and death records established properties and rules concerning sampling, actuarial tables, and ways to predict behavior and events occurring in population. [Litt63]

Money and financial interests drove early thinking on the topic of risk. Aristotle, in his treatise *Politics*, discusses the concept of *options* – a financial instrument that allows individuals to buy and sell goods from one another at pre-arranged prices. Since then the derivative market has grown and also the term insurance. Insurance is a financial tool that reduces risk for a person or party by “sharing” potential financial burdens with others, who are compensated in various ways for taking on the added risk. The roots of insurance reach back to 1800 B.C.E. when it was used to help finance voyages by ships. An early form of life insurance was provided by trade and craft guilds in Greece and Rome. Lloyds of London, one of the best-known insurance companies in the world, was born in a coffee shop near the Tower of London in 1687, in part because the shop was a gathering place for ship captains who shared information about past and upcoming voyages, routes, weather, and hazards. [Litt63]

Uses on insurance have expanded greatly since. The Industrial Revolution created new risks derived from technological factors. Steam engines, especially in ships, were the vulnerability that could cost more human lives than any other human invention until the late 1700s. Since the Industrial Revolution, risks and hazards have transformed rapidly. The size, usability and potential disasters vary [PDA12]. After World War II, large companies with diversified portfolios of physical assets began to develop self-insurance against risks, which they covered as effectively as insurers for many small risks [EhBe72]; [DiEe85].

Risk management began to be studied after World War II, associated with the use of market insurance to protect individuals and companies from losses associated with accidents. Several sources [Croc82]; [WiHe95]; [HaNi03] date the origin of modern risk management to 1955-1964. The first two academic books were published by Mehr and Hedges [MeHe63] and Williams and Hems [WiHe64]. In 1980s, still with a financial orientation, risk regulations began, with firms developing internal risk management models and cost calculation formulas to hedge risks and reduce losses. Risk management acquired its importance in corporations in the late 1990s, where management policy and monitoring of risks was reported to the board of directors. Risk management or audit committees led to the creation of the Chief Risk Officer (CRO) position. Merrill Lynch in 1987 created the first risk management department in a bank. [DiGe13]

Various scandals occurred in 1994-1995 associated with misuse and speculation of derivatives, and with an increasing impact. Many regulations emerged to govern such incidents. The financial crises and security violations are an everyday proof that those rules, regulations and methods don’t prevent effectively the worst. The goal of risk management though is not safety, but in a corporate environment risk management aims to create a reference framework that will allow companies to handle risk and uncertainty, at acceptable levels for their own needs. An integrated risk management approach must evaluate, control, and monitor all risks and their dependences to which the company is exposed. [Litt63]

In general, risk is a combination of the probability or frequency of an event and its consequences, which are usually negative, unwanted. It can be measured by the volatility of results and the distribution of incidents during time. Uncertainty is less precise because the probability of an uncertain event is often unknown, as is its consequence. In this case, it is preferably to refer to precautionary rather than preventive activities to protect against uncertainty. Lastly, in finance, risk related to activities with future risks that may generate positive or negative results. The term risk has also been categorized in the business terminology to pure, market, default, operational, liquidity and many others. [DiGe13]

3.3 Scope and Logic of this study

As enterprises are all the more dependent on automation and integration, in this study, the emphasis is given to the information security risk management. Here the risk is related to the use of information technology and digital systems [StGoFe02]. The IT risk requires as the other risks, such as market risk, credit risk, operational risk and liquidity risk, treatment and management preferably based on comprehensive framework and guiding principles. In Figure 2 is shown the elements involved in risk management. Identifying the potential risks, assessing, measuring, monitoring and controlling them are the necessary general steps that an organization needs to undertake in order to meet its strategic goals and objectives [TeAs10]. Information technology risk management takes those processes and deals with the unique characteristics of technology and cyberspace.

The process and methodology of risk management is adjusted to the stature, environment and nature of information systems.

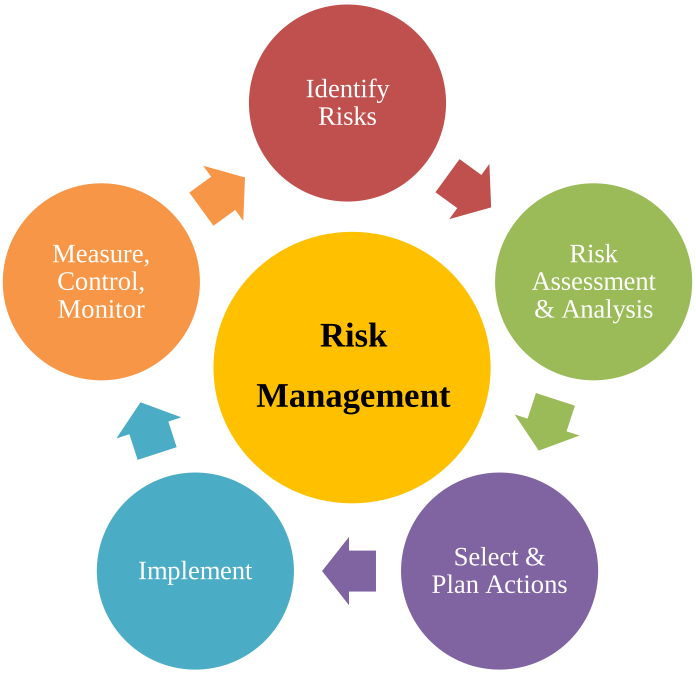

Figure 2: Risk Management Process

Having seen some of the important basic terminology used in this thesis, the structure of the research will be briefly presented. Risk management and information security will be examined an analyzed in more detail in the next chapter as they are in the core of the research subject. The aim is to examine the state of IT Security, focused on the aspect of confidentiality and connect it to the IT risk management practices and objectives. In order for that attempt to be achieved is necessary first to examine the relationship between security and risk management, then to evaluate the state of confidentiality from a technological perspective. After that if the subject is of financial interest, especially for organization, IT risk management practices will be analyzed.

The remainder of this thesis is structured as shown in Figure 3, Table 1 shows which sections are related to our four research questions presented in Chapter 2. The research is assembled in four parts:

- Part 1: Risk Management and Information Security
- Part 2: Confidentiality Violations
- Part 3: Impact/Cost of Data Breaches

- Part 4: Objectives and Obstacles of IT Risk Management

These parts examine the relationship of information security and risk management, the state of information security, focused on confidentiality, analyzes the impact of security failures and searches of advances in IT risk management to improve the current state of information security.

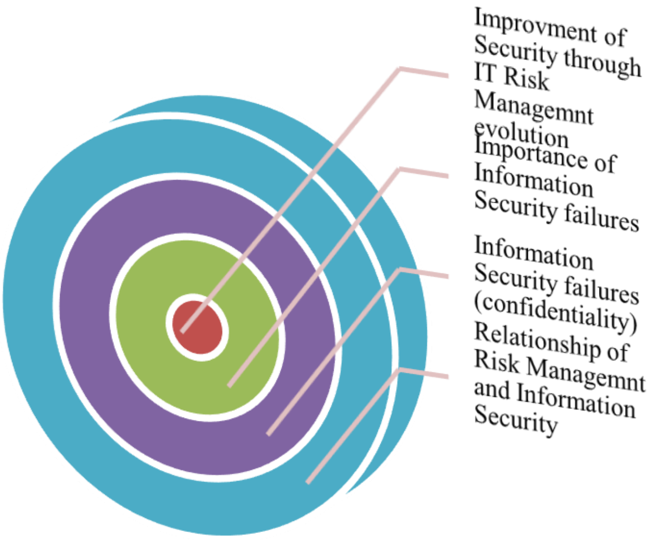
Improvment of Security through IT Risk Managemnt evolution
Importance of Information Security failures
Information Security failures (confidentiality)
Relationship of Risk Managemnt and Information Security

Figure 3: Structure of this thesis

Table 1: Research Questions and Chapters

Chapter	Research Question
Chapter 4: Risk Management and Information Security	What is the relationship between IT Risk Management and Information Security?
Chapter 5: Information Security Fails	Does Information Security fail? (emphasis to confidentiality)
Chapter 6: Cost of Data Breaches	What is the impact of Information Security failures?
Chapter 7: Factors that lead to Risk Management Failure	What factors of It Risk Management should be reexamined and evolve to improve Information Security?

The foundations of relevant technologies and the theoretical background are introduced in Chapter 3. Based on these foundations the main part of this thesis is divided into four major components. First, Chapter 4 presents an in depth description of the differences and similarities of risk management and information security and examines their relationship. IT security failures with an emphasis to confidentiality are studied from multiple angles in Chapter 5, in order to examine the hypothesis that information security fails. In Chapter 6, is presented and estimated the impact of information security failures in monetary terms. The purpose is to verify that this area of study is of importance to corporations. Finally, in Chapter 7, we analyze the factors that may keep the potentials of IT risk management limited. In that way the areas where the information security inefficiency is lying are tried to be identified. This study attempts to serve as a basis and indication of the weaknesses that can be improved or adjusted to improve the implementation of information security. In Chapter 7 the conclusions and limitations of this research are stated, along with indications about future work.

4 Risk Management and Information Security

The purpose of this chapter is to present the main goals and methods used from information security and risk management. Apart from the presentation of the basic issues in the field examined from experts, the weaknesses found will be discussed. In our research breaches of information security are examined. How information security is related with risk management is what this chapter attempts to discover and present. It is a quest that has a changing answer through time. At the early years searching for a connection between information security and risk management is like searching for a 'needle in a haystack'. The one was preceding the other; still their components were eventually related and finally connected.

The relationship of information security and risk management is essential to be established in order to be able through the examination of the violations of security to discover areas of risk management that can be improved. The research conducted for this chapter, explores past literature sources related to information security, risk management and offers a comprehensive view of how those two areas have formed the information security risk management. This section is the first one analyzed because as Ormerod has remarked, it is hard to navigate with a map if you are unaware of your current position [Orm03].

4.1 Information Security

Current markets are worldwide characterized from uncertainty. It is therefore important, especially for corporations to improve their ability regarding information security. For that purpose to be accomplished there is a necessity to understand the history of information security. The reason derives from the need to explain why the current situation is formed in that way and seemingly vulnerabilities, data thefts, cyber-attacks and hacking, look never-ending. Ignorance is a luxury because it is followed from costs. Knowing the root causes of a situation help to prevent the same errors to occur and to prepare actions rather than thoughtless but necessary reactions [Bel10].

Information security has started along with the existence of information [RuGa91]. As data were stored, transmitted and processed, their protection emerged as a prerequisite. During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage [Bhav08]. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD (Message Of The Day) file, and another administrator was editing the password file, but a software glitch mixed the two files, and the entire password file was printed on every output file. [Sal98].

Security imposed on documents, adjusted to telegraphs, then to telecommunications and finally can be applied in all kind of devices, especially digital. During World War II, when the first mainframes were developed to accomplish more complex and sophisticated tasks and communication code breaking begun. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data by means such as badges, keys, and the facial recognition of authorized personnel by security guards [Sal98]. At the same time, the need for communication among the mainframes became necessary. The Department of Defense’s Advanced Research Project Agency (ARPA) began examining the feasibility of a networked communications system to support the military’s exchange of data. Larry Roberts, developed the project—which was called ARPANET [Bhav08].

In the early 1970s public key cryptography came into existence. The Data Encryption Standard (DES) was adopted by the then National Bureau of Standards (NBS) of USA, known today as the National Institute of Standards and Technology (NIST). At around the same period, as ARPANET became popular and more widely used, the potentials of weaknesses increased. In 1973 Robert M. Metcalfe developed Ethernet, one of the most popular networking protocols. That led to the identification of fundamental security problems of ARPANET [Denn98]. Some of the problems found were, vulnerable passwords, lack of safety for dial-up connections, insufficient protection from unauthorized remote users of individual remote and nonexistent user identification and authorization processed to the system. The growing need to maintain primarily national security, eventually led to more complex and more technologically sophisticated computer security measures [Bhav08].

Computing hardware was moving to automated production. In parallel operating systems were also evolving and the concept of microprogramming was introduced by IBM in 1960. The microprocessor brought the personal computer and a new age of computing. Mini-computers, like PDP-8, PDP-12, and the PDP-11 series, were introduced by DEC in the mid-1960s and early 1970s. During this time, O/S technology made the leap from single-user/batch to multi-user and timesharing. Thus the concept of security in the form of memory protection was introduced for both the hardware and software dimensions [Bel10]. In 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. In October of 1967 formulated recommendations, which ultimately became the contents of the Rand Report R-609, which was the first widely recognized published document to identify the role of management and policy issues in computer security [Ware79].

The use and popularity of computers was exploding at a phenomenal rate. In addition, businesses were becoming totally dependent upon these machines and less tolerant of shutdowns and malfunctions, including hardware and software installations and upgrades. Companies started to automate their process and operations. Soon, new security threats appeared threatened critical corporate data stored on easily accessible secondary storage [Stol00]. The scope of information security further widened. For economic purposes the interface between hardware and software had to remain static for upward compatibility purposes. There has been little innovation in this area for twenty-five years, and any fundamentally different operating system, requiring the purchase and deployment of an entire set of new apps was not financially possible. Slow changes were made but with the preservation of existing architectures. As Dr. Belovich has put it very nicely *“while some evolution is still happening, revolution has almost ceased”* [Bel10].

The decentralization of data processing systems **in the 1980s** gave rise to the interconnection among personal computers and mainframe computers. The computer community was able to use all the available resources together. The networking capabilities arise. In the late 1980s also the anti-virus software started to appear [Car08]. At the close of the twentieth century, networks of computers became more common as well as the connection of these networks to each other. Security was not required for early networks because access was physically controlled. This gave rise to the Internet, which was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals [Bhav08]. While networking was improving, the initial operating systems for PCs discarded or ignored concepts of shared resources, multi-user access, memory protection, multi-layer operation modes, privileges and quotas regarding among mainframe and mini computers [Bel10].

Towards the end of the 1990s attackers changed from using worms and viruses to more sophisticated attacks. The introduction of distributed denial of service (DDoS) and malicious code attached to business emails (spam) and web pages shifted the focus of security to gateways and firewalls were introduced [DlEl08]. Although the weaknesses of the desktop operating system were well-known early on, IT managers found the technology to be very attractive, convenient, easier to understand and cheap. The maintenance contracts were expensive, but the ‘scale-up’ of computers for enterprises became rapidly. Information security, that period, was perceived as a “necessary evil that hinders productivity.” [Co-Mu03] but as the network boundaries disappeared and attackers had financial objective [Gelb06], enterprises became more interested to invest in the field. Making profits is important, but keeping them is a task that requires measures and eventually came to realize it.

Clearly, businesses require more secure systems but the marketplace is not providing it because it's listening to the consumer side and any core change will be costly. Then, more digital devices appeared to the market. Personal Digital Assistants, Smart phones, Laptops, Tablets, PCs, Sensors, Cloud and others emerged [DlEl08]. **In the 2000s** it is difficult to clearly define a computer, because all those devices in an essence are computers. Mobile computing, with roaming capabilities, Bluetooth and Wi-Fi, create an even broader realm where security is challenged. Online payment systems, e-banking, e-commerce, social media, mobile applications made security issues even more critical. The demand grew far faster than the ability of the market to deliver them and security wasn’t and isn’t a priority in development. Is another factor that is taken into account, but when the cost is presented the priority is diminishing. This high demand put an unbelievable time pressure on software suppliers and systems integrators to get the job done in a specific deadline, regardless of the number of bugs. They are corrected in the various relishes and updates later [Bel10].

It is said that every solution creates new problems. There is a belief that economics and the size of the changes required make effective security impossible. Fundamental changes are not affordable and the users-consumers are trained in a direction already designed. There is no universal software quality, reliability and safety standards and it has been yet to found a ‘bag-free’ way to develop software. Also, in the market, software of same general functionality can be found in redundant quantities [Snee14]. Hardware is also evolving with quantum computers, sensors, smart grid and internet of things, emerge. Again, those developments take the weaknesses of the past, create better protocols and energy efficient machines, improved cryptography and are advertised with increased functionality and utility. Simply, time will reveal the weaknesses. Imperfect humans create imperfect machines. But that may be for our shake. Privacy and other aspects of security are initially protected, but the overall culture and sensitivity of the majority has changed. When a crime occurs everybody searches for cameras, but when they are in home usually they ask for privacy, or actually selective exposures that make them ‘look good’.

As cryptography initially it was an art but nowadays is a science. Information security has a broader spectrum, a wider impact and an increasing criticality [DlEl08]. Information security contains many and different field. In some cases is depicted as a puzzle. One of these puzzles is the one presented in Figure 4, which is based on an illustration initially presented from Dr. Rizomiliotis [Riz14]. Security in a corporate environment can be segregated, as it takes many forms and variations. They various forms of security depend on each other and together build the concept of security [Finn00]. Information security has evolved, addressing minor and also dealing with incidents of huge organizational impact. As times changed, threats and attacks have incised in sophistication and severity of the impact caused. When information is endangered, the consequences depend upon the other information the attackers poses and the importance of the data contained. Furthermore, what it looks trivial and revealed easily, in some cases is the information that allows an attack to begin and escalate. Thus information security is related with the necessity of being alerted at all times and it’s not only related with the past, present or future.

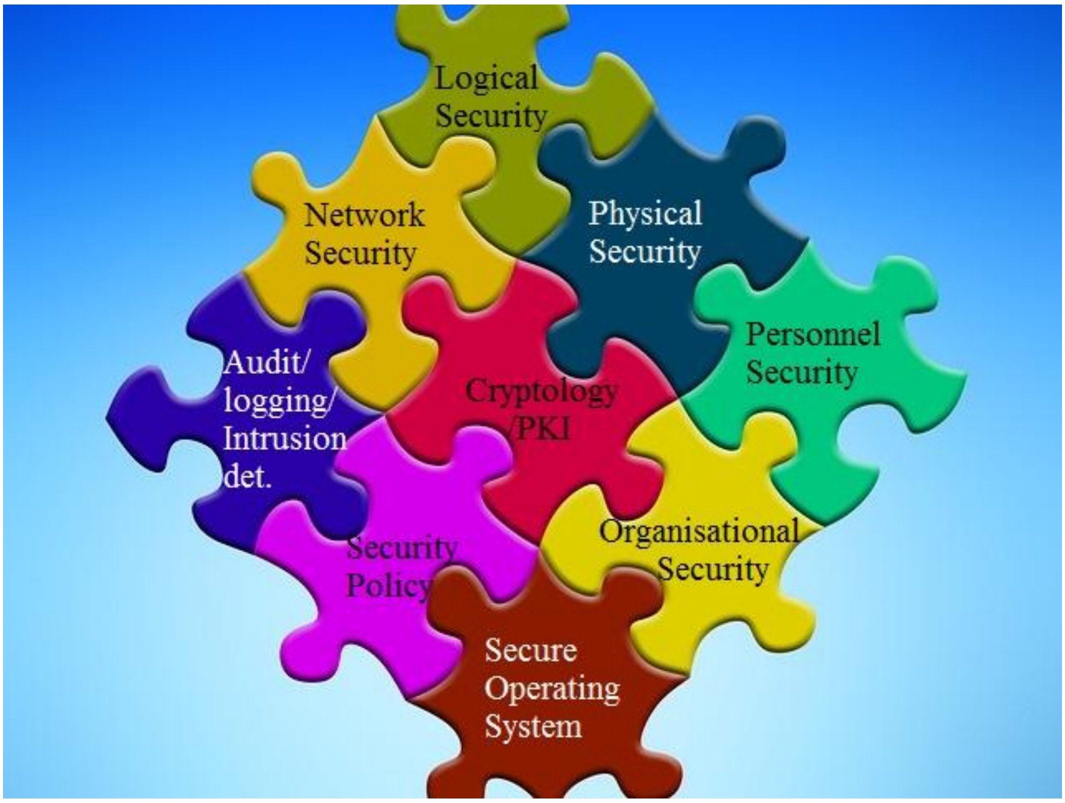

Figure 4: The puzzle of Information Security

Eventually has been realized that security controls alone cannot enforce a secure IT environment. There is the need to be supported by proper operational controls, that they will dictate the actions and behavior of users when working with information [Ross99]. From the above it can be derived that the need for security is evident and the lack of security prevalent, consequently various standards and certifications have arisen to ensure certain sustainable levels of security. The DoD (Department of Defense), the NIST (National Institute of Standards and Technology), NIAP (National Information Assurance Partnership) and the ISO (International Standards Organization), along with many others, have all issued and/or endorsed standards for system security [Bel10]. By Dlamini et al. information security has been characterized as a 'moving target' [DlEl08] and that is indicated from the changes required in the standards. In order to understand better what and how is regulated regarding information security, a brief presentation of some of the most important standards is following.

4.2 Information Security related Standards

Security can be assured and regulated from different perspectives, such as technical and operational. From a technical perspective, in 1983 the USA published the Trusted Computer Security Evaluation Criteria (TCSEC), commonly known as the Orange Book and in 1990 the European Commission announced the Information Technology Security Evaluation Criteria (ITSEC, 1990), known as the White Book. Their differences are that TCSEC only evaluates technical security features of products, whereas ITSEC evaluates products as well as systems. The factors examined through evaluation are functionality, assurance of correctness and effectiveness. In application of those factors TCSEC consider all three factors together, whereas ITSEC handles functionality independently and assurance of correctness and effectiveness together. They have also many other differences, but as far as individual organizations were concerned, with their use, evaluating their products and systems, secure operating environments wasn't achieved but a structured attempt has been made [Ross99].

A secure IT corporate environment was also necessary. To plan and manage IT security in a company effectively security plan for technology alone needs to be established. Many IT security programs appeared to cover this need, in the form of guidelines. GMITS, CobiT, IT Baseline Protection Manual, Generally Accepted Information Security Principles (GAISP), the System Security Engineering CMM (SSE-CMM) [SSE99], and BS7799 and its derivatives (BS7799, BS ISO/IEC17799: 2000), COSO, ISO 31000, Basel II etc. briefly shown in Figure 5, based on the ISACA presentation [Fisc09]. Some of them will be briefly presented. The purpose is to give a general picture of what has been established and the needs covered.

GMITS or TR 13335 was introduced jointly by the International Standards Organization (ISO) and the International Electro-technical Commission (IEC). In these guidelines, the IT security issue is put in place for top and/or senior management, important definitions, concepts, models, are given and explained to ensure a common understanding of the terminology and describes IT security management and planning aspects and is relevant to design, implementation, testing, procurement, or operation of IT systems and managers who are responsible for activities that make substantial use of IT systems [Ross99].

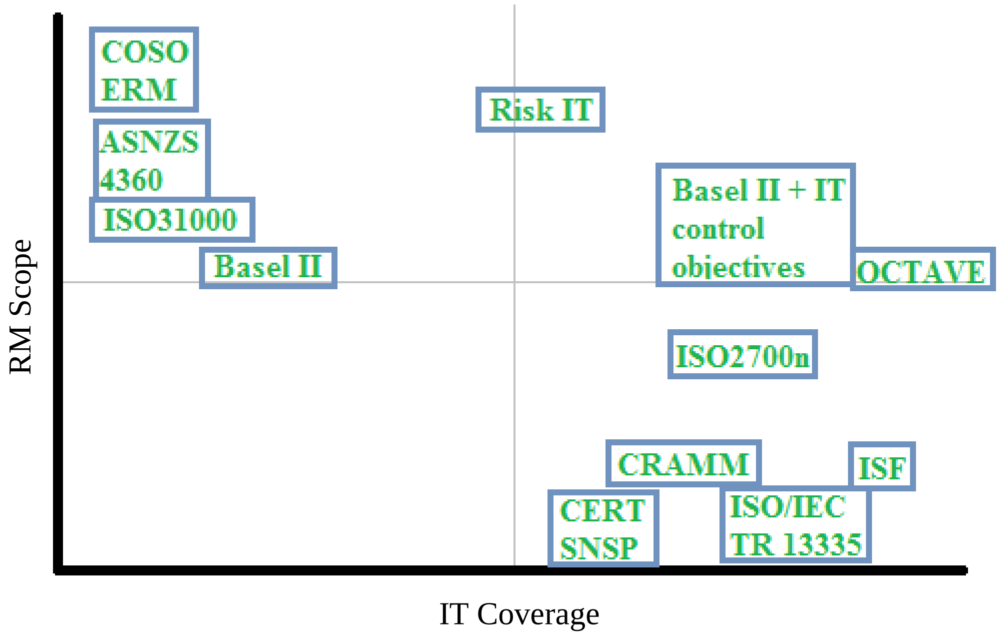

Figure 5: IT risk-related frameworks

Another security standard is the **BS 7799-2:2002** which is referring to information security management systems and specifies their use. Also, **BS 7799-3:2006** give guidelines for information security risk management [SiWi09].

The **ISO/IEC 20000** is a family of standards which is continually improved and updated. A complete catalog of the ISO standards can be found in the web page of ISO(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on&includesc=true). **ISO/IEC 27000:2014** with an introduction and basic terminology has recently being updated. **ISO/IEC 27001:2013** specifies requirements for an information security management system where an organization needs to demonstrate its ability to protect information security assets and give confidence to interested parties. **ISO/IEC 27002:2013** provides implementation guidance that can be used for the continuing improvement of controls in order information security to be maintained. **ISO/IEC 27003:2010** provides practical guidance for implementing an information security management system based on ISO/IEC 27001:2005. **ISO/IEC 27004:2009** provides guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.

ISO/IEC 27005:2011 provides guidelines for an organization to define their approach to risk management to address the requirements in ISO/IEC 27001.

ISO/IEC 27006:2011 specifies requirements for bodies providing audit and certification of information security management systems. **ISO/IEC 27007:2011** gives guidance on the principles of auditing, managing audit programs, conducting quality management system audits and environmental management system audits, and the competence of quality and environmental management system auditors. **ISO/IEC 27011:2008** contains an implementation baseline of ISM within telecommunications organizations to ensure the confidentiality, integrity and availability (CIA) of telecommunications facilities and services. **ISO/IEC 27031:2011** is relevant to business continuity management as an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand and value creating activities.

ISO/IEC 27032:2012 is the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect organization and user's assets on the cyber environment. **ISO/IEC 27033** consists of many parts, under the general title *Information* technology — *Security techniques* — *Network Security*. It was developed to replace the ISO/IEC 18028 for network security. Consists from the parts *Overview and concepts, Guidelines for the design and implementation of network security, Reference networking scenarios – Risks, design techniques and control issues, Securing Communications between networks using security gateways - Risks, design techniques and control issues, Securing communications across networks using Virtual Private Networks (VPNs) - Risks, design techniques and control issues.* Under development are the parts *IP convergence* and *Wireless.*

ISO/IEC 27034 which also consists from more than one parts, provides guidelines for application security. It specifies an application security life cycle, incorporating the security activities and controls for use as part of an application life cycle, covering applications developed through internal development, external acquisition, outsourcing/offshoring[1], or hybrid approaches. **ISO/IEC 27035:2011** provides the information and guidance for organizations to implement and maintain a quality approach for information security incident management. **ISO/IEC 27036** gives in different parts, guidelines for supplier relationships, provides an overview and common requirements for supply chain security. **ISO/IEC 27017:2015** is still under development and it would be related to cloud computing security and privacy management system and security controls. It will provide guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 [ISO.org] [iso27001security.com]. in Table 2 those standards are presented in a more brief way.

Table 2: ISO standards for IT

ISO/IEC 27000:2014	Overview of ISNS, terminology.
ISO/IEC 27001:2013	Specification of requirements for establishing, implementing, maintaining, monitoring ISMS and assess and treat information security risks.
ISO/IEC 27002:2013	Guidelines for organizational information security standards and information security management practices.
ISO/IEC 27003:2010	Design and implementation aspects of ISMS.
ISO/IEC 27004:2009	Measures and measurements for implementation assessment of ISMS and controls.
ISO/IEC 27005:2011	Guidelines for information security risk management.
ISO/IEC 27006:2011	Specifies requirements and provides guidance for bodies providing audit and certification of ISMS.
ISO/IEC 27007:2011	Guidelines on how to manage an ISMS audit program, conduct the audits, and on the competences of ISMS auditors.
ISO/IEC 27011:2008	Support in the implementation of information security management in telecommunications organizations.
ISO/IEC 27031:2011	Concepts and principles for having and improving the information and Communication technology readiness of an organization, to ensure business continuity.
ISO/IEC 27032:2012	Guidelines for improvement of Cybersecurity.
ISO/IEC 27033-1:2009	Overview and guidance on network security.
ISO/IEC 27034-1:2011	Assist in the integration of security into the processes used for managing their application.
ISO/IEC 27035:2011	Structured approach to information security incident management (detection, report, assessment, response, management, continuous monitoring).
ISO/IEC 27036-1:2014	Overview of the security of corporate information and information systems within the context of supplier relationships.
ISO/IEC 27017:2015*	Information security controls for cloud services.

The above brief presentation of the security standards, indicate that information security is a system. Farn, Lin and Fung resemble information security to a chain which is as resilient as its weakest knot [FaLiFu04]. With the wide spread use of technology and the increasing dependence of enterprises, information security needs to be secured. The corporate environment needs to assure a level of security and for that risk management processes become necessary to be established [SaAl11]. As Peter Bernstein has identified past and present are divided from the thread of danger. In the past risk was something only the gods knew, until humans used the past, current factors and assessment methods to make predictions based on different scenarios [Bern96]. Security is not only a matter of measures, processes and controls, quality is also important, but in order to examine those aspects, risk management is the angle from which information security has to be seen through. It follows a brief introduction to risk management, to make the connection with information security clearer.

4.3 Risk Management

Risk management is a very broad area. Information has become a core factor to most business activities. Without the right information in time, quality and quantity, business will be unable to operate and achieve their strategic goals [Owen98]. To ensure business continuity, the protection of information resources must be pursued. When a company doesn’t have information, or information that loss, disclosure, modification or availability won’t impact the operations, security is not an issue. In all other cases, the company needs to apply risk management practices for information security [Brod01]. Caelli et al. defines the aim of risk management to the identification, measurement and control of “uncertain events” in order to minimize possible losses and optimize the return on investments for security purposes [CaLo89]. Risk Management in the field of information security, should be applied to all aspects of how information is created, processed, stored and disposed. The identification, assessment and prioritization of risks, followed by monitor and control measures are used in order to protect the company from possible events that if they occur there is a probability of damage [Hub09]. In other words the main goal of risk management is to help organizations better manage risks associated with their missions [NIST98].

Risk management is important because every corporate unit must be assured that the organization has the needed ability to achieve the intended goals. The best controls and measures for encountering obstacles in the completion of the business missions should be selected among the various security measures. The process of selection is unavoidable, because the affordable solutions are countable. In other words security choices should be made, because of financial constraints. Effective use of risk management processes help managers to identify the controls needed to maintain IT factors at an acceptable level and for this reason most organizations allocate budgets for IT security more effectively, according to their purposes [GeSo05].

A risk can be deled in four ways. It is common in risk management the choices to variety among four alternatives. Avoidance of the risk, meaning that no action is taken that could lead to a specific exposure, reduction, with investment or controls to mitigate the possibility or the impact of occurrence, transfer the risk to someone else, for example an insurance and acceptance of the risk [Hub09]. According to Hamid Tohidi, the effective application of risk management requires its integration to the five stages of System Development Life Cycle (SDLC). The stages are presented more analytically in based on a more complete table presented and analyzed in Tahidi's relevant article [Toh11]. As it has been presented in the previous chapter, risk management consists of many steps. The first process is risk assessment, which estimated the sources of danger and the likelihood of future hazardous events. The output of this step is used for the choice of proper controls and reduction of risk exposure. These are main issues dealt in the risk reduction step, which prioritizes and evaluates risks in order controls to be placed where mitigation is considered as necessary. Continues assessment and evaluation of the existence, proper functionality and update of the current controls is briefly the last, ongoing step [StGoFe02].

Table 3: System Development Life Cycle Stages

System Development Life Cycle stages	**Risk Management role**
Start (need, purpose and scope of the system)	Identification of risks to support a system.
Development (design, purchase, programming, reconstruction)	Use of defined risks to support the development of an IT system.
Operation (functional, tested, approved)	Risk management processes used to support evaluation of a system's operation.

System Development Life Cycle stages	**Risk Management role**
Protection (changes for ongoing improvement according to processes, polices, etc. when functioning)	Risk management continuous monitoring gives feedback to environmental/organizational/technological changes that affect a system.
Administration (h/s, filtering, rejection, destruction, activation of information)	Assurance of proper hardware and software resources consumption.

Giving emphasis to risk analysis phase, it was traditionally used to analyze risks posing a threat to mostly IT assets [Jun99]. That led to the rise of security controls used to reduce the risks that were considered as important to acceptable levels. Risk analysis is used from information security professionals in order to establish the feasibility of information systems controls. It can be held prior or after the occurrence of an incident [Brod01]. As it has been mentioned information security is a multidisciplinary field [Lyyt90]. The interdisciplinary nature of information security raises concerns about the effectiveness of risk management. As the use of IT changes and becomes increasingly more important and critical for business operations, the security controls have to be adjusted [GeSo01]. In literature there is a belief that risk management fails in terms of scientific method. It lacks, according to this opinion, statistical rigor and is subject to social misuse. It is possible that risk analysis is misconceived [Bask91]. There is a difference between the perception of risk and the actual risk. As technological knowledge is used for practical and especially, for this study, corporate purposes, the terms risk and risk management should be connected with information technology.

4.4 Information Security and Risk Management

Information security is part of the larger corporate strategy for managing risk and compliance [Lew13]. When dealing with information security the risks cannot be totally eliminated, because of the nature of the subject of information security and because some risks are beyond the reach of what a corporation can control or predict [Finn00]. Technologies, like hardware, software and network tools have also been perceived as assisting to the risk management process, providing valid data for better decisions regarding IT risks [Loud02]. It seems that information technology and risk management can assist one another. The use of information technology may come with risks which hinder the success of businesses, but companies can control those risks applying effective risk management through the use of technology, which boosts the effectiveness and efficiency of risk management [BaRi05]. Teymouri and Ashoori have investigated the impact information security may have on risk management. Examining the IT usage in 50 Iranian oil companies, have concluded that IT tools assist risk management process [TeAs10].

Standard administrative security structures seem to be inefficient after a while in a dynamic and flexibly technological environment, where deception, cheating and concealing are just tools used for higher purposes. Like the protection of a company's information, costumer/consumers data, mergers and acquisitions that can impact stakeholders worldwide and many others. In this essence, other constructive models of risk have been examined. 'After action reviews' form a standard practice which recognizes that plans and standards operation in some cases properly, may not be as effective in different context, settings, means and participants. [Comf05]

Decision making, especially for risk, drops under emotions of stress [Flin97]. The models used assess the problem from different angles and perspectives, identifying alternatives and comparing them with consequences and their likelihood. Risk management doesn't finish but it should be performed in a mode where the actions taken prevent potential failures from occurring or/and escalating. But under the factor of stress/pressure what is text is the current corporate performance against a model. The context is difficult to be taken into account especially if the mental security model is complicated, but application of any control doesn't define security [Kle93]. Time, cost, subjects and settings should be adjusted.

Companies seem that they have to avoid the unknown and the chaos. The same goes for disaster. But where one losses money some else gets them. In this state, risk management is not about security, but to manage when more or less security is needed. For the continuity of companies risk prevention and counter threats are crucial. As it has been already stated although risk management approaches differ, based on their implementation, the stages of identification, assessment, prioritization and continuous monitoring are fundamental [AlDo05]. Risk management in information security is complex. Requires knowledge about the assets, their values, weaknesses, vulnerabilities, threats, probabilities to be stolen, modified, unavailable etc. Then those factors should be balances with economic impact of threats and the cost of controls and countermeasures [NIST11]. They are already studies that combine risk-aware business processes with security practices to support operations with security controls that benefit businesses [GoEk08].

In the current market place, in order for companies to compete and survive, information and information systems are assets that have to be protected. As it has been mentioned, in the information security literature, attacks, threats, consequences and defenses have been examined [DiP-C05]. As IT and information become all the more valuable and data seem to be more lucrative than money in all cases except those that are spend for more money, research examines security aspects in relation to management practices [ChHo06]. In the corporate environment management is crucial and here relevant to information security. Information security is linked to risk management in corporate environments where the prerequisites and benefits are understood. The role of users is crucial to the results delivered [SpBe10].

For companies' terms such as trust, intellectual property, networks, communications, databases are of importance and need to be taken into consideration when risk management is applied for information security. According to risk management physical, personnel, hardware, software and procedural security can be applied and modified according to changes in effectiveness, prioritization, cost, criticality, convenience and others. [FaNa05]

With information systems many things can go wrong. But the cost of security violation incidents as it will be shown in Chapter 6 can't be neglected, not only in monetary terms that over the business impact it may result. As has been seen many standards indicate that is a best practice for information security risk management to be applied. Before the effect of risk management to information security effectiveness is examined the current state of information security is analyzed and the impact of violations of confidentiality is attempted to be quantified in the following two chapters.

5 Information Security Fails

Part of the main hypothesis is that information security fails, more specifically concerning violations of confidentiality. In order to examine this statement, an analysis of three stages is conducted. It starts from historical review and security statistical analysis held from well recognized and accepted organizations. After the main points of the already examined and published material regarding the state of security are stated, specific areas and case studies are conducted and presented in order to show what, from data available to the public, someone can observe about security.

5.1 Brief History of Data Breaches

The list below is not intended to be comprehensive, but to saw how information security has been emerged from the need of protection. By knowing these and other incidents it becomes also clear that technology and legislation have difficulties to move in parallel and generally that results in spaces which attackers take advantage of. Furthermore, it becomes clear that information security fails in the course of time and worldwide.

The core technologies of the Internet, i.e. TCP and IP, were finalized in 1981. There was no mention of security in these technologies. From that can be assumed that the scientific society was not, at that time period, concerned about the security of the UNIX systems, which were widely used at universities and various organizations, such as banks and telecommunications. [Geer11]

Computer intrusions began soon after TCP and IP were integrated into industrial equipment. The most highly published incident of this time was the gang of 414’s, a group consisting by six teenagers from Milwaukee. Their name comes from the telephone area code of Milwaukee. With the use of home computers, phone lines and default passwords, were able to break into approximately 60 high-profile computer systems. The incident received wide coverage, including a Newsweek cover story titled “Beware: Hackers at play.” It is believed that this was the first time the term ‘hacker’ was used in the context of IT security. While harm hadn’t been caused, the simple tricks in the hands of professionals with controversial interests can cause damages, which are difficult to estimate and predict. The US Congress realized the extend those incidents could take and after some other important incidents reacted, passing in 1986 the Computer Fraud and Abuse Act which recognized as illegal the actions of breaking into federal and commercial computer systems.

In the network dimension, Robert Morris longed as a student the first, very intelligent, warm. The threat was found relatively early from suspicious logs, seemingly from MIT but finally from Cornell University, and mainly university professionals disassembled the code and by sharing information between them and other organizations, such as NASA, they were able stop it before its real potentials were shown. The reasons of this attack are officially an attempt to measure the size of the Internet, but others sources seem to refer to a more aim oriented attack. This action was the first convicted under the 1986 Computer Fraud and Abuse Act. As a result of this incident the US Government established the CERT/CC (CERT coordination center) at Carnegie Mellon University as a single point to coordinate industry-government response to Internet emergencies. [Geer11]

Microsoft released on August 24 of 1995 Windows 95, an operating system with graphical interface. At the beginning it didn’t have security features as it was originally designed for individual desktops. The fact that most users didn’t used passwords, most applications run with administrative privileges and TCP/IP technology was combined with the above, has led to what Dan Geer called in 2011 [GeerD11], the source of the information security profession.

In 1996 the Health Insurance Portability and Accountability act, known and as HIPAA, focused on the protection of the sensitive data of patients. In order to lower the health costs this act supported the use of electronic health records. The confidentiality of these records brings the importance of security with intension to a first raw prerequisite. [Geer11]

Reomel Ramores and Onel de Guzman, from Philippines, released on 5th of May, 2000 the well-known ILOVEYOU virus [ArnW00]. The virus deleted images on infected computers and automatically sent itself as an email attachment to the Outlook contacts list of infected computers. The impact of the virus was pervasive, millions of computers were infected and the costs derived were estimated to billions. The attackers were traced but lack of legislation in Philippines led to non-conviction. [ArnW00]

This incident has showed from very early that the law faces a new challenge, trying to cope with the speed of the technological advances. Corporate fraud incidents like Enron's, Tyco's and WorldCom's, led to the establishment of the Sarbanes-Oxley Act in 2002. This Act makes the key executives accountable for the correctness and truthfulness of the financial reports, on which investors decisions are based. Section 404 requires the declaration from CEO and CFO for personal knowledge of all the information in annual reports, based in formal internal controls, had a major impact in the security profession as more investments have been made to the establishment of security controls. [Geer11]

In December of 2006, T.J. Maxx reported breach, started from July 2005. Investigations showed that other groups were also hacked, included Office Max and Boston Market. The group wanted to drive along US Route 1 in Miami and seek out insecure store with wireless networks to enter the corporate networks. As the attacks became more advances these methods took the form of SQL injection attacks to enter the networks at Hannaford Brothers and Heartland Payment Systems, a credit card payment processing company. SQL attacks created an awareness of the need to pay attention to information security during software development and introduced the term "secure SDLC" to the IT lexicon. [Geer11]

In 2008 Georgia became victim of distributed denial of service attacks (DDOS) [Naz09]. Aim was many media and government organizations, which they couldn't communicate news to their incidents. This incident in literature is referred reluctantly, as it is relatively recent, as cyber war tactic. The same one was used in Estonia. DDOS and DOS attacks have earned popularity during the last years, but it is believed that their more advanced forms are those that the systems operate but not to their fool potential. Generally, it can be observed a shift in the behavior of the attackers. Whereas in the past they would make their presence known to the victims, recently they prefer to remain silent until the right moment or as long as they need. [Naz09]

In 2009 Wall Street Journal [GoCoDr09] reported that intruders had broken into the computer networks of defense contractors developing the Joint Strike Fighter (F-35 Lightning II). Also the same source [Gorm09] reported that the US electricity grid had been penetrated and software has been inserted that can cause damage by remote control. On this basis on June 23, 2009 it was established the US Cyber Command for defense and reaction. Concerns aroused at the same time for the civilian Internet users, in this point it may be important to note that Internet started from Arpanet and is given to the public, which has accepted it. [GoCoDr09]

On 12th of January, 2010, Google had detected an attempt to steal its intellectual property originating from China (Operation Aurora) [Damb10]. The attackers were also aiming to access email of Chinese human-rights activists. The US Government after investigation traced the attacks to two educational institutions in China, the Shanghai Jiaotong University and the Lanxiang Vocational School. [Damb10]

On 17th of April, 2011, Sony PlayStation Network (PSN) announced that hackers had obtained personal information on the 70 million subscribers of the network. Because of uncertainty relative to the existence or not of breach in credit card numbers, the company took the network offline. The impact for young users and their families seemed to be bigger compared to the network affected from the attack. [Anth11]

In 2012 two Liberal Russian media outlets and an election watchdog became victim to huge cyber-attacks during Russian elections. Sites belonging to the Ekho Moskvy radio station, online news portal slon.ru and election watchdog, Golos, went down on December the 4th [Aust11]. Not even Coca Cola was immune from hackers [Kum11]. A hacker called Greek Hacking Scene (GHS) defaced the official company’s website. The Personal cyber war between India and Pakistani hacking crews is ongoing. One of the incidents was from Indishell who performed a huge defacement campaign against websites belonging to Pakistan which affected more than 800 sites [Pass12]. Africa is also in the field of the cyberwar. A planned and coordinated bank robbery of over $6.7 million executed during the first three days of the New Year in Johannesburg, targeting South African Postbank [Vaas12].

One of the most well-known and analyzed attacks of 2013 was against Target. The attackers gained access in the computer network of Target and stole financial and personal information of 110 million customers of Target’s. After that they removed this information from the company’s server in Eastern Europe [CCST14]. At the end of 2012, the L0NGwave99 Digital Group launches the “Operation Digital Tornado” [Schw12] and took down the NASDAQ stock exchange besides a number of US stock markets. More precisely the taken down sites include: nasdaq.com, batstrading.com, cboe.com, ms4x.com, www.mynasdaqomx.com, www.esignal.com. Members of TeaMp0isoN target the UK's foreign intelligence organization, MI6, for accusing innocent people of terrorism, so they drop a 24 hour phone bomb on them and after the phone bombing stopped, TriCk, the leader of the group, called the MI6 offices in London and made fun [Mezz12].

A small number of eBay's employees' log-in credentials were compromised in 2014. That resulted in 145 million of customers to be affected and investigations from state attorneys general and the UK Information Commissioner's Office to be held. The customers' information compromised varies from encrypted passwords, names, e-mail and mail addresses to phone numbers and dates of birth [Wake14]. With 4.5 million affected the Community Health Systems incidents was the largest health data breach of the year. A Chinese group seems to be suspected for breaching the organizations system and pilfering sensitive patient details [FiCa14]. Sony Pictures was hit with a massive malware that resulted in the exposure of intellectual property and employee personal details. There is a debate about the source of the attack whether or not was launched by North Korea [Schw14].

The interest today for security reaches the space. The main idea is that security and space are two correlated ideas. The world is all the more dependent on space-based services. The space domain face also a number of security risks and any factor that can degrade the current state will impact interactions among nations and people. Software developed to jam or to take control of a satellite constellation and collision with space debris are some of the current challenges. Security failures cannot be neglected as they threaten the stability and security of any governmental, corporate and scientific space activity [SSI13].

It is clear from the above that the cyberspace is an arena of conflict "that basic defense and attack strategies are still unclear" as Kenneth Geers [Geer11] have stated. The data breaches are spread during the years and knowledge about attackers and attacks increase. The security world has been taught that size and sector don't matter. Every company is vulnerable to attacks, and the consequences can derail companies and employees careers [Roma14]. In the next subsection a perspective from studies of security companies will be presented.

"If a system is connected to the Internet or operating on a wireless frequency, it can and will be exploited" [DHS09]. In the category of technological system crime many offences are included, such as use viruses, worms, trojans, bots, privilege escalation, unauthorized access, modification or theft of information, denial of service, website defacement, jamming of network traffic, etc. As it can be easily observed, the majority of those criminal offences are business related. Technological means are widely used as milestones in communication and commerce. Since the adoption of those technologies has from a new state of transactions of any type, security breaches result in important losses for all the participants and stakeholders but also for anyone not only directly but also indirectly related to a breach [Wang10]. Knowing better the current situation is a necessity for more accurate actions in the future.

5.2 Review of Information Security Studies

This subsection presents a review of the breaches occurred, based on media reports and expert analyses that have been published since the incidents were publicly acknowledged. Facts already available in the public record provide a great deal of useful information about the attackers' methods and defenses. The emphasis here is to present the overall picture of the most current situation in the security area in order to analyze in the next chapter the consequences of violations for enterprises. The reports refer mostly to the analysis of breaches between 2010 and 2014; the reason is that every five years approximately important changes occur in security. Having data for the most current five years gives a sustainable base to depict the state of change or the situation as close to reality as possible, with the credibility of its sources.

In the technical report of Infosecurity Europe and PwC in 2010 [PWC10], has been found that business environment changes rabidly, the popularity of social networks and the use of software as a service created new vulnerabilities, technical controls should be combined with processes, people and technology to protect organizations, awareness of the dangers is important for all the participants and collaborations among companies give new opportunities. In numbers, 92% of large organizations, of more than 250 employees, had a security incident and 45 was the average (median) number of breaches. Furthermore, 62% were infected by a virus or malicious software, 61% has detected a significant attempt to break into their network, 15% have detected actual penetration by an unauthorized outsider into their network and 25% has suffered a denial of service attack. For small organizations, less than 50 employees, 83% had a security incident and 14 was the average (median) number of breaches. Important are also the findings that 46% of large companies responded to the survey had staff lose or leak confidential data and 45% of confidentiality breaches were very serious. [PWC10]

In the security intelligent report of Microsoft [Micr11] the infections per country are depicted in Figure 6. Worldwide the host infection rate from malware and unwonted software were the first quarter of 2010 10.8, the second quarter 9.6, the third 9.9 and the fourth 8.7, the average of the year 9.75. The report contains 117 countries/regions and assesses the threats from a global perspective. That indicates once more that security violations and threats are existent worldwide. In this particular study the countries with the most software vulnerabilities and exploits, malicious code threats and potentially unwanted software are Turkey, Spain, Korea, Taiwan and Brazil. Other countries that rang high are Poland, Mexico, Portugal, El Salvador, Peru, Hungary, Greece and Saudi Arabia. The data from 2010 would have changed but still they are of importance as they address the global character of the security challenge. [Micr11]

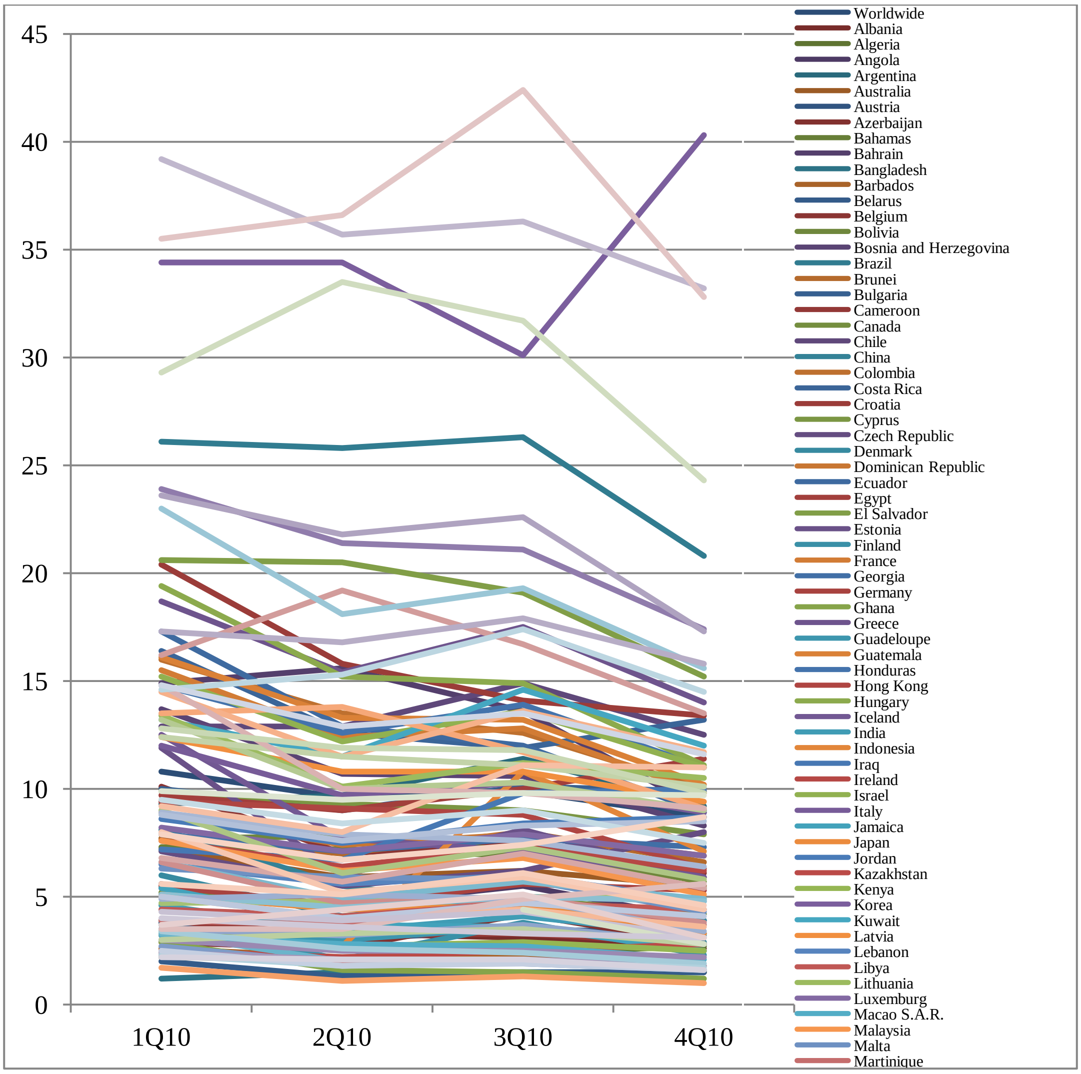

Figure 6: Host Infection Rate per Country, 2010

As it is stated in the 15th annual computer crime and security survey of the Computer Security Institute (CSI) "*Understanding the cyber threat is the first step in defending against it*." [CSI11]. In the same report it is found that for 2010 malware infection is the most common attack with 67.1% of the respondents reporting it, 45.6% of the respondents have experienced at least one security incident in the year. Furthermore, 22% of the respondents have encountered incidents involving targeted attacks, 3% experienced more than 10 targeted attacks, that was a strong indication that targeted attacks are not theoretical but evolve as a subject of importance for security. Except from malware infection other attacks were 'being fraudulently represented as sender of phishing messages', theft or loss of laptop or mobile devices, bots/zombies within the company, denial of service and unauthorized access and privilege escalation from an insider. [CSI11]

In the Public Interest Advocacy Centre study in 2011 [PIAC12] for data breaches in Canada it was found that they are vastly underreported from the private sector and the Best Buy and Air Miles case studies are examined to revile legal actions necessary to improve. The Californian Department of Justice in 2012, again in the same context of how state laws can improve to protect/prevent against data breaches and increase security, found that 55% of the breaches resulted from intentional intrusions by outsiders or by unauthorized insiders. The remaining 45% resulted from failures to adopt or carry out appropriate security measures. In addition, the retail industry reported 26% the majority of the data breaches, followed by 23% of financial and insurance institutions. In average a breach involved the information of 22,500 individuals. [PIAC12]

In the 'Cybersecurity: Authoritative reports and Resources' of Rita Tehan [Teh14], they are summarized the findings based on statistics of other studies relevant to cyber incidents, data breaches and cybercrime. Some relevant to the context of the current study is that 48% of large companies and 32% of all the companies have been victims of social engineering attacks. Also hacking attacks seem to be responsible for 25.8% of the data breaches reported in the Breach Report of 2011 from The Identity Resource Center. Electronic devices and data that leave corporate premises are responsible for breaches with 18.1% and 13.4% of the data breaches occur due to insiders. [Teh14]

Navigant's 'Information Security Data Breach Report' updated on April 2012 [Nav12], identifies healthcare entities as the main target of data breaches and the slowest in discovering and disclosing such incidents. Hacking attacks target companies with 50% to 67% of the cases. The average number of records breached per incident fluctuates among the last two quarters of the year from 18,253 to 31,069, with an increase of 71%. The types of organizations experiencing data breaches following healthcare are corporations with 27%, education with 16% and government with 10%. The types of data breached are mostly names, social security numbers, and contact information, date of birth, medical information, financial, credit cards, e-mails and miscellaneous. [Nav12]

Verizon's data breach report of 2012 [Ver12] identifies in terms of sources outsiders as the dominating agents that commit theft of corporate data with 98%, whereas insider incidents follow with 4% and reduction compared to the 2011 date of -13%. Less than 1% of the breaches were committed by business partners.

The breaches occurred 81% from hacking, 69% incorporating malware, 10% involving physical attacks, 7% employing social tactics and 5% from misuse of privileges. Generally the targets seem to be selected based on opportunity (79%) rather than on choice. In other words most of the victims possess an exploitable weakness and thus the majority of attacks are not highly difficult and unavoidable. [Ver12]

In the RiskBase Security 'An Executive's Guide to Data Breach Trends in 2012' [RBS12], the business sector is identified as the main sources of incidents reported with 60.6%, followed by 17.9% from government, 12,6% from education and 9,5% from the medical sector. Sources of the incidents once more are mainly with 76.8% external agents and 19.5% insiders. Also, 84.7% of the records exposed belonged to the business sector, 12.6% to governments, 1.6% to education and 1.1% in the medical/healthcare sector. The Shanghai Roadway incident alone that year exposed approximately 150 million records from a total of 267 million records exposed in that year. Excluding this incident the median of records exposed in 2012 was 55,863 records breached. [RBS12]

The Executive Summary of the technical report of PwC and InfoSecurity Europe 2013 for United Kingdom [PWC13] show that 93% of large organizations has a security breach, with an increase in the average number of breaches per year. In the same direction, 87% of the small businesses had a security breach with 17 incidents to be the median for a small business, compared to 113 incidents to be the average of breaches suffered by a large organization. The sources are 78% outsiders for large companies and 63% for smaller businesses. From the respondents 23% hadn't carried any form of security risk assessment and 31% don't evaluate if the security measures are effective, 26% hadn't inform the board on security risks and 93% of companies had security polices poorly understood from staff and consequently suffered staff-related breaches. [PWC13]

Check Point security report for 2013 [Chec13] botnets are identified as a threat that will remain, affecting 63% of the organizations that year. Also hosts accessing malicious websites occur in 75% of the organizations. With 71% United States are by far the country were the most malware was found, followed by Canada (8%) and the United Kingdom(4%). Important to mention are also Germany, Israel and Turkey with 3% and China, Czech Republic, France and Slovakia with 2%. More exploits are also result of increased number of vulnerabilities. In 2010 the vulnerabilities were 5279, in 2011: 5235 and in 2012: 5672. Most susceptible to cyber-attacks are the popular products used from companies coming from vendors such as Oracle (384), Apple (260), Microsoft (222), Firefox (150), Adobe (119), Cisco (119), IBM (118), Google (80), PHP (62) and HP (59). The types of attacks were buffer overflow (32%), corruption of memory (32%), DoS (32%), code execution (24%) and stack overflow (19%). [Chec13]

The Irish Information Security and Cyber Survey of Deloitte and EMC^2 [DelE13] found that 49% of the respondents consider their organizations unprepared to deal with cybercrime incidents, 33% believes that detection of cybercrimes is inappropriate and not adequate, 67% haven’t searched for insurance solutions and 63% finds that their organization is partially equipped or the company to have not sufficient means to deal with cybercrime. External or internal incidents identified weren’t followed up in 57% of the respondents. They also believe that the evolution of already existent threats possesses the major challenge of information security (30%). The existing policies are viewed from a 76% as partially or even failing to address the rapid changes in the technological and business environment. [DelE13]

In the European Parliament’s report entitled ‘Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts’ in 2013 [EUPar13], it is mentioned the lack of a common framework, under which security incidents and data breaches are collected. The trends resulting from various reports resulting from different private and public institutions suggest that incidents are increasing, but the rate of increase is characterized as uncertain. Consequently, the effects of policy innervations are difficult to estimate. Eurostat data indicate that 0.004% of GDP is the impact of all types of security incidents and for other countries is 0.061% of GDP. They also present different sources for data breaches such as anecdotal evidences, industry statistics, official statistics and reports from information security companies and present some of the most crucial findings for the context examined. [EUPar13]

Kaspersky Lab and B2B International [Kasp13] state that maintenance of the information security infrastructure is a major challenge for IT management, 91% of the respondents had at least on external security incident and 85% of the companies surveyed had internal incidents. The cost of serious incidents is estimated between $649,000 for large companies and $50,000 for small and medium-size enterprises. Some of the most popular external threats are in 66% viruses, worms, spyware and other malicious programs, 61% spam, 36% phishing attacks, 24% network intrusion/hacking, 21% theft of mobile devices and 19% DoS and DDoS. Common internal threats are 39% vulnerabilities/flaws of existing software, 32% accidental leakage and sharing of data by staff, 30% comes from loss or theft of mobile devices and 19% from intentional leaks of data by staff. Mobile phones emerge to a big threat for sensitive and business data. [Kasp13]

The Ponemon Institute in ‘The Post Breach Boom’ [Pon13a] report characterizes the data breaches as fact for the daily life of organizations. It identifies that incidents increased in severity and frequency and security investments are also directed to forensic and investigation tools. Negligence of employee or contractor and malfunction and error systems are considered as the main types of data breaches, occurring within the business unit or when transmitting data to a third party. Failure to wipe or degauss a device with sensitive and confidential data has occurred in 44% and lost devices were the reason of breach in 39% of the cases. The time of discovery of data breaches is in average 80 days for malicious incidents and 49 days for non-malicious. [Pon13a]

Sophos security threat report for 2013 [Soph13] highlights the fact that polices such as bring your own devices (BYOD) and the use of cloud services give to data a higher mobility compared to the past. Platforms are also more diversified and mobile devices have emerged to an important target of malware. Also, with the mobility and the various devices that in some cases belong to the employees raises the question of who is the responsible party that owns, manages and secures the data. As the main source of malware remains the web. Blackhole emerges as threat with a 30% approximately. More accurately has been found that 58.5% comes from drive by redirect, 26.7% from drive by redirect (blackhole) and 7.5% from payloads. Countries of origin for Blackhole exploit sites are United States (30.81%), Russia (17.88%), Chile (10.77%), Italy (5.75%), Turkey (5.74%) and China (5.22%). Targeted attacks also increase in importance and impact. [Soph13]

Verizon’s data breach investigations report for 2013 [Ver13] deviates in terms of threat actors 92% of the breaches to be caused from external actors, 14% from internal actors, 1% from partners, 7% involved multiple parties and 19% from state-affiliated actors. The targets were 38% large organizations, 37% of the breaches have affected financial institutions, 24% retail companies and restaurants, 20% manufacturing and transportation utilities and 20% information and services firms. Hacking with 52% of the breaches is the main threat action, followed by malware (40%), physical (35%), social engineering attacks (29%), misuse of data (13%) and errors (2%). Compromised assets were mainly servers (54%), users (71%), people (29%), media (6%) and networks (1%). [Ver13]

WhiteHat Security [WSec13] reported that out of all the websites tested 86% had at least one serious vulnerability, with an average of 56 vulnerabilities each. From those vulnerabilities 61% were resolved requiring a median of 193 days from the first notification from the customer. In terms of protection website security 57% of the companies provide relevant training to their programmers, 53% has centralized security controls, 39% perform static code analysis to the underlying applications of their websites and 55% uses we application firewall (WAF). From the organizations examined 23%experienced a data or system breach due to vulnerabilities in the application layer. Security measures sometimes had the expected results and some other not. That varies from each company and the reasons vary. [WSec13]

SafeNet [SaNe13] presents security breaches as a new reality stating that cost for security increase but the effectiveness doesn't against the 'epidemic' data-breaches. According to the SafeNet's Breach Index in 2013 there were 1,056 incidents of data breaches where more than 575 million data records were lost. For 2014 without being yet passed, 760,044,022 million data records have been already lost or stolen. The sources of those incidents are according to the report the corporate security strategies and the unfortunate fact that it doesn't exist a way to fully protect a data breach from occurring. The means recognized as appropriate against a data breach are encryption, secure storage and management of keys and users access control. [SaNe13]

For New York State alone, according to the New York State Attorny General, Schneiderman, E. T. [Sch14], from 2006 up to 2013 breaches have exposed 22.8 million personal records and cost approximately $1.37 billion for businesses. During the year elapsed, the number of data breaches has tripled between 2006 and 2013. It is stated that as Big Data are more widely used and are affordable they possess a new threat for companies. During 2013 alone 900 data breaches in the New York State has exposed personal data of 7.3 million New Yorkers. Hacking is once more a primary source of breaches with 40.78%, followed by stolen or lost equipment (23.51%), inadvertent (20.24%) and insider wrongdoings (10.37%). [Sch14]

In Trustware's *Global Security Report* for 2013 [Trus13], the most targeted industries are retail (45%), food and beverages (24%), hospitality (9%), financial services (7%) and nonprofit organizations (3%). The assets more commonly targeted are E-commerce websites (48%), points of sale and payment processing (47%), data centers and corporate infrastructures (4%) and ATMs (1%). Mobile malware increased by 400% especially for Android, resulted by the increasing mobility of data. Third parties and outsourcing were in 63% of the incidents the way business respond to them and the average time for detection was 210 days. From the victims 64% detected the intrusion after 90 days whereas a 5% identified criminal activity after three or more years. [Trus13]

The 2013 (ISC)2 Global Information Security Workforce Study [Suby13] highlight important security threats and vulnerabilities such as application vulnerabilities (69%), malware (67%), mobile devices (66%), internal employees (56%), hackers (56%), cloud-based services (49%) and cyber terrorists (44%). Organizations want to protect from those attacks mainly their reputation (83%), breaches of laws and regulations (75%), service downtime (74%) and costumer and privacy violations (71%). Corporations consider as important for the security infrastructure the management support and security policies (89%), the security staff quality (88%), the adherence to the security policy (86%), training of staff related to the security policy (83%) and budget allocation to security (80%). [Suby13]

In the presentation of ISACA's North America for ISRM Conference 2014 [ISACA14], entitled 'Prevention of Data Breaches', was shown that targeted attacks have increased, with small organizations of 250 or less employees to be targeted in 39%. E-mail based targeted attacks used in 24.7% of the cases attachment of .exe file. Main targets of organized crime (origins Eastern Europe and North America) were financial institutions, retail businesses and food industry; state-affiliated attackers (from East Asia) were oriented to manufacturing businesses and transportation whereas activists (mainly from Western Europe and North America) were more concerned in attacking information and public companies and organizations. The attack actions, targets of the attacks and the data aiming for vary based on the profiling of threat actors as above. [ISACA14]

The Annual Security Report of Cisco for 2014 [Cisc14] it is found that 21% of the treats are buffer errors, followed by resource management errors, input validations, permission, privileges and access control, information leak/disclosure, cross-site scripting (XSS) and code injection. Companies that are most threatened from malware are agriculture and mining industries, as well as electronics manufacturing businesses. Cisco detects 50,000 network intrusions every day and stops 4.5 billion emails in the same time period. The number of new security alerts increase, opposed to updated alerts. In the mobile devices Androids are attack in 99% of the cases and their users have 71% encounter rate with all forms of web-delivered malware. [Cisc14]

In the *2014 Information Security Breaches Survey* of PwC and InfoSecurity Europe, for the United Kingdom [PWC14b], observed that security breaches have in average slightly decrease but the costs show a significant rise. It is also referred that 10% of the companies that were breached had to change the nature of the business due to the damage of the attacks. More precisely, security breaches occurred in 81% of the large organizations with an average of 16 breaches and 60% of the small businesses with an average of 6 breaches. The external attacks to large organizations were 73% viruses and malicious software, 55% unauthorized outsiders, 38% DoS and 24% network penetration. An important key observation made is that 70% of the businesses don’t reveal the worst security incidents that have faced those results to have a very partial picture of the real situation. [PWC14b]

Philip N. Howard for the CMDS [How14], examining data breaches in Europe from 2005-2014, found that 229 data breaches affect personal data of European citizens and 200 cases were confirmed is involving Europeans. In Europe-specific breaches 227 million records were lost. For every 100 people, 43 records were compromised and for every 100 internet users, 56 records have been compromised. Compromised corporations were offered 89% of the breached records. The records were compromised in 57% of the cases due to organizational errors and 41% due to clear actions of theft through hacking. In this study is also mention the fact that only were reporting incidents is mandatory by law data for compromised records were able to be collected and examined. [How14]

In the data breach report of 2014 conducted by the Identity Theft Resource Center [trc14] for 2014, had been identified 636 data breaches and the records exposed were 78,098,439. Generally the ITRC Report present individual information about the data exposed and statistics based on the type of the entities affected. In the medical/healthcare sector 42.1% of the breaches had occurred, followed by 34.9% incidents occurred in businesses, 11.6% in government and military agencies, 7.5% in educational centers and 3.8% in banking, financial and credit institutions. [trc14]

Cyber risks have been characterized as a growing threat from the study conducted by the Insurance Information Institute in 2014 [III14]. The number of data breaches within the year are estimated 614 affecting medical/healthcare organizations (43.8%), business (34.4%), governmental and military institutions (9.1%), educational institutions (9.0%) and banking, credit and financial sector (3.7%). The majority of records exposed (84.0%) are from businesses and they reach the 77.3 million records. DoS (21%), malicious code (21%) and web-based attacks (13%) have been found as the most costly cybercrimes for 2013 , account for more than 55% of the cyber costs for every U.S company annually. ‘High profile’ data breaches of 2013-2014 are also refereed as EBay, Target, Adobe, New York Times, Google, Facebook, LinkedIn, twitter, Yahoo and ADP. [III14]

Verizon’s investigation report for data breaches in 2014 [Ver14] examined 95 countries identified 63,437 security incidents and 1,367 data breaches were confirmed. The number of security incidents resulting to data losses by industry put the financial industry with 465 incidents in the first place followed by public sector (175), retail businesses (148), accommodation (137) and utilities (80). The majority of the attacks come from external parties followed by internal offenders and the major motives for attackers are financial, espionage and ideology/fun. The most popular type of attacks are: hacking, malware, social, physical attacks, misuse and errors. [Ver14]

In the white paper of EMC^2 and RSA Research about cybercrime [EMC^{2}13] new trends were identified. First rang the increasing sophistication of mobile attacks. Characteristically is refereed in 2013 1.4 million Android apps were malicious and of high-risk. Fraudsters have also developed SMS sniffers designed to work along with Trojans. The popularity and anonymity of Bitcoin are associated with its popularity as it has similarities with cash. The protocol of Bitcoin and online exchange activities have been attacked, where at the same time forum-specific currencies and the invention of new virtual currencies increase. Attacks and especially malware increase in sophistication, hit-and-run POS malware attacks become common and APTs continue to occur with new players and similar tactics. The uses of more passwords for different devices with increase mobility make credentials weaker and easier to be stolen and transform user authentication to a formidable weakness. [EMC^{2}13]

The data breach report for California from the Californian Department of Justice [Kam14] identifies 167 reported breaches in 2014 that endanger mainly payment card data and health information. The 18.5 million data breached in 2013 were 600% more compare to 2.5 million records breached in 2012, without the Target and LivingSocial incidents the increase would have been 35% meaning 3.5 million records. Malware and hacking are the main causes (53%) of the data breaches, followed by physical losses or stolen devices (26%), unintentional errors (18%) and intentional misuse by insiders (4%). The industries reporting the most breaches were with 26% the retail sector, 20% the finance and insurance industry and 15% healthcare institutions. [Kam14]

PwC’s survey for US cybercrime [PWC14a] states that the US Director of National Intelligence has categorized cybercrime as the top national threat. The results from past experience seem to be that corporations cybersecurity, in most of the cases, is not at an acceptable level compared to attacks that grow in precision, tactic and effectiveness. According to the Global State of Information Security Survey, 82% of businesses that perform high security practices choose to collaborate with others to gain a more thorough knowledge about trends of security and threats. The numbers of the breaches identified seem to increase and for each industry sector deferent incidents are mostly detected. As cybersecurity involves cost strategic approaches to the issue are increasing and 38% of the businesses already prioritize cybersecurity investments based on risk assessment. NIST Cybersecurity Framework is also suggested for organizations to advance their security potentials as it is flexible and fit for various industries. [PWC14a]

MANDIANT’s threat report for 2014 [Mand14] recognizes security breaches as inevitable, as cyber threats have a broader scope and evolve in skills and tools. Companies and other cyber victims are more willing to share data about the attacks. The targets have grown and attacks have pervasive and influential results more than before, showing more than ever how the digital world overlap and affects the reality. Financial companies are attacked frequently with 15%, followed by Media and Entertainment (13%), Manufacturing (10%) and Aerospace and Defense (6%). The majority of compromises 67% are detected from external entities and the victims discover 33% of them. One of the main concerns are that attacks are detected after approximately 229 days, whereas in mean time attackers achieve their goals. [Mand14]

Studies indicate that information security trends should not be seen through reports as the above. The main argument is that the data presented are anecdotal, not generalizable and are reported cumulatively [RyJe03]. The non-reliable character of those data is concerned and ii is not attempted to masquerade them as reliable. They are used here for the purpose to provide evidence of threats and incidents caused by the violation of security. It is not claimed that those data should be used for decisions neither to make general conclusions. Their reliability should not be taken from the reader as high and reliable for decision making. At the same time, given the resources and time and without presenting trends, the main point of the existence of security violation can be made. [RyJe03]

More accurately, from the above reports can be conducted that security is violated in many cases. The trends change as time passes, but security seems to be the follower and not the leader in the cyberwar. But the consequences may leave not place for second place. If the security should advance to the next stage is a matter of importance. For corporations that can be only interpreted in monetary terms. As security doesn’t give earnings to enterprises except from some fields such as insurance and security companies, can be better interpreted in terms of cost. In the next chapter it is examined the hypothesis that security is important for corporations, analyzing funds lost and also records that have been breached. In order to be more accurate in some cases the costs for a company are compared with their equity. More details are showed in the following section.

5.3 Data Breaches Worldwide

Based on worldwide data provided by the datalossdb.org from 2010 up to 2014, 10,668 incidents involving the loss of personally identified information were reported. These cases involve a much greater number of lost records and organizations, institutions and companies. During the course of those five years a great rise is indicated, until the year 2012. In 2013 a decline in number of incidents reported can be identified but in 2014 the punctuations remain, but the tops are of relevant high and above the scoring of 2013 average. More accurately Table 4 shows the numbers that resulted from the above defined sample.

Table 4: Number of Data Breaches 2010-2014

Year	Number of Data Breaches (reported in datalossdb.org)
2010	953
2011	1241
2012	3219
2013	2343
2014	2912

Still those results should not be generalized or taken for granted. They come from a particular source which collects data breach notification letters scented to various jurisdictions in the United States. Consequently the sample is not equilibrated among the various countries not even states, weights are not assigned to the results and where by low report of data breaches is obligatory the regional results will end up to be biased against the more transparent. Furthermore, the Data Loss Database doesn't include every breach. A set of criteria is used and the resulted lists contain breaches involving the release of personal information, preferably related with an organization.

What can be observed from a more wide perspective and proprietary sources is that multinational companies may reveal the existence of a breach, but won't provide any quantification, or the records lost will be reported but the company or parties involved remain unknown to the public eye. That shows that indeed data about the past are collected, lessons can be learned, but its study and report is sensitive and should not be taken outside the context of each study. Also, the picture of the past is nothing more than what the name indicates, past and it is a picture and not reality. To mach information is hidden, maybe from the majority, but not lost.

Competition, laws, technological expertise make companies more or less aware about their own breaches, and it's one of the players choose according to their best interest how to announce or not their losses from mistakes or attacks. The situation should not be over- or underestimated. In order to access the impact of data breaches from the above described sample, data for the time period of 1st of January, 2010 up to 31st of December, 2014 were collected in a monthly base.

From a first examination 10,668 data breaches were identified. During the course of time the period 2012 was the most intensive. The illustration of the data is presented in the Figure 7 Compared to 2010 it can be easily seen that the breaches have increased in 2014, whereas in 2013 the average number of breaches is lower than that of 2014.

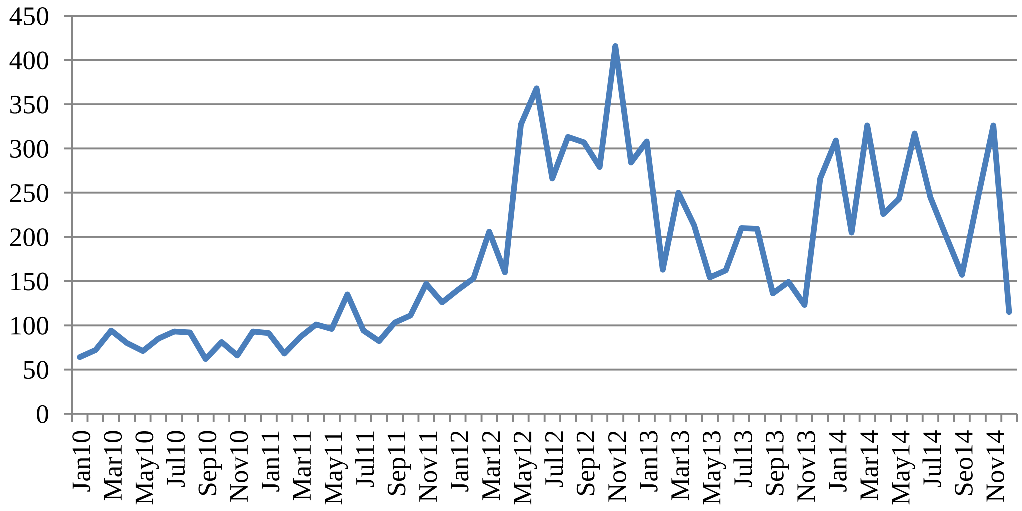

Figure 7: Number of Data Breaches per month 2010-2014

The goal of the analysis of those data breaches is to show that data breaches occur worldwide. As the sample examined contains sensitive and personal data, for instance social security numbers and financial information, by law security measures are in place. The breaches are reported mainly due to law obligation. At the same time, companies also report the records stolen or lost. As it will be explained in more detail in the next Chapter 6 about cost, the number of records lost is an indication for the impact to an organization. From the data collected the Figure 8 depicts how during time the number of records lost from organizations punctuates.

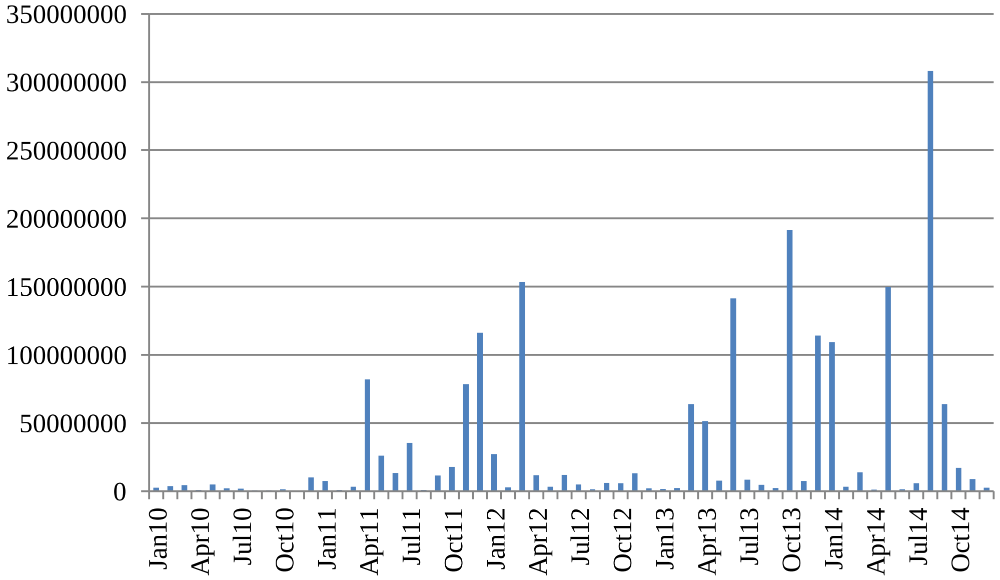

Figure 8: Records Lost from Data Breaches 2010-2014

The records lost per month are approximately between 100,000 and 300,000,000. From the above diagram it can be easily observed that there are punctuations among the months and years. The months with greater losses in terms of records are December of 2011, March of 2012, June, October, December of 2013 and January, May, August of 2014. As for the years 2012, 2013 and 2014, show that as the time elapse either the number of records lost is increasing or/and that more companies assess and report what they have lost. The Figure 9 bellow illustrates, in an unavoidable complicated way, in which month and year more losses of records have been found and reported.

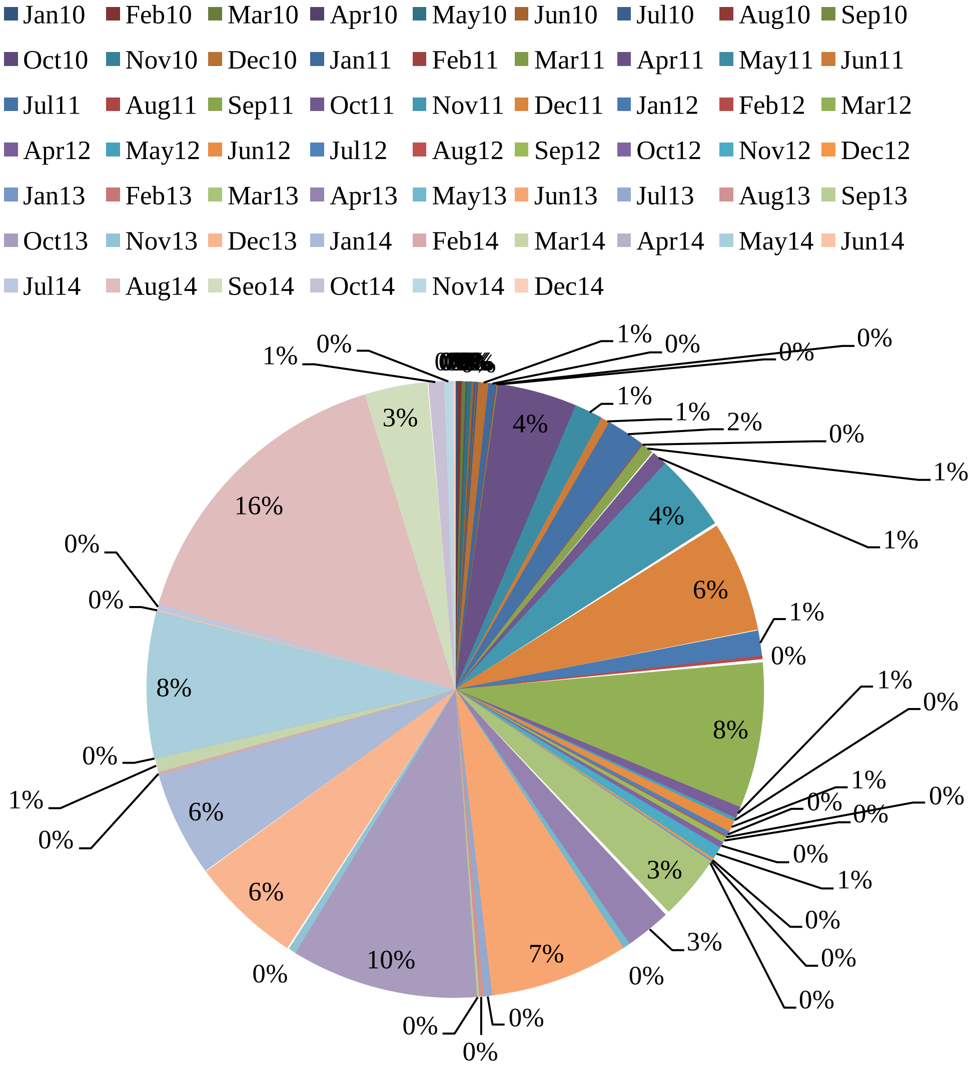

Figure 9: Number of Records Lost per month 2010-2014

The question that may arise from the above diagram is: what the cause of those increases is. In 2010 the data breaches have caused a relatively small amount of important records lost, but in 2012 The Sony incident led to the loss of 77,000,000 records alone. At the same year from an outsider attack Nexon lost as well 63,000,000 records. In 2012 the overall number of records lost has increased, but an incident alone didn’t affect the overall results as in the previous year. In 2013 a series of important data breaches have occurred. From outsiders attack Adobe lost 152,000,000 records and Target 110,000,000 records. Also, the Pony bot had from Google, Facebook, LinkedIn, Twitter and Yahoo 2,000,000 records under control. In the year 2014 the EBay data breach resulted in the loss of 145,000,000 records and the JPMorgan incident to the 83,000,000 records breached.

The Figure 10 and the Appendix A show in more detail the number of data breaches that occurred and reported between 2010 and 2014. In addition, the incidents where the numbers of records lost were reported are correlated. The reason of this comparison is to estimate how accurate and reliable the above presented data are. It will be seen clearly that there are various limits to this type of analysis, because the proprietary data are limited. Consequently it can be said that the real number of records lost per year is much greater than the one presented. The reasons are mainly that companies don't report what they have lost and also the difficulty to realize and calculate what information has been exposed, after an attack or a mistake.

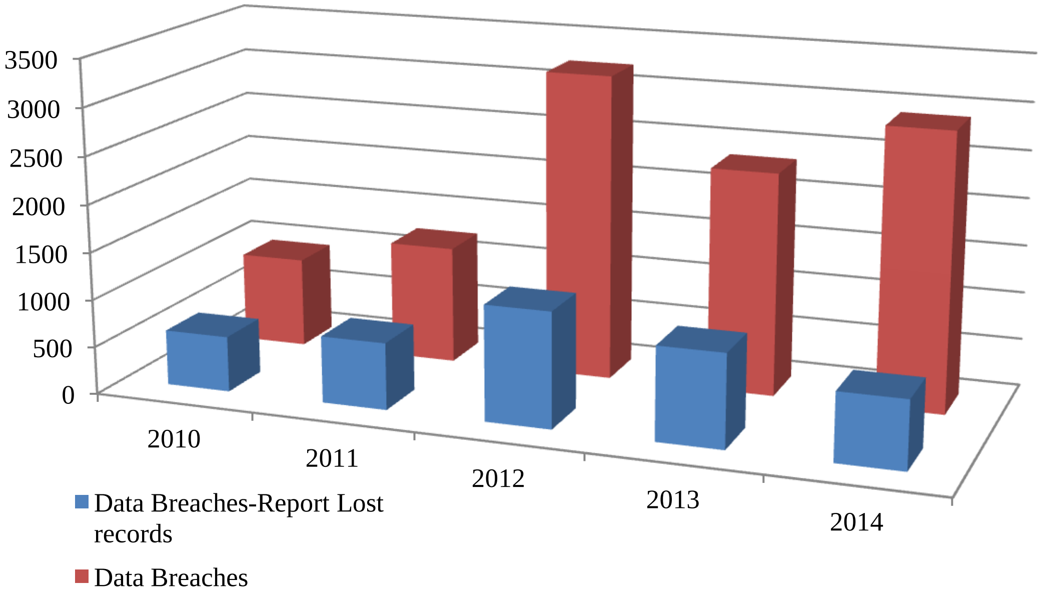

Figure 10: Comparison of Data Breaches Reports and Number of Records Lost Reports 2010-2014

From the above examination can be seen that the data breaches is a worldwide phenomenon, which takes place during the years. As the time passes, not only the number of data breaches increases, but also the number of records lost. The records examined are important, because of their content, and they are included in this study because the latter will be shown as a basic measure of the cost that follows a data breach and has various consequences for the corporations involved. Not only the low takes the number of records as a measure for the potential penalty, but also the possibility for individuals to be affected and civil charges to be placed against an organization is increasing.

5.4 Privacy Breaches in United States

In this subsection statistic data that have been extracted from the Privacy Rights Clearinghouse (https://www.privacyrights.org/) are collected, presented, processed and analyzed. The emphasis is given in cases where personal data are lost as a result of a corporate information breach. The results are astonishing considering the narrow area of interest. They are used because they address the importance of the security failure and what can cause data breaches to occur.

According to the laws of California and more specifically the Civil Code section 1798.80-1798.84, even a small let alone a big company has to establish the means that will ensure the safety of the data of their clients. This obligation by law is taken as the indication that the examined companies all have imposed security measures. Still they fail to properly protect the data of their customers and the results are multiple and for both companies and customers.

Because not only incidents from the state of California are reported, but from the United States, is important to include information about the legislation for other states. "*Some states have state laws that require breaches to be reported to a centralized data base. These states include Maine, Maryland, New York, New Hampshire, North Carolina, Vermont and Virginia (Virginia's notification law only applies to electronic breaches affecting more than 1,000 residents). However, a number of other states have some level of notification that has been made publicly available, primarily through Freedom of Information requests. These states include California, Colorado, Florida, Illinois, Massachusetts, Michigan, Nebraska, Hawaii and Wisconsin".* This analysis can be found in more detail in the following webpage http://datalossdb.org/primary_sources.

From the above is clear that companies in United States not only have to secure the data of their customers but also to report and share information about breaches that may occur. Even though, as it will be seen many types of disclosures and hacks are taking place for at list ten years. At the same time structured information is collected for the attacks.

In the following analysis data breaches in the United States are examined from 2005 up to 2014. They include data breaches, mainly but not exclusively of compromised personal information, reported in the United States and not only to the state of California. They offer a total number of records compromised, which is an approximation of the records but as such they are fewer than the reality. The list of incidents is representative and the goal is not to include everything. Still is a useful indication of the categorization of breaches and their intensity and variations during the years.

More precisely, the incidents examined had impact on more than nine individuals, or in case they are fewer if there is a need for public concern. Main source is the Open Security Foundation (www.datalossdb.org) which is in turn derived from verifiable media stories, government web sites/pages, or blog posts with information pertinent to the breach in question. Also for data from January 2010 sources include also the Databreaches.net (www.databreaches.net and www.PogoWasRight.org), Personal Health Information Privacy, so called PHI Privacy, more accurately the web pages www.phiprivacy.net/ and http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html and National Association for Information Destruction, Inc (NAID) (www.naidonline.org). From March 2012 the California Attorney General list of data breaches is also used as a source. It is important to make clear that if a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely that the breach will be reported anywhere.

The update of the data takes place every two days and it was last checked for changes in 24th of December 2014. Abbreviations are used in the initial presentation of data and have been adopted in the statistical analysis because they offer an efficient categorization of the data and make the analysis more understandable. The following tables Table 5 and Table 6, contain the analysis and details given from the Privacy Rights Clearinghouse, given in each dataset.

Table 5: Type of Breaches

Abbreviation	Type of breach	Description
DISC	Unintended disclosure	Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
HACK	Hacking or malware	Electronic entry by an outside party, malware and spyware.
CARD	Payment Card Fraud	Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
INSD	Insider	Someone with legitimate access intentionally breaches information - such as an employee or contractor.
PHYS	Physical loss	Lost, discarded or stolen non-electronic records, such as paper documents
PORT	Portable device	Lost, discarded or stolen laptop, PDA, Smartphone, portable memory device, CD, hard drive, data tape, etc
STAT	Stationary device	Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
UNKN	Unknown or other	Not included in the above categories.

Table 6: Organization Types

Abbreviation	Organization Type
BSO	Businesses-Other
BSF	Businesses-Financial and Insurance Services
BSR	Businesses-Retail/Merchant
EDU	Educational Institutions
GOV	Government and Military
MED	Healthcare-Medical Providers
NGO	Nonprofit Organizations

In any case, the data that are going to be analyzed and presented should not be taken as reliable. They are used here for the solid purpose to depict what has been reported from a particular source and a certain time. Generalizations should not be made upon those data. Data distributions, variants and averages don't provide a good statistical quality, still for the purpose to indicate a situation where security is violated and data are collected in the course of time the above analysis for the context of this paper is useful.

The incidents of data breaches that are examined can be sum up in the following diagram, Figure 11. It depicts the distribution of the various types of breaches among 4,467 incidents. Cyber-attacks from outside parties, malware and spyware, seem to be the main source of breaches with a small precedence to the loss of portable devices. Mishandled sensitive information posted publicly or is send to a wrong mail; fax; email etc. seem to be another of the main sources of data disclosure. It is also common legitimate users to intentionally breach information.

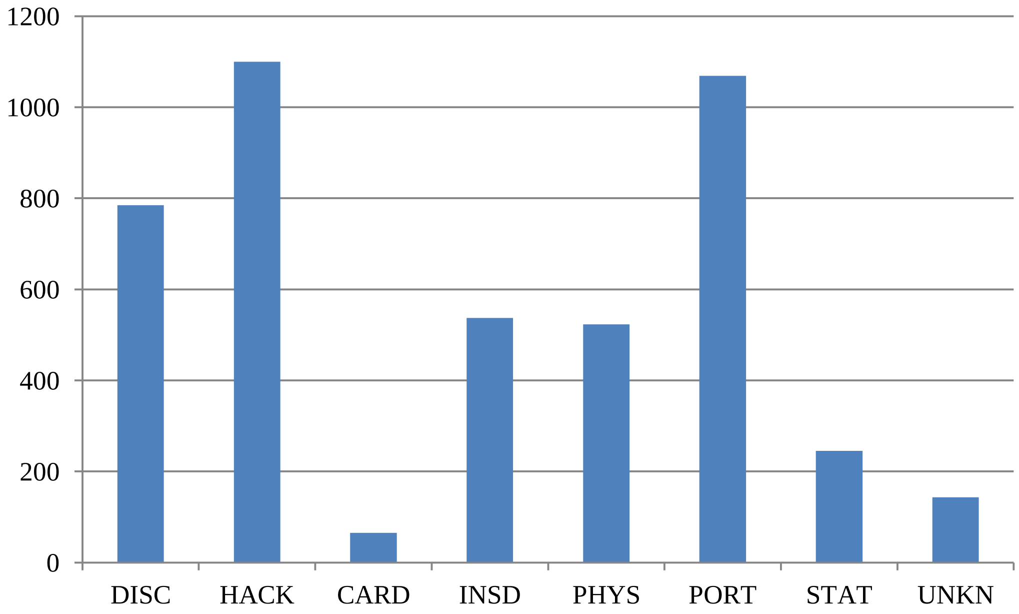

Figure 11: Number of Data Breaches Reported 2005-2014

As it has been already mentioned, these data are limited only to the Privacy Rights Clearinghouse database and show trends that may be applicable only for the United States. Also, it should not be neglected that those data have been processed and they depict selective cases. Nevertheless, they are available to the public for purposes of awareness and to alert for changes in trends. In that context, they can be examined further. The results examined are not claimed as international but useful to prove that data preaches occur at least throughout the United States and that the problem for this geographic area exists.

A prioritization of types of breaches has been attempted with the above analysis. Every one of the examined types punctuates in the course of time. Cyber-attacks weren’t always the preferable way to steal data, before those stolen portable devices were preferable. Lower but study seem to be the unintended exposure of information mainly from mismanagement and mistakes. The insider’s threat from 2009 grows. The Figure 12 illustrates those changes in trends.

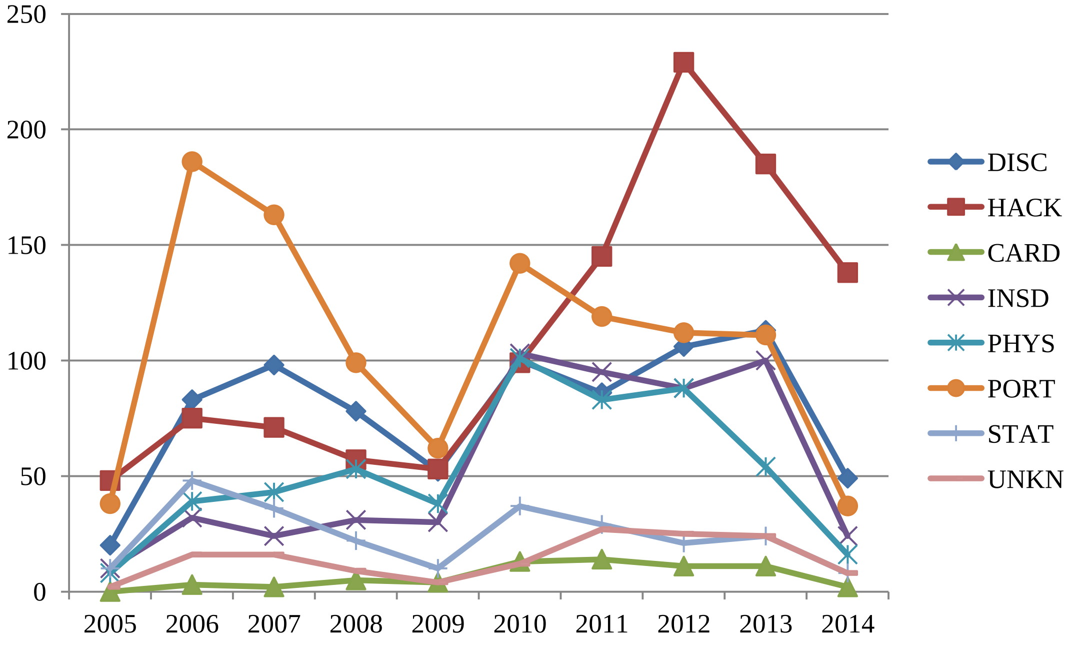

Figure 12: Trends in Data Breaches Types 2005-2014

What cannot be neglected from the above diagram is that all of the types of breaches seem to diminish drastically in 2014. Even if the remaining time of the 2014 is considered as the case, meaning that the shamble when collected wasn’t complete for the last month of the year, still is clear that from 2012 companies, state agencies or both are more active and the security becomes more effective. Other explanations can be that attackers are eliminated or that corporations have less important and sensitive data. From the above closer to reality it may be that the knowledge of the past failures leads to more to the point defense and the results are obvious.

An interesting observation is that different types of organizations are attacked differently as well. General businesses are exposed with different intensity to the same attacks that a financial and insurance institutions are. The same is true among retail companies, educational services, governments, medical providers and nonprofit organizations. The pie charts show these differences in Figure 13 to Figure 19.

The first of the pie charts indicates that businesses generally tend to be attacked from outside, in the cyberspace in order information to be retrieved. Portable devices are also stolen with the same goal. Mistakes also unintentionally disclose information to the public or to third parties. Employees or contractors and other types of legitimate users are also a source that causes breaches intentionally. Lost documents, discarded or stolen non-electronic records still are a source of breaches. Fraud involving debit and credit cards, stationary electronic devices and any other type of exposure of data seems to be less possible but still occurring.

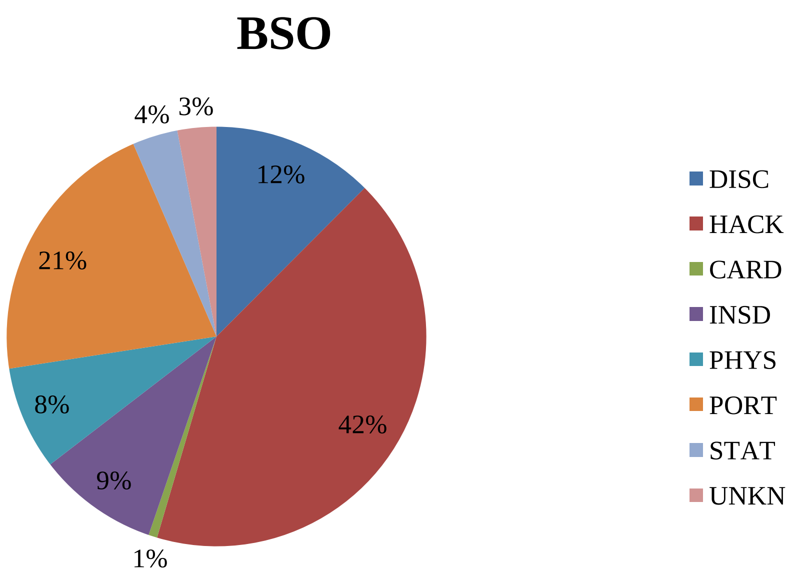

Figure 13: Businesses and Breaches Types 2005-2014

In the financial and insurance industry the main threats are stollen portable devices, cyber attacks, mishandling of sencitive information and unintentional publication. The incider threat is greater and the lost, discarded orstollen data are exposing valuable data of those organizations. Card fraud and stationary electronic devices also are more intencively attacked. The reasons can be that financial institutions are oblaged to apply security which leads attackers in more inovative and less exploited areas. The attacks are of more categories and sometimes combined. This is also indicated from the unknown category, which is also of interest here.

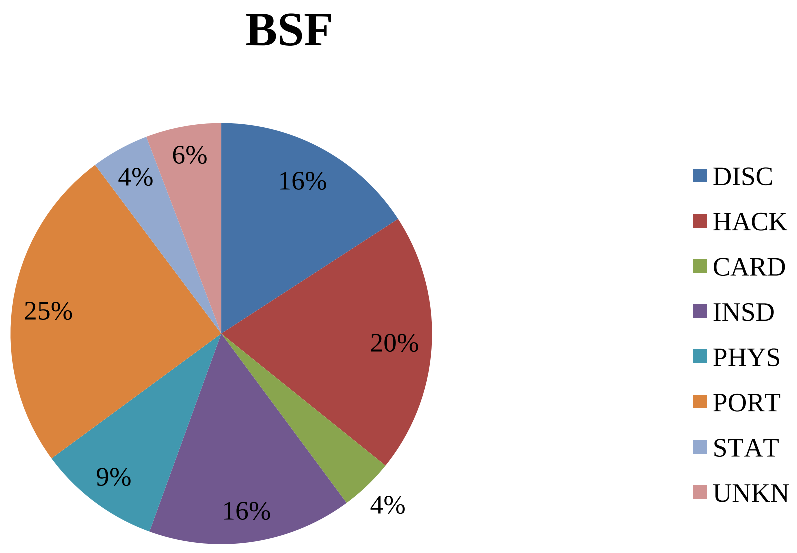

Figure 14: Financila and Insurance Services and Breaches Types 2005-2014

The majority of attacks in retail-merchant businesses seem to come from cyber-attacks and legitimate users reviling intentionally data. Stolen-lost portable devices are also the trend in this category. Documents and card fraud are occurring as well and cannot be neglected. In the businesses so far the patern seem to be unintented disclosure of sensitive data, cyber attacks, portable devices and inciders threats.

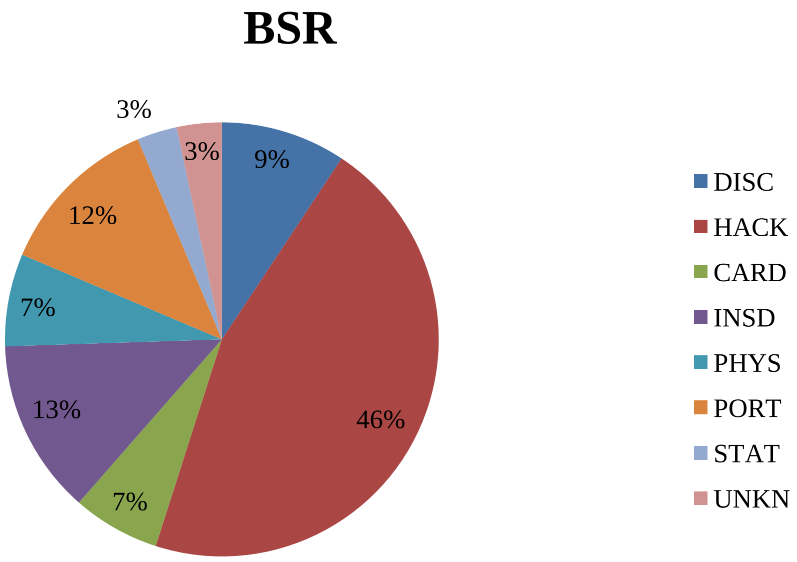

Figure 15: Retail/Merchant Businesses and Breaches Types 2005-2014

In educational institutions hacking–malware attacks and unintended publicity or mismanagement of sensitive information are the main types of data breaches occurring. Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc are also an important percentage of the causes of breach. Non-electronic records and stationary electronic devices such as computers and servers not designed for mobility seem also to be the target of attacks. The rarest type of breach to occur in this field is the intentional breach from an insider. This contrast with the cases presented for the other types of businesses, where it was one of the most possible sources of disclosure.

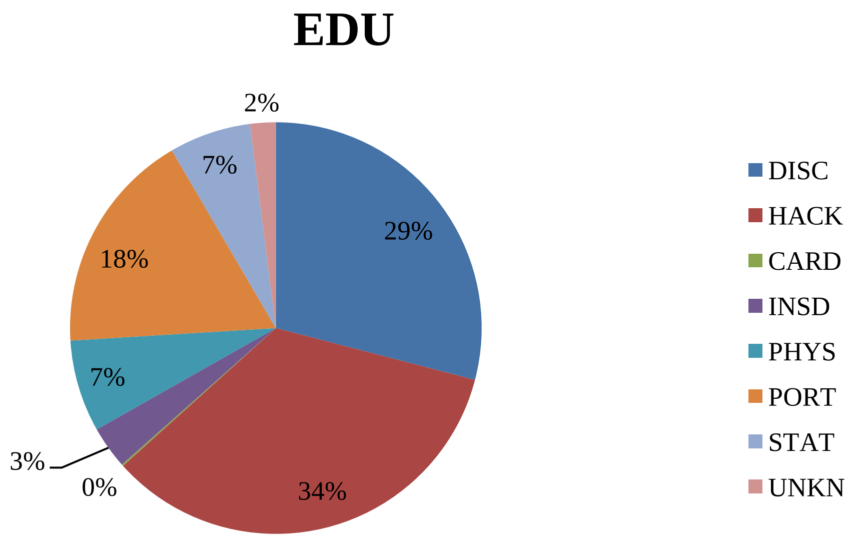

Figure 16: Educational Institutions and Breaches Types 2005-2014

Governments and military are disclosing information unintentionally on websites, or mishandle and sent to the wrong party sensitive data. Portable devices are also the Achilles heel as lost, discarded or stolen devices seem to be common scenario, especially as they decrease in size. Documents and non-electronic data along with willing insiders to reveal information that are not supposed to are occurring as well. Commonly with all the above cases rarely stationary devices are lost or stolen and result to breaches.

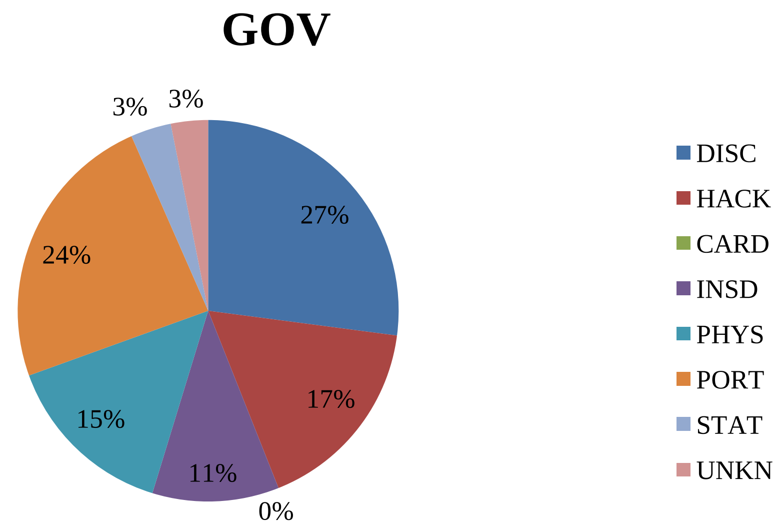

Figure 17: Government/Military and Breaches Types 2005-2014

In helthcare the majority of the reported data breaches are related to portable devices that have been lost, not efficiently discarded or stolen. Data in non-electronic form are also another common cause of breach. People with legitimate access intentionally breach information is a common occurance and in the medical sector. Unintentional disclosure by mistakes and stolen or lost stationary devices are more rare but still important, especially considering the criticality the data have themselves and the maltiple ways that can be used for targeted individual attacks, experiments, transplants etc. Surprisingly, hacking and malware in this sector are used in few cases or they are not found.

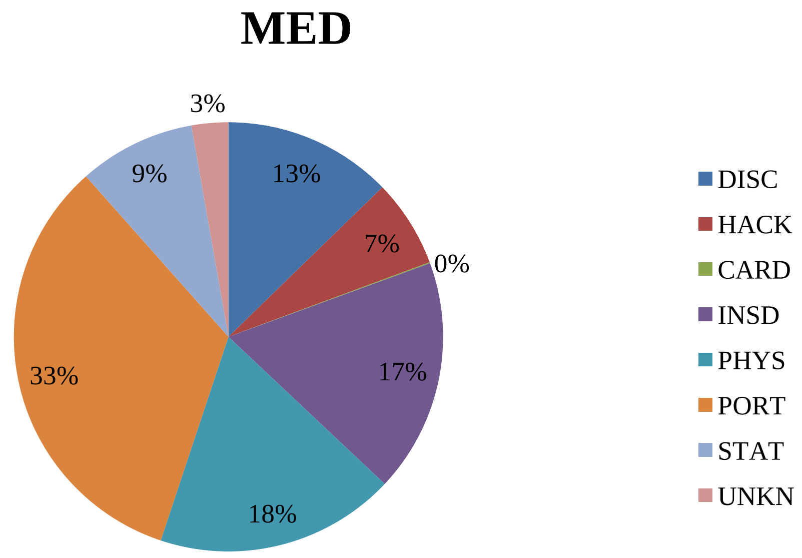

Figure 18: Healthcare/Medical Providers and Breaches Types 2005-2014

Nonprofit organizations are common targets of cyber attacks. Except from hacks and malware they are almost equaly targeted in the physical dymension in terms of portable devices. Paper documents and willing employes or any type of insider are common also in those organizations. Unintended disclosure of sensitive information and sented to wrong parties information are in some cases the source of breach. Payment card fraud not accompliced via hacking is more rare bur still present.

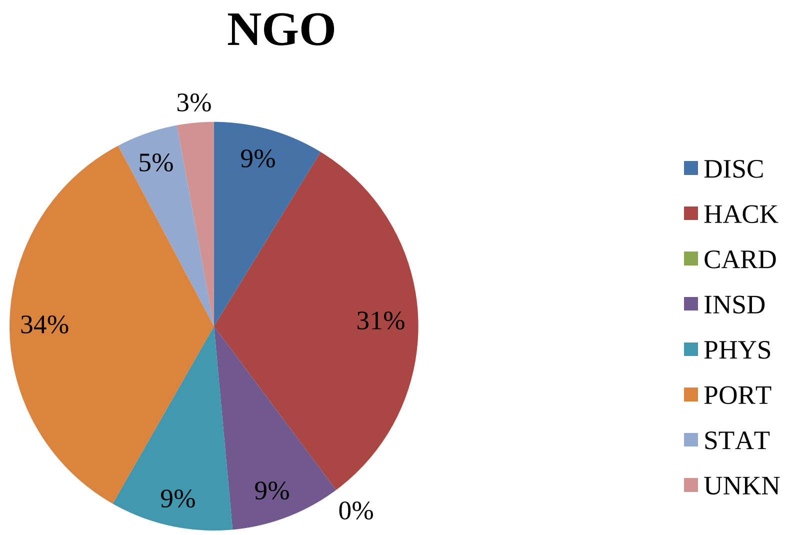

Figure 19: Nonprofit Organizations and Breaches Types 2005-2014

Simply correlating the above data, hacking seem to be the most common threat especially for educational institutions, retail/merchant businesses, governments and generally for companies. Organizations also were exposed to the loss of portable devices, which for medical and healthcare institutions seem to be the most commonly reported type of breach. Financial and insurance institutions even though they face the insiders threat might be the very well prepared, as the following visualization Figure 20 shows, the incidents occurred are the least compared to the rest in percentage.

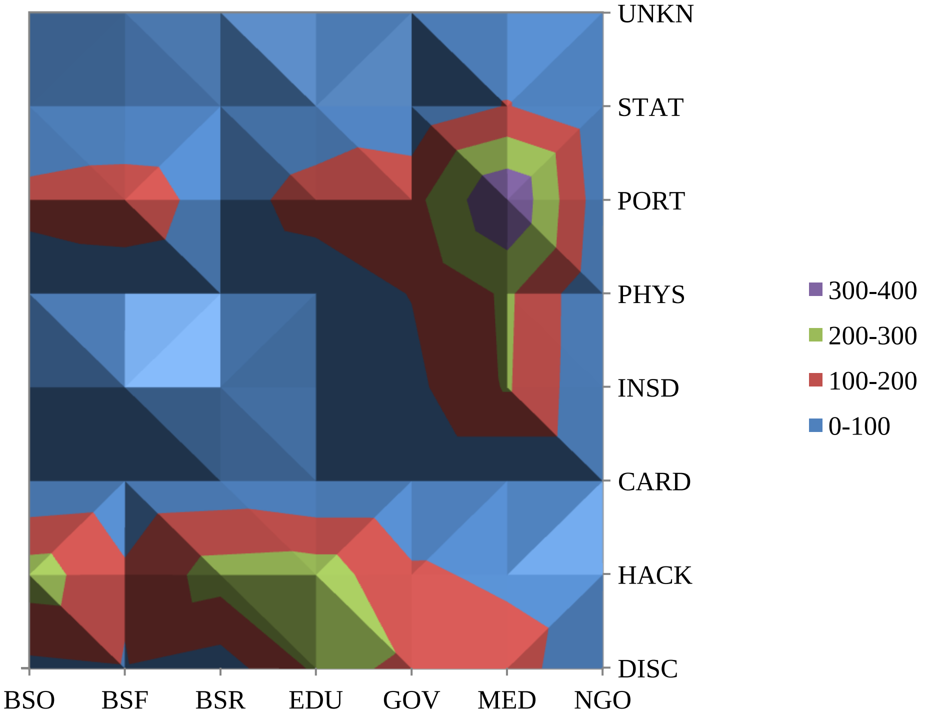

Figure 20: Organizations and Breaches Types 2005-2014

It is important to mention that each sector has a different intensity of breaches. The Figure 21 illustrates that fact. More precisely shows that the medical sector is the one more attacked from 2005 to 2014 and nonprofit organizations are in the other end. Those results though are not wide and don't claim that can be generalized. But it shows that nevertheless data breaches occur in various fields that have security in place.

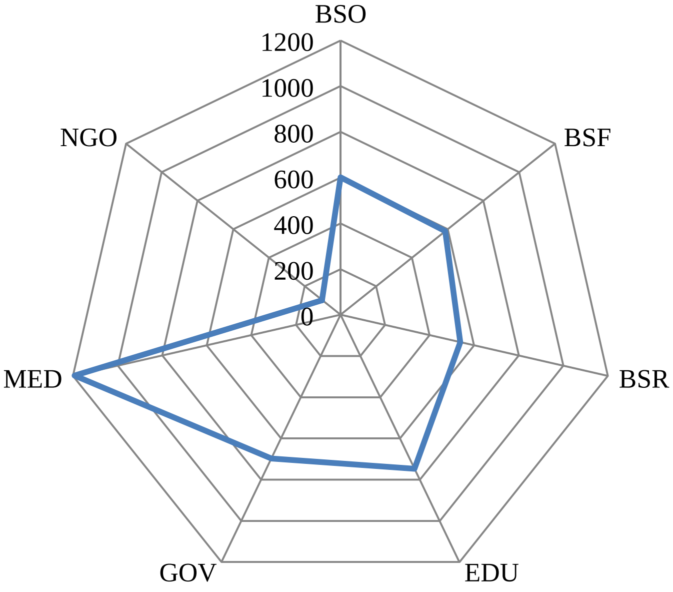

Figure 21: Data Breaches per Sector 2005-2014

From the above subsections what can be derived is that data losses occur, at least in United States and are existent. In the businesses and the market security measures against attacks, polices, best practices, laws, certifications and any other type of control are in place. Even though, breaches occur and where solutions seem to be found new attacks or evolved already existent attacks surpass the old measures. Those are more the case of the past. The next subsection will briefly analyze some important and more worldwide cases and will conclude with studies from trusted organizations and institutions in order to prove that security fails.

6 Cost of Data Breaches

Security is violated and that implies that there is place for improvement. Before such a perspective is examined, it should be presented how important are those breaches for corporations. As businesses prefer monetary terms and the major concern here are data breaches, their costs for enterprises, seen to be the most rational and accurate measure. The events analyzed are correlated with the announcements of data breaches. The term 'data breach' here corresponds, based to the Wikipedia definition, to the intentional or unintentional release of information that was secured in an untrusted environment [Wiki14]. In this chapter is attempted the examination of the impact of information security breaches on the firm value. The sources of the incidents and their impact derive from publicly announced sources. The incidents analyzed are from 2006 up to 2014 and the event study methodology is used for the quantification of the impact.

Before the estimation of the cost of data breaches, based on proprietary information from the web page privacyrights.org, a review of studies about the estimation of the data breaches cost will be presented. After a better understanding of the methodologies applied and the results they have given, the methodology and results of our experiment will be presented. The platform used is related to the United States and provide information about the releases of the breaches and the number of records lost. Based on well-known and recognized data from the Ponemon institute, again related to the cost per record lost for US, estimation about the cost during the last nine years, related to data breaches, is made. The previously presented results from the review of other studies, as well as the results of the approach in this research are limited in truthfulness as they are based on samples and assumptions. Generalizations are better to be avoided.

6.1 Related Work

In the information security literature the impact of cyber-attacks to corporate value has analyzed from to perspectives. The corporate estimations that require internal data and analyze quantitatively with even automated methods factors such as, lost sales, business expenses, lawsuits, incident investigation costs, etc. (http://www.databreachcalculator.com/, http://www.ibmcostofdatabreach.com/) and the academic perspective where event analysis, borrowed from the financial sector and adjusted to the cyber reality, is widely applied and accepted.

Calculators are offered for business purposes such as the CyberTab (https://cybertab.boozallen.com/) for the estimation of the cost of a specific cyber-attack, the Symantec and Ponemon data breach calculators (https://databreachcalculator.com/GetStarted.aspx) that provide the risk of a data breach, the average cost per record and per breach. Furthermore, makes comparisons within the same industry or other and with similar or different characteristics. The HUB International (http://www.hubinternational.com/data-breach-cost-calculator/) also offers a calculator for the estimation of incident investigation, crisis management and regulatory costs. In this study the emphasis though will be given to the academic approach.

From an academic perspective the methods introduced from Loderer and Mauer (1992) [LoMa92] have led to the event study of Dos Santos et al. (1993)[DosS93], where the applications of these methods have been used in the field of information technology. Many studies followed with similarities and differences. Ettredge and Richardson (2002) [EtRi02] investigated the market reaction to security breaches. They were focused to DoS attacks, launched from hackers on Internet firms. The sample examined was for February 2000 and they found significant negative abnormal returns to be the way markets behave after a data breach incident.

In 2003 Hovav and D’Arcy (2003) [HoD’A03] examined also the impact of DoS attacks to firms. There work was based on Ettredge and Richardson (2002) [EtRi02] as well as Campbell et al. (2003) [CaGo03]. A sample consisting of 23 incidents was analyzed and the findings indicated insignificant negative results for all the sample and significant results only for Internet firms, highlighting that where the markets expect technological expertise, when a data breach occur, the consequences are of importance. In the same year Garg et al. (2003) [Garg03] also examined 22 events between 1999 and 2002. Among the results, it was found that the average loss in share price the day of an event’s occurrence was nearly 5.6 per cent over a three-day period after the news of the event. The authors recognize that the results may be biased due to the fact that Microsoft makes multiple appearances in the sample. Furthermore, the results are claimed as not applicable for non-public and non-Internet dependent companies. The average loss of a company was estimated in $17-28 million, but maybe the most crucial result was that differences in the market reaction were found based on the various types of IT security breaches that were examined separately. [Garg03]

Hovav and D’Arcy (2004) [HoD’A04] examined as well a sample of 186 incidents, but only including cases related to virus attacks. The mean abnormal returns calculated were positive, a result that indicated that virus attacks may require a different approach in order the impact to be calculated as they have a more pervasive impact which wasn’t depicted in those findings. Cavusoglu et al. (2004) [CaMiRa04], examining 66 incidents from 1996 to2001, take into account that the time period analyzed was of high market valuation and volatility, resulting in possible increase of errors. Among the results, a significant negative abnormal return for the whole sample of events was found.

While previous research have involved the use of regression analysis to explore the relationship between firm and attack characteristics and the occurrence of the cumulative abnormal returns (CAR), in the paper of Andoh-Baidoo, F.K. and Osei-Bryson, K-M. (2007) decision tree (DT) induction was used instead, to examine this relationship [A-B&O-B07]. The results of the DT-based analysis indicated that both attack and firm characteristics determine CAR. In this paper, DT induction, a data mining technique, was used for the development of a model that predicts the likelihood that an information security breach would lead to negative cumulative abnormal stock market return of the breached firm. Also, new factors that predict abnormal (negative) stock market returns of breached firms were identified. [A-B&O-B07]

Goel, S. and Shawky, H.A. (2009) [GoSh09] applied event study for a sample of 168 incidents from 2004 up to 2008. They found that security breaches can have a significant impact on the financial performance of firms. Also, the disclosure of private information of clients can damage firm reputation and lead to governmental sanctions, negative effect on the firm returns on the day of the event and a highly significant negative impact occurring on the day following the incident. On average the announcement of a security breach was estimated to have an impact of about 1% of the market value on the firm. Davis, G., Garcia, A. and Zhang, W. (2009) [DaGaZh09] analyzed the potential effects of cyber security incidents on companies that predominantly conduct their businesses in an online fashion. Using the time series associated with web traffic for a representative set of online businesses that have suffered widely reported cyber security incidents, they searched for structural changes resulting from these cyber security incidents. They found that cyber security incidents do not affect the structure of web traffic for the sample of online businesses studied. [DaGaZh09]

Patel, N. (2010) [Pat10] as well, examined the impact of security breaches, in this case, the direct and indirect costs associated with a firm's negatively affected stock. In this study 34 incidents were included in the sample referring to a period between 2001 and 2009. The study found that direct and long-term costs are not consistently significant. On the other hand, Gatzlaff and McCullough (2010) [GaMc10] concluded to the identification of significant negative abnormal returns for their overall sample. Also, e-commerce firms was found that suffer more from security breaches and DoS attacks, compared to other security breaches, cause the most harm to the majority of the companies. Though, the more recent the event the least impact for the firm was identified.

Yayla and Hu (2011) [YaHu11] examined 123 incidents from 1994 to 2006. Similarly for approximately the same period Gordon et al. (2011) [GoLoZh11] investigated 121 events, using the Fama-French three-factor model along with the CAPM in order to estimate the abnormal returns. Humayum, Z., Myung, S.K. and Kweku-Muata, O-B. (2012) [HuMyK-M12] searching in the same direction, found that a security breach announcement of a breached firm has a ripple effect to the industry as a whole. In their study weren't evident the competition effects with a statistical significance. Still, the lack of incentives for companies to publish data breaches was recognized in cases where the low doesn't force it. Also, in some cases, the performance of the firm after the breach was better.

More recently, Pirounias, S., Mermigas, D. and Patsakis, C. (2014) [PiMePa14] investigated 105 events, from 2008 to 2012, applying once more event study methodology with Capital-Asset-Pricing-Model (CAPM) and Fama-French three-factor model, to investigate the impact of security breach announcements on firm value. It was considered that the period examined was of high volatility. Among the findings are that on average technological firms suffer higher total costs of a security breach compared to the sample, investors are less sensitive to react. A very large-scale incident was recognized with the possibility to severely impact a firm, independent from the sector. [PiMePa14]

Layton, R., and Watters, P.A. (2014) [LaWa14] investigated 2 entities, more specifically, Telstra and Linkedin. They found that data breaches negligible impact on company reputation as reflected in the stock price. The stock price, after the attack, rose in both cases. The direct costs were significant and estimated potentially to thousand dollars. In addition, policy and procedures were recognized to have a large effect on the overall cost. The absence of standardized cost calculation methods was recognized from Clemens, M., Amina, K. and Ghada A-S. (2014) [ClAmGh14] that they undertook the task of quantifying the internal costs of security breaches as well as the costs of managing them. More precisely, they developed a method which assumes that alternative tasks that do not rely on the affected IT resource are performed, hence, the employees' time is not considered as completely idle and consequently the total costs decrease.

What is in common in most of the previous work is the use of event study as a methodology to estimate the impact of data breaches in terms of stock value. The size of the sample varies depending on the context and the initial hypothesis examined. The same is rationally true for the results were in the majority of cases varying greatly. Still, the contribution of the above studies is great, apart from their results, allowing further investigation to the issue, giving already reliable sources, tools and methodologies.

6.2 Scope of this cost analysis

Based on data for the United States, provided by the privacyrights.org from 2006-2014, 4341 incidents involving the loss of personally identified information were reported, as shown in Table 7. These cases involve a much greater number of lost records and organizations, institutions and companies. During the course of those nine years the data breaches reported, duo to loss of private or sensitive information are between 253 and 680, with an average 482 number of reported data breaches in US per year. In 2012 was a rise in the number of incidents of data loss reported. After 2010 it can be said that the number of data breaches reported has increased. In 2014 a decline is observed, but even though the data collected and processed here where updated in 2015 and the web page used as a primary source is updated approximately every two days, might not all of them are yet discovered and reported.

Table 7: Number of Data Breaches 2006-2014

Year	Number of Data Breaches (privacyrights.org)
2006	482
2007	453
2008	354
2009	253
2010	607
2011	598
2012	680
2013	622
2014	292

Still those results should not be generalized or taken for granted. They come from a particular source which collects data breach notification letters scented to various jurisdictions in the United States. Consequently the sample is not equilibrated among the various countries not even states, weights are not assigned to the results and where by low report of data breaches is obligatory the regional results will end up to be biased against the more transparent. Furthermore, the privacy-rights database doesn't include every breach. A set of criteria is used and the resulted lists contain breaches involving the release of personal information, preferably related with an organization and affecting more than nine individuals.

What can be observed from a more wide perspective and proprietary sources is that multinational companies may reveal the existence of a breach, but won’t provide any quantification, or the records lost will be reported but the company or parties involved remain unknown to the public eye. That shows that indeed data about the past are collected, lessons can be learned, but its study and report is sensitive and should not be taken outside the context of each research. Also, the picture of the past is nothing more than what the name indicates; past and it is a picture and not reality. To mach information is hidden, maybe from the majority, but not lost.

Competition, laws, technological expertise make companies more or less aware about their own breaches, and it’s one of the players choose according to their best interest how to announce or not their losses from mistakes or attacks. The situation should not be over- or underestimated. As it has been seen from the brief literature review, the changes in share prices have been used as an indication and the security index (http://www.pircenter.org/en/static/international-security-index-isi) provides the trends claimed from experts. Still within these years of economic uncertainty and fear, technological changes are astonishing. The environment, in other words, is alternated ‘in bulk’.

Many and different aspects of cost could have been examined. From the sample chosen information about the documents lost were collected. In many of the already referenced work the average cost of a record lost has been estimated. The average price per record was used, as will be described further in the methodology subsection, in order to estimate the costs of data breaches. This approach observed in detail indicates that for each country and sector the price of a record breach differ. Taking that into account a calculation that approximately shows possible costs for the data breaches examined has been developed for the United States. The reason of this specialization is because more and accurate information is available and accessed for the public. In addition the existing regulations control and keep track of the incidents involving lost data from the past. As a result comparisons and studies can be more in depth and accurate.

In any case, it should be stated that the results of the reviews and studies are more accurate and accountable. This approach is limited to the information, tools and time given. It is held in order to observe if a simple experiment as this gives results that are similar to the studies or not. In other words as the studies published cannot be examined it is attempted at least to find what someone can deduce from what is widely given to the public and can be extracted and understood easily from an average person. It is widely claimed that those databases are important for information sources. What remains is to examine what can be derived from them and what are the limits.

6.3 Methodology

In order to access the impact of data breaches from the above described sample, data for the time period of 1st of January, 2006 up to 31st of December, 2014 were collected in a yearly base. From a first examination 4341 data breaches were identified. During the course of time the period 2012 was the most intensive. The illustration of the data is presented in the Figure 22. Compared to 2006 up to 2009 it can be easily seen that the breaches have increased after 2010, whereas in 2014 the average number of breaches is lower than that of the previous four years.

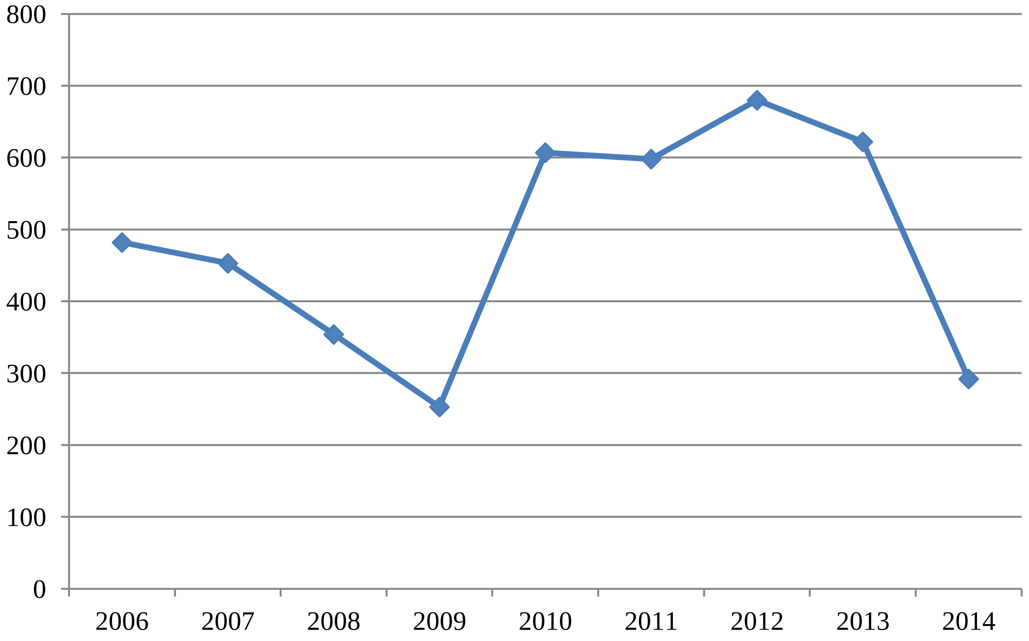

Figure 22: Number of Data Breaches in U.S 2006-2014

The goal of the analysis of those data breaches is to estimate the impact for corporations. The cost approach seems to be the most crucial for companies. As has been already mentioned some of the widely accepted studies give estimations for the cost of data breaches. In the years the cost is different and increasing. Because of that the chosen sample examined, takes different costs of data breaches among the different years. Another challenge was the price with which each recorded will be charged. Among countries those costs differ. Main reasons are the different legislations, costs of crisis management and the importance of the information included in each record. Here the focus is given to the United States and as a result the prices correspond to dollars.

From the report of Ponemon Institute, entitled “2014 Cost of Data Breach Study: United States” [Pon14] it has been found that the cost per record is increased compared to 2013 from $188 to $201. This price has been deducted after examination during January 2013 up to March 2014. The term record is used to refer to information that identifies an individual whose data are compromised. In the same direction and because the attempt to collect costs for forensics, support, monitoring, investigations, communications, customer and reputation loses were above possible, the numbers given are used. The limitations are that these numbers are only valuable for the United States organizations with no less than 5,000 and more than 100,000 records breached.

The per capita cost of data breaches over nine years, from 2006 up to 2014, has been estimated among $138 to $214. Figure 23 based on the diagram from the Ponemon Institute research report, shows the cost with which the records collected from the above described sample will be calculated. The per capita cost estimated in the Ponemon study have been calculated by the division of the total cost of data breach with the number of lost or stolen records. Table 8 shows that our sample is much greater compared to the Ponemon research. It can be seen that the results are based only to what is available and as a result they are not accurate. Still they fulfill the original purpose, which is except from studding what is already studied, to find what proprietary data offered publicly indicate. With this attempt a more active research of the issue is dared further from the more reliable and important literature review.

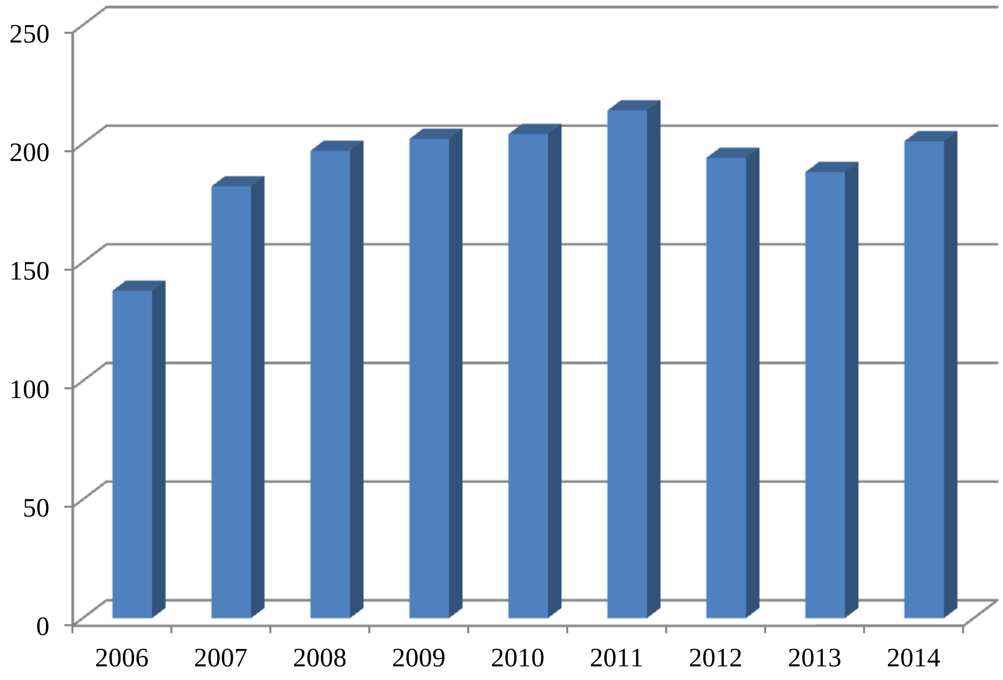

Figure 23: Per capita cost of data breach (Ponemon Institute) 2006-2014

Table 8: Sample size for 2006-2014

Year	Sample of Data Breaches Ponemon Institute	Sample of Data Breaches (privacyrights.org)
2006	14	482
2007	31	453
2008	35	354
2009	43	253

Year	Sample of Data Breaches Ponemon Institute	Sample of Data Breaches (privacyrights.org)
2010	45	607
2011	51	598
2012	49	680
2013	54	622
2014	61	292

In the sample collected for this research, the cases where they were not social security numbers and financial losses haven't been reported are not included. Furthermore, when the number of the information related to unknown SSNs and financial data are also excluded. The main reasons for these choices are that where this type of information is not provided individuals may not be affected and also it is a common practice where fragments of what may have been exposed is known, those cases to be excluded from the final sample. In the same direction and with the danger of an underestimation the final cases included in the sample analyzed, where selected. The final sample formed is shown in Table 9, in comparison with the Ponemon Institute sample and this studies initial pool of data.

Table 9: Final Sample size for 2006-2014

Year	Sample of Data Breaches Ponemon Institute	Sample of Data Breaches (privacyrights.org)	Final Sample of Data Breaches (privacyrights.org)
2006	14	482	103
2007	31	453	100
2008	35	354	95
2009	43	253	53
2010	45	607	77
2011	51	598	53
2012	49	680	51
2013	54	622	78
2014	61	292	43

From the Table 9 can be seen that the final sample is much closer to the sample size the Ponemon Institute have used. Also, the cases taken may differ as the primary sources are different. What is common is that in our final sample the final cases included are of middle breaches, meaning the number of records lost, the time period is the same and they are also incidents that caused losses to companies in the United States. It is also important o mention here that the year in which the data breach is included and counted is that of the incident. In some cases the year of the breach and the actual year of the discovery differ. In our sample the year of occurrence of the incident is the same as the year where the losses in terms of records are calculated.

Furthermore, in Table 9 and in our sample, for consistence with the prices with which the number of breaches is correlated to deduce cost estimation, cases where less than 5,000 records or more than 100,000 records where published, reviled, stolen or hacked, are also not included, because that is related with extreme cases of breaches where average prices are not a reliable measure. Appendix A contains the big data breaches that occurred from 2006 up to 2014, were reported but have not been taken into account for this study. Also, cases where the firm has agreed to pay a penalty and the number of SSNs involved are unknown are not included along with incidents where partial SSNs were exposed. The prices for a data breach in the US for a certain year are for casual, limited scale incidents and won’t be proper to use for more pervasive incidents. To summarize, the final cases investigated include breaches that exposed from 5,000 up to but no more than 100,000 and due to the information provided individuals were affected or at least they can be identified.

The details can be found in Appendix B, which summarizes important data breaches that most of them are well known to the public, because of their potential impact. Due to the fact that the number of records lost in each one of those cases is very high, if used in a sample, the cost criteria used for our research will be inaccurate. When data breaches of that scale occur, and as it can be seen it becomes a common scenario especially for well-known companies and oligopolistic markets, the average number of records lost that year increases dramatically. Of course data breaches of that scale should not be ignored, but as it has been explained if included in our sample the results would have been invalid.

6.4 Data selection criteria

The data set was built with a focus in the companies of United States, and a market wide perspective, as all types of businesses are included, with incidents that occurred between the years 2006 and 2014. The final sample has been further processed and cases were extracted based on criteria. Companies whose records did not contain personal or sensitive information couldn't be used, because they are not important for the companies neither for this study and the scope of security. It is necessary for the accuracy of the results to be estimated not only the cost of a breach but also how important is for each corporation in particular. This is though very difficult to found because it will be possible only for companies enlisted in the stock market and their balance sheets are published. Furthermore, whenever the number of records lost weren't provided the incident was also excluded from the sample.

Concerning the above limitations should be mentioned that data loss incidents studied is far from a complete sample. Also, many data breaches cases that would have been of importance offer very few information to the public. This is rational from a corporate perspective as they make the breach less reported and quickly forgotten. As a result the losses the companies suffer are limited in that period [Attr07]. Considering though that rarely corporate attacks increase in complexity, precision and sophistication it may expose the enterprises in greater future risks. The above imply that numbers are important but still when their quality and usability is limited they can misdirect rather to inform and the real situation is far from being reviled.

Thus, the data and result that will be examined and presented in this section suffer from many statistical problems. They are derived from sources that may use the same terminology to represent different things, they are collected from particular sources and only what could be studied further was selected. The sample is in that way not random neither stratified random. The statistics are used because they give a summary of a large amount of data in an easy understandable way. Here they are used for the solid purpose to examine if data breaches cost money to corporations. However, the reader should question the accuracy of the results for uses outside of this study.

The cases collected were further filtered. They were breaches where multiple companies were attacked, such as Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card and Target Brands, Inc., Fazio Mechanical Services, Inc or even Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank, North Middlesex Savings Bank, Golden Chick. These cases were also related with stolen laptops, but the reports were for all of them together. Citigroup, Time Warner Inc., Towers Perrin, Altria, United Technologies, Prudential Financial, Random House, Stanley, Inc., Bertelsmann Services Inc., AGL Resources Inc., Salvage Association, The Nielsen Company, Major League Baseball, Unilever, Harlequin Holdings, Celanese Americas Corporation, The Interpublic Group, Dover Corporation, Continuum Health Partners, Roman Catholic Diocese of Brooklyn, Cambrex Corporation, Strategic Industries, Shorewood.

An analysis of these incidents could produce misleading results where separate data are not provided from each of the institutions. Those cases were excluded for that purpose along with incidents where the victim organization is unknown. In addition, the incidents selected have thousand records lost and were considered as important, as they represent the average type of breaches occurred. They were selected because the impact they have for corporations can be showed more clearly, based on the data available. An important disadvantage is that in some cases an initial attack is followed by the real attack, or many attacks that look final or unconnected can potentially have a wider scope and a different target. This has not been taken into account because it requires a different perspective to the data presented above and this is not the purpose of this study.

By not examining well published and discussed incident it can be assumed that the public was aware of them and the costs caused can be isolated or observed more easily. Especially through the punctuations in their stock prices, as it has been seen that is the most common method used. On the other hand, in the real market the ceteris paribus hypothesis is untrue. Keeping that in mind it is assumed that if all the other factors that could have caused any type of corporate costs are steady, or the same, the costs caused by data breaches can be observed. The sample and orientation though of our study is different. The final cases examined are wide, but only for the United States and furthermore are not unbiased as the differences among states and the distribution of corporate data breaches are not taken into account. That was the main reason of the presentation of other studies on the subject along with their findings in the first subsection of this chapter.

6.5 Results

The following are the most salient findings and implications of the above examination:

- The cost of data breaches decreased. Approximately, the cost of a data breach for companies examined in this study is $5.3 million. Table 10 shows with more accuracy how the average cost of a data breach varies among the years for an organization.

Table 10: Corporate Cost of a Data Breach 2006-2014

Year	Cost of a Data Breach for an Organization
2006	3,808,243.98
2007	5,007,480.66
2008	5,909,539.64
2009	6,917,836.83
2010	4,953,928.05
2011	5,907,631.51
2012	5,469,362.12
2013	4,227,478.87
2014	5,592,006.98

- The cost of data breaches for companies has decreased. As in can be seen in detail, examining every year approximately 73 companies, their cost of data breaches is between $500million to 300million. The year 2014 has lowest cost, but also only 43 companies have provided data that fulfilled the predefined criteria for our study.

Table 11: Findings from the cost experiment 2006-2014

Year	Number of Companies Examined	Number of Records Lost/Stolen	Cost per record	Cost of Data Breaches
2006	103	2,842,385	$138	$392,249,103
2007	100	2,751,363	$182	$500,748,066
2008	95	2,849,778	$197	$561,406,266
2009	53	1,815,076	$202	$366,645,352
2010	77	1,869,865	$204	$381,452,460
2011	53	1,463,105	$214	$313,104,470

Year	Number of Companies Examined	Number of Records Lost/Stolen	Cost per record	Cost of Data Breaches
2012	51	1,437,822	$194	$278,937,468
2013	78	1,753,954	$188	$329,743,352
2014	43	1,196,300	$201	$240,456,300

- The cost of data breaches is related with the number of data breaches that occurred at the same year. As Figure 24 illustrates the outside cycle shows the percentage of the annual cost companies have suffered due to breaches. the inside cycle depicts the percentages of the number of breaches examined at each time period. In the years 2007, 2012 and 2014 the number of data breaches and the cost impact has the same percentages. In 2008, 2009 and 2011 the breaches examined were fewer compared to the cost affecting the overall losses for companies. Finally, in 2006, 2010 and 2013 the number of breaches examined were greater compared to the cost estimated for the same years.

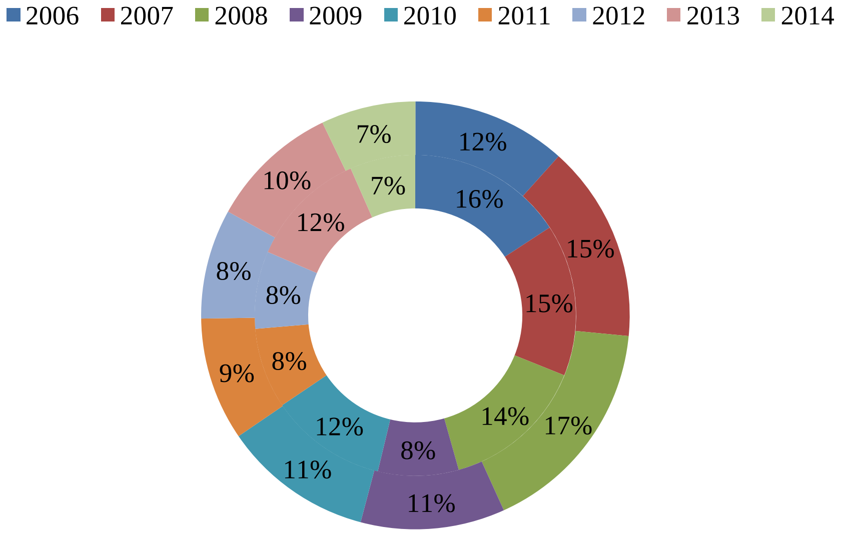

Figure 24: Number of Data Breaches and their Costs 2006-2014

- The cost of data breaches has increased in 2014. After reaching a peak in 2009 with an average cost for a company $6.9million per data breach, in 2011 has also reaches $5.9 million and after a decrease for two years in 2014 has reached the$5.5 million. Still overall even the years of the higher costs show a diminishing impact. Those data are also depicted in Figure 25.

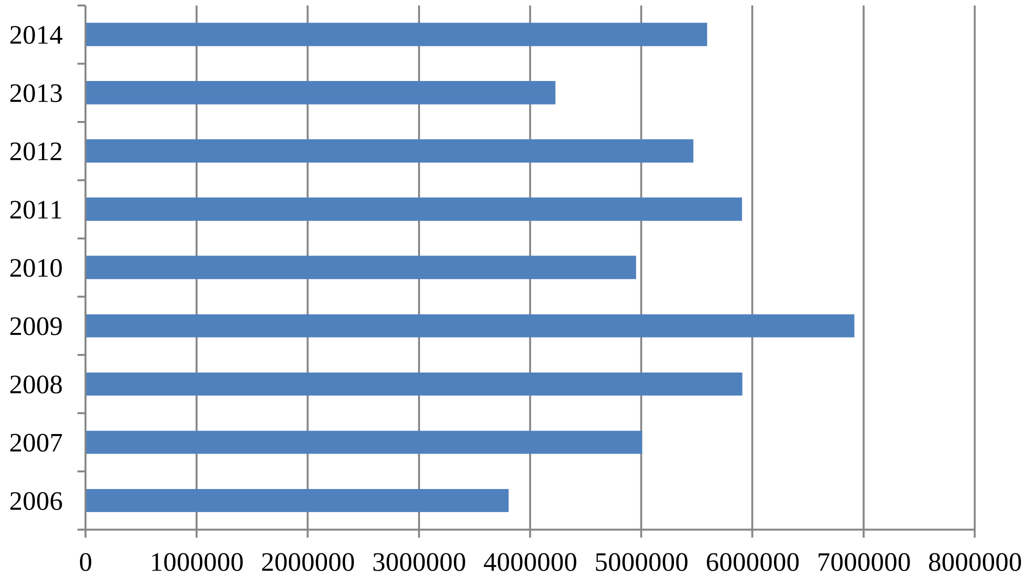

Figure 25: Data Breaches Costs Variations 2006-2014

Regarding these results but also the experiments of the Chapter 5 the following should be made clear:

Our study utilizes data and proprietary benchmark that have been deployed from important organizations and earlier research. However, our approach has inherited limitations and limits that should be taken in consideration before drawing conclusions from the findings presented. More accurately our experiments are based on statistical samples that contain entities involved in breaches where loss or thefts of customer or consumer records have occurred. As our sampling methods are not scientific, but based on availability, statistical inferences, average amounts and confidence intervals cannot be applied. Furthermore, the findings are based on small samples compared to the real market. There is always the possibility that companies that didn't participate to have substantial differences, especially regarding the estimation of costs, which differ among countries and even business sectors of the same country.

In addition, the quality of final results is also limited to the extent the sample is representative of the population. In our belief the current sampling frame is biased especially towards companies with more advanced information security in countries where the law forces publication of data breaches. Focused on consistency with our goals, we omitted other important variables from the analysis, such as treads and organizational specific characteristics. The cost results are further dependent on the honesty and accuracy of the companies reporting them and the cost methods used from the sources of the estimated amounts.

Having stated the above, it is attempted to show that the final results may introduce inadvertently bias and inaccuracies and are not presented to deceive. Rather they are accompanied from literature reviews and findings of international studies, in order the real to for his/her own conclusions based on data given and found throughout time.

7 Factors that lead to Risk Management Failure

In this study the focus is in information security risk management, regarding confidentiality. Risk management efficiency is approached from this angle and before what can be improved is presented, the purpose and strengths of risk management will be reminded briefly. Instead of focusing to the collection of weaknesses of risk management for a particular company, we preferred a broader approach which can be useful for any organization. Our approach achieves to avoid the exposure of an enterprise and at the same time to cover issues of wider interests.

7.1 Scope and Purpose of Risk Management

Planning under uncertainty and with restrict resources is a challenging task. Not only for the current state of a company but also about future choices to be made, is risk management used. Vulnerabilities, threats, probabilities, consequences can be estimated and managed. This information can be gathered for long and short term plans and even for ongoing tasks. Furthermore, risk management offers a framework which can be applied and adjusted according to circumstances. Risk management can be specified and access threats and casualties, costs and probabilities oriented to an attacker profile, or a type of information or any other factor of central interest. From assessments to situations best practices and mitigation techniques are also offered.

The goal of risk management is not absolute security. That is not related with whether security can be achieved or not, but to the role of risk management, which regarding information security issues don't change. Companies have strategic goals. Concepts such as continuity, profitability, quality and competitive advantage are common goals. Risk management, as any other corporate component; assist businesses to achieve their goals. Information is an increasing value for the company but is a unique type of asset. Similarly technology is not only critical for firms but also necessary for even trivial operations, let alone decision of high priority.

Collecting, assessing, categorizing, selecting and updating what should be the priorities in terms of information security form the bottom-line for every other decision. Risk management offers a common reference, vague situations where uncertainty is present are assessed and alternatives are calculated. In some cases processes of risk management are faced as not entirely scientific. What has been proposed is a conservative approach. When approaching an issue in such a way, it is taken into account and used as a central point of reference the worst case scenario and the resulted possible casualties [ACRC07]. In the basic theory of the philosophy of science regarding the aims and scientific results two perspectives are analyzed. The two main schools of science are the scientific realists and the scientific antirealists, commonly referred also as instrumentalists. The scientific relists perceive the scientific goals and findings either as true or approximate true that can form a theory. On the other hand, instrumentalists' perspective is that science is not after truth. It aims to be useful and the theories derived should not be considered as scientific truths but as descriptions with utility [Lad02]. A popular argue is that of Popper who conceded the falsifiability, meaning that every scientific claim can be proved wrong. If such a proof is not found after sufficient effort then the claim is possible true) as the central property of science [Popp05].

Even what is science is an issue that scientists disagree even for its importance [EnBr13], but living that aside mistakes are not something that degrades a scientific method. Even in mathematics, statistics, econometrics the error is a factor that is always taken into account but doesn't degrade the science, but the truthfulness of the specific result which is always limited and related to a specific context. The same is true for information technology risk management. The fact that it has weaknesses, which are studied continually, is in its own nature and terms as security, control, transparency, peace are taught as unadoptable beneficial goals for humanity but can be used against other words of diminishing importance through the years, such as privacy, freedom, weaknesses, emotions which are redefined correlated with doubt, uncertainty, fear, inability.

To recapitulate, the goal of risk management is to create a reference framework that will enable corporations to manage according to their interests' risks and uncertainties [Dion13]. Risk management has been defined in various ways. It is either presented as a framework of risk management policy that aims to direct and individual management of each threat or it is approached as a part of a security policy, which handles possible global and indirect risks [CLUSIF09]. In either cases risk management is an activity which integrates processes such as recognition of risks, risk assessment, controls and strategies to manage it, and mitigation of risk using limited corporate resources. Risk management is a broad sector which cavers financial, operational, physical, legal, technological and other risks. Taking that into account the objective of risk management is redefined to the management of risks related to a pre-selected domain of interest. Here this domain is information technology and especially security focused to confidentiality [Berg10].

Having stressed the importance of information security, present the general essence of science and risk management, what can be improved in the field or information risk management follows in the form of a literature review. We present arguments that belong to the general scope of risk management and then we emphasize to information security related arguments. In addition, opinions that regard risk management as a poorly applied and not correctly understood are presented. The goal is to find what has been argued up until now regarding the issue. To show that in term of weaknesses, scientists other times are identifying flows and others see the flow to the particular practices where the results are not acceptable. In its approach different arguments are presented and all together offer a better understanding to the particularities of risk management and especially regarding the security of information. Furthermore after each section we express our opinions based on the theory of risk management, in order to assess the various arguments.

7.2 Arguments regarding Risk Management

In the 20th century risk management emerged. As any human creation is imperfect and can be improved. Early papers argue that the concept of risk is subjective and related to psychological, social, cultural and political factors. Whoever determines how risk is defined, controls the solution risk management would propose. In other words, how risks are defined, lead to different ordering of priorities and controls. For this approach risk management should be publicly acceptable [Slov99]. There is a belief that the risks addressed are based on threats that are known and can be predicted. Consequently, there is a possibility yet not relieved dangers to be neglected, which may be more consequential compared to those estimated [Stul08].

Another argument is that risk management doesn’t offer an unambiguous, universal way for determining what identified risks must be controlled or mitigated compared to others that may be accepted without any further action. Different interests and methodologies presented in an organization indicate other risks as more important and the final decision of the prioritization of risks remains challenging [RoSc04]. In other words, it’s commonly claimed that even if objective methodologies assess risks, the calculations are conditioned to subjective judgments. Risk-analysis techniques are affected from a variety of interpretations, depending on which method is used, by whom and which data have been selected and used [Renn85].

Regarding risk assessment in particular, some limitations have being identified. Risk assessment can be held ether in a qualitative or quantitative manner. For the qualitative approach has been found that the risk rating doesn’t contain sufficient data to guide the allocation of the available resources. In addition, scores assigned to consequences and vulnerabilities resulting to risks can lead to results where the resulted risk is nonzero even if the consequences or the vulnerabilities have been estimated as close to zero. Another issue of concern is the assignment of scores to risks, where a greater risk may not be assigned with the right criticality. It has also been argued that in quantitative approaches the calculation of average values is incorrect mathematically, as the estimations can be easily manipulated, not all the risks can be represented or analyzed and if a scale of risks is created the all estimated ranging can contain errors. [Cox08]

The overemphasis to complicated measurements regarding the estimation of risks is recognized as important but sometimes as also dysfunctional. The argument claims that the quantitative methods used come from certain disciplines and effectiveness measures are rare. What has been measured up until now have been also criticized as not important neither sufficient. The main problem identified in those claims is that reality is different from theory. There is a gap between what methods in a laboratory give results compared to a business environment where not only different knowledge background coexist but also vocabulary used can be interpreted from different scientists in many ways. [Hub09] A characteristic example is the term risk management itself. For an economist it will lead to financial instruments like bonds, futures, options on the contrary an information security analyst will thing of it resources, vulnerabilities and controls.

Regarding how risk management is perceived, when controls are selected according to importance and resources, an interesting observation is that after imposing them there is a false sense of security. The existence and even the operation of controls are not sufficient. Market, industry, technology, people, attackers and generally the internal and external corporate environment changes rapid. Security should be defined with a specific scope of time, cost and attack. The culture of each business regarding risks, the level of integration of controls and operations [PoDe09] are other factors that can affect the results of risk management negatively and a general framework can only offer indications not solution. Every company, because has each own culture, should adjust the practices to what brings the best results to them in particular. General indications are the baseline, the absolute necessary. The flexibility of the guidelines offers many opportunities for improved adjustments for different needs and wants.

It has been observed that companies dealing with risks emphasize to what have experienced recently [Hub09]. Companies have to face with the use of risk management an increasingly more complex environment with external risks to create greater threats than the internal. At the same time personnel with risk management knowledge and experience is found yet not sufficient to cover the demand [Econ11]. Space for improvement has also been found between risk management processes and other business operations. A recent trend is build-in controls, embedded to the everyday business processes as part of the operations [Econ11].

From the above is important to mention once more that the processes a company accepts as more appropriate can be adjusted and adopt differently, as the definition of risk is meant to be modified according to the unique circumstances of each firm [MAS13]. Regarding the predictability of risks in risk management practices the factor that there are unidentified risks which are currently unknown to the company but existent, are taken into account [HKMA03]. Decision making and managerial positions are presented as lucrative. At the same time they come with responsibilities and if something goes wrong those who lead are taking the blame. Management is approached as a talent and a science, risk management is a tool. No matter how good the tool is the one who use it should be able to extract the most out of it.

Companies are seeking profits that won’t lose. Blaming general tactics from being inappropriate doesn’t make sense. Improve the tools, judge why for some businesses achieve great results and for others not. Some questions that can be asked in those cases are: why those methods were selected in the first place? Have been existent and applied? What went wrong? Couldn’t be found earlier? Having a follow up to risk management processes is important for the improvement of future decisions and actions. Focus to the weaknesses and adjust. Profits are important but if they cannot be kept the strange to accurate them is meaningless. Risk management is absolutely essential, not to ensure, but to guide in a general way living space for the best or the worst, but that depends to the users [Bask91]. That can be seen as an advantage and disadvantage, but even when something is enforced by law companies complain for compliance costs. As the environment becomes more competitive, such as in oligopolistic markets, rivals become fewer, with more strategic funds and targeted goals [Hub09]. The competition leads to spend on security and risk management more capital. In other words, competition in the cyber field and that indicates that given the circumstances digital security cannot be neglected.

7.3 Arguments for Information Security Risk Management

Such approaches may be important for the broader definition of risk management. In information security, though even more specific flows have been reported. As the analysis of the arguments above, the different opinions are presented with related comments and analysis in order to make clearer their importance and relevance with the purpose of information technology risk management. Compared to risk management in other areas, when it comes to information and technological means, the calculation of the assets is challenging. Hardware, software, databases, emails, digital accounts, identities, communications, cloud accounts form the assets that have to be collected and calculated. The picture becomes more complicated when some of the sources are outsourced or shared with other organizations. [RaSn91]

From that difficulty, another challenge emerges. In order for the risk to be estimated, the value of the asset should be estimated. They are different methods for the assignment of value to assets. For example, the market value, the cost of replacement, the accounting value, the option-based value and many others. But the value of an account or an e-mail’s or an identity’s, create uncertainties, regarding the most accurate method to be used and its applicability [Bon01]. Another gap in the early literature of risk management was the absent of a comprehensive framework regarding the identification, analysis, controls and monitoring processes of risk management adjusted to the needs of information security [BaMy99]. Letter such models and even frameworks have been developed, some of them were presented briefly in Chapter 4. New chapters are continually added to them regarding the security for new technologies used like cloud services. Another opinion considers the weakness not in risk management practices but in the available information security measures, which seems to have also vulnerabilities [BlMc01].

In spite of security efforts regarding safety of information, data breaches, even of large-scale can be still observed (c.f. Chapter 5). The technological environment is dynamic and in many cases this is considered as an asymmetric threat for security. Risk management is traditionally used with information security. It has been argued though that the results are not satisfactory. The reasons presented differ, but what seems to be common is that the way risk management is implemented, understood and supported is important. The cost of security is the bottom-line of business decisions. It seems to be forgotten that underestimation or overestimation of dangers comes also with losses. At the same time, the estimation of risks even if it is quantitative can contain subjectivity; controls used for mitigation purposes don’t imply security and risk management is a broad field that is learning and improves as it is applied for each organization differently.

The above presented arguments are important indications of what may be the reasons that data breaches occur even regarding cases where risk management processes are by low enforced. It seems though that the human factor may is also a factor to be concerned, because the subjectivity integrated to the term ‘management’ is perceived as a weakness but is the reason individuals holding such positions are perceived as prestigious, held by skillful individuals. In any case, the answer is not necessarily one. Different factors would be more or less important for different firms. Overall, risk management doesn’t seem to fail, it can be always improved and assisted with technology a loop of improvement can lead closer to the targeted state of information security.

8 Conclusions

Information technology has a critical role in most of today's organizations. The dramatic increase in devices interconnectivity and the popularity of Internet are offering companies unprecedented opportunities to improve operations by reducing costs, process and store information and communicate internally and externally. At the same time, however, attacks on digital systems are increasing at alarming rates, posing serious risks to business operations. Any event or action that could potentially threaten or violate and endanger the security of data, information and IT resources consist a matter that cannot be overlooked. Thus, the success of companies' ability to use interconnected systems to carry out critical operations depends greatly on their ability to protect their data and systems. Companies come to realize, all the more, those consequences and potential impacts which threaten not only organizations but also individuals associated with them.

Risk management is a common practice used in many fields to manage risks based on needs and resources. For private and sensitive information related to social security numbers and financial data, by law, companies used practices of information security risk management. We examined the effectiveness and efficiency of those practices based on the delivered results. We assessed (1) whether information security and risk management are connected, (2) whether information security in terms of confidentiality fails, (3) whether failures to secure confidentiality cause losses for corporations, and (4) the effectiveness of risk management structure and implementation regarding information security. We selected to give a worldwide representation of the state of security regarding confidentiality as data related to data breaches were available. We also emphasize, in terms of impact, to the US because we identified serious deficiencies in other samples attempted, we found evidences that companies report lost information and in many cases assess the impact and cost estimations and their variations are studied for at least nine years, offering a compare and contrast opportunity.

We found that confidentiality is not effectively managed, depending on the company. Hacking attacks, lost or stolen portable devices, insider threats and accidental exposure of data are common causes of data breaches. The information lost come with various consequences for corporations. We estimated the records lost per year and US and correlated them with the average cost per record as estimated from the Ponemon Institute. We found that data breaches are costly. The exact importance of the cost resulted may differ depending to the value of the company but the national and international impact increases the losses and reduces profits. Risk management has opportunities of improvement. A review conducted based on bibliography shows that how it is perceived and applied changes its efficiency.

This study can be expanded in many ways. Firstly, the same questions can be answer in different ways. Using the same samples, different metrics can be applied to answer the same questions. Different samples can be selected to apply similar or different methods. An updated bibliography and literature review will be necessary, regarding the spread with which this sector is progressing. Furthermore, security is examined in terms of confidentiality. Integrity, availability, non-repudiation and other aspects of security are intentionally excluded. Those areas are also of interest and can be investigated in analogous or different ways. It will be also interesting if on a corporate specific level a study could be conducted. Having internal information and concluding if the available controls are sufficient, risk management is appropriately applied and if the results are satisfying the predefined goals. As part of continuous monitoring, such a study will be more practical and closer to the needs of a business audience. In order to be more scientifically interesting the results could be related with a periods of time and be compared with competitors. Another interesting aspect to examine could the proof that risk management is important and affects information security. Studies for the beneficial impact of information security has on risk management have been already held.

In the best of our knowledge, we collected, examined and present data, results, experiments and findings regarding data breaches and information security risk management. Limitations of time, cost, available material, skills and tools have resulted to a series of decisions in handling this research. We tried to be objective and to offer to the reader not only our opinions related to the results, but threw presentations of others' findings to make possible to any reader to make its own judgment. The purpose of this study was to research and learn more about information security risk management. We would like this study to be like information security risk management "a beginning with many ends" [Geer11].

APPENDIX

Appendix A: Comparison of Data Breaches Reports and Number of Records Lost Reports

Year	**Reported Data Breaches**	**Data Breaches reporting also the Number of Records Lost**
2010	953	584
2011	1241	703
2012	3219	1212
2013	2343	979
2014	2912	716
Month	**Reported Data Breaches**	**Data Breaches reporting also the Number of Records Lost**
Jan10	64	44
Feb10	72	45
Mar10	94	60
Apr10	80	51
May10	71	41
Jun10	85	49
Jul10	93	60
Aug10	92	53
Sep10	62	36
Oct10	81	48
Nov10	66	32
Dec10	93	65
Jan11	91	48
Feb11	68	37
Mar11	87	55
Apr11	101	59
May11	96	57

Month	Reported Data Breaches	Data Breaches reporting also the Number of Records Lost
Jun11	135	67
Jul11	94	46
Aug11	82	45
Sep11	103	65
Oct11	111	67
Nov11	147	85
Dec11	126	72
Jan12	140	78
Feb12	153	79
Mar12	206	129
Apr12	160	85
May12	327	174
Jun12	368	149
Jul12	266	90
Aug12	313	110
Sep12	307	89
Oct12	279	74
Nov12	416	89
Dec12	284	66
Jan13	308	90
Feb13	163	46
Mar13	250	88
Apr13	213	84
May13	154	61
Jun13	162	69
Jul13	210	94
Aug13	209	92
Sep13	136	68
Oct13	149	74
Nov13	123	54

Month	Reported Data Breaches	Data Breaches reporting also the Number of Records Lost
Dec13	266	159
Jan14	309	83
Feb14	205	59
Mar14	326	73
Apr14	226	65
May14	243	62
Jun14	317	68
Jul14	245	63
Aug14	200	53
Seo14	157	45
Oct14	243	71
Nov14	326	44
Dec14	115	30

Appendix B: Excluded Data breaches with more than 100,000 records lost

Company, State	Number of records lost or stolen
2006	
Boeing Seattle, Washington	382,000 current and former employees
University of California at Los Angeles (UCLA) Los Angeles, California	800,000
Aetna, Nationwide, WellPoint Group Health Plans, Humana Medicare, Mutual of Omaha Insurance Company, Anthem Blue Cross Blue Shield via Concentra Preferred Systems Dayton, Ohio	396,279
Greenville County School District Greenville, South Carolina	At least 101,000 students and employees

Company, State	Number of records lost or stolen
Look Tours LLC North Las Vegas, Nevada	300,000
Colorado Department of Human Services via Affiliated Computer Services (ACS) Dallas, Texas	Up to 1,400,000
Link Staffing Services Houston, Texas	332,000
Akron Children's Hospital Akron, Ohio	235,903
Sisters of St. Francis Health Services via Advanced Receivables Strategy (ARS), a Perot Systems Company Indianapolis, Indiana	266,200
Chicago Voter Database Chicago, Illinois	1,350,000 Chicago residents
Kentucky Personnel Cabinet via Bluegrass Mailing Frankfort, Kentucky	146,000
Circuit City and Chase Card Services, a division of JP Morgan Chase & Co. Wilmington, Delaware	2,600,000 past and current Circuit City credit cardholders
U.S. Department of Transportation Washington, District Of Columbia	132,470
American Online (AOL) New York, New York	650,000 (Unknown number of high-risk personal records)
Sentry Insurance Stevens Point, Wisconsin	112,270
Kaiser Permanente Northern California Office Oakland, California	160,000 records. Because the data file did not include SSNs, this number is not added to the total below
Nelnet Inc., UPS Lincoln, Nebraska	188,000

Company, State	Number of records lost or stolen
CS Stars, subsidiary of insurance company Marsh Inc. Chicago, Illinois	722,000
Nebraska Treasurer's Office Lincoln, Nebraska	309,000
Western Illinios University Macomb, Illinois	180,000
American International Group (AIG), Indiana Office of Medical Excess, LLC New York, New York	930,000
Denver Election Commission Denver, Colorado	150,000
Ernst & Young New York, New York	243,000
Texas Guaranteed Student Loan Corp. via subcontractor Hummingbird Round Rock, Texas	1,300,000 plus 400,000 for total of 1,700,000
Mortgage Lenders Network USA Middletown, Connecticut	231,000
U.S. Department of Veterans Affairs Washington, District Of Columbia	26,500,000
American Red Cross, St. Louis Chapter St. Louis, Missouri	1,000,000
A merican Institute of Certified Public Accountants (AICPA) New York, New York	330,000 [Updated 6/16/06]
Ohio University Athens, Ohio	300,000 (137,000 SSNs)
Ohio Secretary of State Cleveland, Ohio	Potentially millions of registered voters
University of Texas McCombs School of Business Austin, Texas	197,000

Company, State	Number of records lost or stolen
U.S. Marine Corp Monterey, California	207,750
Georgia Technology Authority (GTA) Atlanta, Georgia	573,000
Fidelity Investments Boston, Massachusetts	196,000
iBill [disputed] Deerfield Beach, Florida	17,781,462 (SSNs and financial information not involved)
Los Angeles County Department of Social Services Los Angeles, California	Potentially 2,000,000
Hamilton County Clerk of Courts Cincinnati, Ohio	[1,300,000] Not included in number below
U.S. Department of Agriculture (USDA) Washington, District Of Columbia	350,000
OfficeMax Naperville, Illinois	200,000, although total number is unknown
Boston Globe (The New York Times Company) and The Worcester Telegram & Gazette Boston, Massachusetts	240,000
Providence Home Services Portland, Oregon	365,000
2007	
The Variable Annuity Life Insurance Company Amarillo, Texas	774,723
Davidson County Election Commission Nashville, Tennessee	337,000
Memorial Blood Centers Duluth, Minnesota	268,000

Company, State	Number of records lost or stolen
Prescription Advantage Boston, Massachusetts	150,000
U.S. Department of Veteran Affairs Washington, District Of Columbia	185,000
Hartford Financial Services Group Hartford, Connecticut	230,000
West Virginia Public Employees Insurance Agency Charleston, West Virginia	200,000
Administaff Inc. Houston, Texas	159,000
Massachusetts Division of Professional Licensure Boston, Massachusetts	450,000
Gap Inc. San Francisco, California	800,000
TD Ameritrade Holding Corp. Omaha, Nebraska	6,300,000
Gander Mountain Greensburg, Pennsylvania	112,000
Connecticut Department of Revenue Services Hartford, Connecticut	106,000
New York City Financial nformation Services Agency New York, New York	280,000 Not added to total. It is not clear that SSNs or financial account numbers were exposed
California Public Employees' Retirement System (CalPERS) Sacramento, California	445,000
Fox News Los Angeles, California	1.5 million Not added to total. It does not appear that SSNs or financial account numbers were exposed.

Company, State	Number of records lost or stolen
Science Applications International Corp. (SAIC) San Diego, California	867,000
Fidelity National Information Services/Certegy Check Services Inc. Jacksonville, Florida	8,500,000
Ohio state workers Columbus, Ohio	1,000,000
Texas Commission on Law Enforcement Standards and Education Austin, Texas	230,000
Illinois Dept. of Financial and Professional Regulation Chicago, Illinois	300,000
Georgia Division of Public Health Atlanta, Georgia	140,000
Community College of Southern Nevada North Las Vegas, Nevada	197,000
Neiman Marcus Group Dallas, Texas	160,000
Georgia Department of Community Health, Affiliated Computer Services (ACS) Atlanta, Georgia	2,900,000
Hortica (Florists’ Mutual Insurance Company), UPS Edwardsville, Illinois	268,000
Los Angeles County Child Support Services Los Angeles, California	243,000
St. Mary's Hospital Leonardtown, Maryland	130,000
Johns Hopkins University and Johns Hopkins Hospital Baltimore, Maryland	135,000 (52,000 past and present employees plus 83,000 patients)

Company, State	Number of records lost or stolen
Merchant America Camarillo, California	130,000
U.S. Department of Veterans Affairs, VA Medical Center Birmingham, Alabama	48,000 veterans plus 535,000
Chicago Board of Election Chicago, Illinois	1,300,000
TJ stores (TJX), including TJMaxx, Marshalls, Winners, HomeSense, AJWright, KMaxx, and possibly Bob's Stores in U.S. & Puerto Rico -- Winners and HomeGoods stores in Canada -- and possibly TKMaxx stores in UK and Ireland Framingham, Massachusetts	100,000,000
Towers Perrin New York, New York	300,000
Wisconsin Department of Revenue via Ripon Printers Madison, Wisconsin	171,000 taxplayers
2008	
RBS WorldPay Atlanta, Georgia	1,100,000
Florida Agency for Workforce Innovation Tallahassee, Florida	259,193
University of Florida College of Dentistry Gainesville, Florida	330,000
Express Scripts St. Louis, Missouri	700,000
The Princeton Review New York, New York	108,000 (No SSNs or financial information reported)
Countrywide Financial Corp. Calabasas, California	17,000,000

Company, State	Number of records lost or stolen
Blue Cross and Blue Shield of Georgia Atlanta, Georgia	202,000
Facebook Palo Alto, California	Unknown 80 million Not added to total since the breach is not SSNs or financial account data.
Saint Mary's Regional Medical Center Reno, Nevada	128,000
Division of Motor Vehicles Colorado , Colorado	3,400,000
University of Utah Hospitals and Clinics Salt Lake City, Utah	2,200,000
CollegeInvest Denver, Colorado	200,000
Central Collection Bureau Indianapolis, Indiana	700,000
University of Miami Miami, Florida	2,100,000
WellPoint Indianapolis, Indiana	128,000
Bank of New York Mellon Pittsburgh, Pennsylvania	Originally 4.5 million customer records, raised to 12.5 million
Compass Bank Birmingham, Alabama	1,000,000
Hannaford Bros. Supermarket chain Portland, Maine	4,200,000
Health Net Federal Services Rancho Cordova, California	103,000
Lifeblood Memphis, Tennessee	321,000
Davidson Companies Great Falls, Montana	226,000
Horizon Blue Cross Blue Shield Newark, New Jersey	300,000

Company, State	Number of records lost or stolen
GE Money , Iron Mountain Boston, Massachusetts	150,000
Wisconsin Department of Health and Family Services Madison, Wisconsin	260,000
2009	
Eastern Washington University Cheney, Washington	130,000
RockYou Redwood City, California	32 million (No SSNs or financial information reported)
Health Net Shelton, Connecticut	1,500,000
National Archives and Records Administration College Park, Maryland	250,000
Virginia Department of Education Richmond, Virginia	103,000
BlueCross BlueShield Assn. Chicago, Illinois	187,000
U.S. Military Veterans Washington, District Of Columbia	76,000,000
University of North Carolina, Chapel Hill Chapel Hill, North Carolina	236,000 (163,000 SSNs estimated)
National Guard Bureau Arlington, Virginia	131,000
Network Solutions Herndon, Virginia	573,000
National Archives and Records Administration College Park, Maryland	250,000
University of California, Berkeley Berkeley, California	160,000

Company, State	Number of records lost or stolen
Virginia Prescription Monitoring Program Richmond, Virginia	531,400
Oklahoma Housing Finance Agency Oklahoma City, Oklahoma	225,000
Oklahoma Department of Human Services Oklahoma City, Oklahoma	1,000,000
Arkansas Department of InformationSystems, Information Vaulting Services Little Rock, Arkansas	807,000
phpBB.com Bellevue, Washington	400,000 Not added to total; SSNs were not accessed.
Heartland Payment Systems Princeton, New Jersey	Over 130 million
CheckFree Corp. Atlanta, Georgia	5,000,000
2010	
American Honda Motor Company Torrance, California	4.9 million (No SSNs or financial information reported)
deviantART, Silverpop Systems Inc. Hollywood, California	13,000,000 (No SSNs or financial information exposed)
Twin America LLC, CitySights NY New York, New York	110,000
Ohio State University Columbus, Ohio	750,000 (Unknown numbers of SSNs and financial information)
Gawker New York, New York	1,300,000 (No SSNs or financial information reported)
Mesa County, Western Colorado Drug Task Force Grand Junction, Colorado	200,000 (Unknown number of SSNs)
Triple-C, Inc. (TCI), Triple-S Salud, Inc. (TSS) San Juan, Puerto Rico	406,000 (No SSNs or financial information reported)

Company, State	Number of records lost or stolen
Houston Independent School District (HISD) Houston, Texas	232,000 (30,000 employees)
University of North Florida Jacksonville, Florida	106,884 (52,853 SSNs reported)
College Center for Library Automation (CCLA) Tallahassee, Florida	126,000
Citigroup Inc. New York, New York	117,600 (No incidents reported)
Colorado Department of Health Care Policy and Financing Denver, Colorado	105,470 (0 SSNs and financial information reported)
South Shore Hospital, Active Data Solutions South Weymouth, Massachusetts	800,000 (unknown number of SSNs and financial information)
Marsh and Mercer Washington, District Of Columbia	378,000
Massachusetts Secretary of State, Securities Division Boston, Massachusetts	139,000
Lincoln Medical and Mental Health Center Bronx, New York	130,495
Anthem Blue Cross, WellPoint Pasadena, California	470,000
Apple Inc., AT&T Cupertino, California	120,000 (No SSNs or financial information involved)
Digital River Inc. Eden Prairie, Minnesota	200,000
Army Reserve/Serco Inc. Morrow, Georgia	207,000
Millennium Medical Management Resources Westmont, Illinois	180,111
Affinity Health Plan Bronx, New York	409,262

Company, State	Number of records lost or stolen
Educational Credit Management Corporation ST. Paul, Minnesota	3,300,000
Wyndham Hotels & Resorts Dallas, Texas	500,000
Citigroup New York, New York	600,000
Valdosta State University Valdosta, Georgia	170,000
AvMed Health Plans Gainesville, Florida	208,000 Additional 860,000 added June 3rd; (11/16/10) Estimate reaches 1.22 million Additional 860,000 added June 3rd; (11/16/10) Estimate reaches 1.22 million
Lincoln National Corporation (Lincoln Financial) Radnor, Pennsylvania	1,200,000
BlueCross BlueShield (BCBST) Chattanooga, Tennessee	1,023,209 (451,274 Social Security numbers involved)
Netflix Los Gatos, California	100 million not added to total
2011	
United States Chamber of Commerce Washington, District Of Columbia	3,000,000 (No SSNs or financial information reported)
Restaurant Depot, Jetro Cash & Carry College Point, New York	300,000
Sutter Physicians Services (SPS) and Sutter Medical Foundation (SMF) Sacramento, California	4.24 million (No SSNs or financial information involved)
Virginia Commonwealth University Richmond, Virginia	176,567

Company, State	Number of records lost or stolen
Steam (The Valve Corporation) Bellevue, Washington	35,000,000
The Nemours Foundation Wilmington, Delaware	1,600,000
TRICARE Management Activity (formerly Civilian Health and Medical Program of the Uniformed Services, CHAMPUS), Science Applications International Corporation (SAIC) ,	5,117,799
Kiplinger Washington Editors Inc. Washington, District Of Columbia	142,000
RxAmerica and Accendo Insurance Company Salt Lake City, Utah	176,300 (No SSNs or financial information)
Sega London, London City of	1.29 million (No SSNs or financial information reported)
Bethesda Softworks Rockville, Maryland	200,000 (No financial information or SSNs reported)
Southern California Medical-Legal Consultants, Inc. (SCMLC) Seal Beach, California	300,000
Citibank New York, New York	360,000
Sony Pictures, Sony Corporation of America New York, New York	1,000,000 (No SSNs or financial information reported)
Spartanburg Regional Hospital Spartanburg, South Carolina	400,000
Massachusetts Executive Office of Labor and Workforce Development (EOLWD) Harrisburg, Pennsylvania	210,000

Company, State	Number of records lost or stolen
Sony, PlayStation Network (PSN), Sony Online Entertainment (SOE) New York, New York	101.6 million (12 million unencrypted credit card numbers)
WordPress San Francisco, California	18 million (No SSNs or financial information reported)
Oklahoma State Department of Health Oklahoma City, Oklahoma	133,000
Texas Comptroller's Office Austin, Texas	3,500,000
Epsilon Irving, Texas	50-250 million (No SSNs or financial information involved)
Eisenhower Medical Center (EMC) Rancho Mirage, California	514,330 (No SSNs or financial information reported)
Health Net Inc., International Business Machines (IBM) Rancho Cordova, California	1,900,000
Cord Blood Registry San Francisco, California	300,000
Cambridge Who's Who Publishing, Inc. Uniondale, New York	400,000
Jacobi Medical Center, North Central Bronx Hospital, Tremont Health Center, and Gunhill Health Center New York, New York	1,700,000
Ankle and Foot Center of Tampa Bay, Inc. Tampa Bay, Florida	156,000 (No SSNs or financial information reported)
Seacoast Radiology Rochester, New Hampshire	231,400
2012	
El Centro Regional Medical Center El Centro, California	189,489
Western Connecticut State University Danbury, Connecticut	235,000

Company, State	Number of records lost or stolen
Nationwide Mutual Insurance Company and Allied Insurance Columbus, Ohio	1,000,000
South Carolina Department of Revenue Columbia, South Carolina	6,400,000
Northwest Florida State College Niceville, Florida	279,000 (At least 200,050 SSNs exposed)
TD Bank Cherry Hill, New Jersey	260,000
United Staes Navy, Smart Web Move Washington, District of Columbia	200,000 (No SSNs or financial information reported)
Apple Cupertino, California	1,000,000 (No SSNs or financial information reported)
Memorial Healthcare System (MHS)	102,153
Wisconsin Department of Revenue Madison, Wisconsin	110,795
Gamigo Hamburg,	3 million American accounts (No SSNs or financial information reported)
Nvidia Santa Clara, California	400,000 (No SSNs or financial information reported)
Yahoo! Voices Sunnyvale, California	453,492 (No SSNs or financial information reported)
Formspring San Francisco, California	420,000 (No SSNs or financial information reported)
LinkedIn.com Mountain View, California	6,458,020 (No SSNs or financial information reported)
Serco, Inc., Federal Retirement Thrift Investment Board Reston, Virginia	123,201
University of Nebraska, Nebraska Student Information System, Nebraska College System, Lincoln, Nebraska	654,000

Company, State	Number of records lost or stolen
Hewlett, Packard, California Department of Social Services Riverside, California	701,000
Office of the Texas Attorney General Austin, Texas	6,500,000
South Carolina Health and Human Services, South Carolina Medicaid Columbia, South Carolina	228,435 (Unknown number of SSNs involved)
Emory Healthcare, Emory University Hospital Atlanta, Georgia	315,000 (228,000 SSNs reported)
Utah Department of Health Salt Lake City, Utah	780,000 (280,000 SSNs)
Global Payments Inc. Atlanta, Georgia	7,000,000
Department of Child Support Services, International Business Machines (IBM), Iron Mountain, Inc. Boulder, Colorado	800,000
MilitarySingles.com New York, New York	171,000 (No SSNs or financial information reported)
University of North Carolina at Charlotte Charlotte, North Carolina	350,000
Manwin Holding SARL (Brazzers) Waltham, Massachusetts	350,000 (No SSNs or financial information reported)
President's Challenge, Indiana University , Indiana	650,000 (Unknown number of SSNs)
New York State Electric & Gas (NYSEG), Rochester Gas and Electric (RG&E), Iberdrola USA Rochester, New York	878,000 NYSEG customers and 367,000 RG&E customers
Arizona State University (ASU) Tampe, Arizona	300,000 (No SSNs or financial information reported)

Company, State	Number of records lost or stolen
Zappos,com Las Vegas, Nevada	24 million (No SSNs or financial information reported)
2013	
Aaron Brothers Coppell, Texas	400,000
St. Joseph Health System Suwanee, Georgia	405,000
Michaels Stores Inc. Irving, Texas	2.6 million cards
Target Corp. Minneapolis, Minnesota	40million
Horizon Healthcare Services, Inc. (Horizon Blue Cross Blue Shield) Newark, New Jersey	840,000
JPMorgan Chase New York, New York	465,000
ADP, Facebook, Gmail, LnkedIn, Twitter, Yahoo, YouTube	2 million (No SSNs or financial information reported)
MacRumors, vBulletin	860,000 (No SSNs or financial information reported)
Maricopa County Community College District Phoenix, Arizona	2,490,000
CorporateCarOnline.com Kirkwood, Missouri	850,000
Court Ventures (now owned by Experian) Anaheim, California	200,000,000
Adobe, PR Newswire, National White Collar Crime Center San Jose, California	2.9 million (38 million user emails and passwords exposed)
Virginia Polytechnic Institute and State University (Virginia Tech) Blacksburg, Virginia	144,963 (No SSNs or financial information reported)

Company, State	Number of records lost or stolen
Advocate Medical Group, Advocate Health Park Ridge, Illinois	4,000,000
League of Legends, Riot Games Santa Monica, California	120,000
U.S. Department of Energy Washington, District Of Columbia	104,000 (5,711 confirmed)
St. Mary's Bank Manchester, New Hampshire	115,775
Citigroup New York, New York	146,000
Texas Health Harris Methodist Hospital Fort Worth, Shred –it Forth Worth, Texas	277,000 (Unknown number of SSNs)
Facebook Menlo Park, California	6,000,000 (No SSNs or financial information reported)
Adobe, Washington Administrative Office of the Courts Olympia, Washington	160,000
Administrative Office of the Courts - Washington Olympia, Washington	1,000,000 (160,000 SSNs)
LivingSocial Washington, District Of Columbia	29 million (no SSNs or financial information reported)
Kirkwood Community College Cedar Rapids, Iowa	125,000
Evernote Redwood City, California	50,000,000 (No SSNs or financial information reported)
Central Hudson Gas & Electric Poughkeepsie, New York	110,000
Twitter San Francisco, California	250,000 (No SSNs or financial information reported)
Cbr Systems San Bruno, California	300,000

Company, State	**Number of records lost or stolen**
2014	
Morgan Stanley New York, New York	350,000
Texas Health and Human Services Houston, Texas	2 million
U.S. Weather System Washington, District Of Columbia	Satellite systems that forecast weather
US Postal Service Washington, District Of Columbia	800,000
Staples Inc. Framingham, Massachusetts	1,200,000
Snapsaved.com Unknown,	200,000
Oregon Employment Department/WorkSource Oregon Portland, Oregon	850,000
The Home Depot Atlanta, Georgia	56,000,000
J.P Morgan Chase New York, New York	76,000,000
Community Health Systems Franklin, Tennessee	4,500,000
Russian hacking discovered by Hold Security Unknown, Wisconsin	1 billion
Goodwill Industries International Inc. Rockville, Maryland	868,000
Butler University Indianapolis, Indiana	163,000
Splash Car Wash Greenwich, Connecticut	120,000
Ebay San Jose, California	145,000,000

Company, State	**Number of records lost or stolen**
Paytime Mechanicsburg, Pennsylvania	233,000
Boxee Ridgefield Park, New Jersey	158,128
North Dakota University Bismarck, North Dakota	290,780
Los Angeles County Department of Health/Sutherland Healthcare Solutions Los Angeles, California	168,000
Indiana University Bloomington, Indiana	146,000
University of Maryland College Park, Maryland	309,079
Neiman Marcus Dallas, Texas	1,100,000

Literature

[A-B&O-B07]
Andoh-Baidoo, F.K. and Osei-Bryson, K-M.: Exploring the characteristics of Internet security breaches that impact the market value of breached firms. J Expert Systems with applications 32 (2007) 703-725.

[Accen14]
Accenture Technology Vision 2014: Every Business is a Digital Business: from Digitally Disrupted to Digital Disrupter. http://www.accenture.com/sitecollectiondocuments/pdf/accenture-technology-vision-2014.pdf, Accessed at 2014-11-24.

[ACRC07]
US Army Combat Readiness Center: Composite Risk Management Chain Teaching Training Packet. US Army Combat Readiness Center, April 2007. Available at: https://crc.army.mil/RiskManagement/detail.asp?iData=2&iCat=710&iChannel=25&nChannel=RiskManagement, Accessed at 2014-10-10.

[AlDo05]
Alberts, C., Dorofee, A., Stevens, J. and Woody, C.: OCTAVE®-S Implementation Guide, Version 1.0: Volume 1: Introduction OCTAVE-S. CMU/SEI-2003-HB-003, January 2005.

[Anth11]
Anthony, Sebastian: How the PlayStation network was Hacked. ExtremeTech, April 27,2011.

[ArFiMc00]
Arbauch, W.A., Fithen, W.L. and McHugh, J.: Windows of Vulnerability: A Case Study Analysis. Available at: http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf, Accessed at 2014-09-01.

[ArnW00]
Arnold, W.: TECHNOLOGY: Philippines to drop charges on e-mail virus. New York Times, August 22, 2000.

[AtCa11]
Atzeni, A, Cameroni, C, Faily, S, Lyle, J. and Flechais, I.: Here’s Johnny: a methodology for Developing Attacker Personas. In: Proceedings of the 2011 6th international conference on vulnerability, reliability and security. ARES ’11, Washington: IEEE Computer Society: 2011: p. 722-727. https://www.cs.ox.ac.uk/files/4007/PID1871807.pdf, Accessed at 2014-10-23.

[Attr07]
Attrition Org: Partial Truths: A Guide to legally Covering Up a Data Loss Incident. Available at: http://attrition.org/security/rant/z/partialtruths.html, Accessed at: 2014-12-29.

[Aust11]

The Australian: Websites downed by Russian poll hack. The Australian, December 05, 2011.

[BaMy99]

Kakoli, Bandyopadhyay, Peter, P. Mykytyn, and Kathleen, Mykytyn: A framework for integrated risk management in information technology. Management Decision, Vol. 37, Iss 5, 1999, pp. 437 – 445.

[BaRi05]

Bahli, B. and Rivard, S.: Validating Measures of Information Technology Outsourcing Risk Factors. OMEGA, the international journal of Management Science, 33, 2005, pp. 175-187.

[Bask91]

Baskerville, R.: Risk analysis: an interpretive feasibility tool in justifying information systems security. School of Management, State University of New York, Binghamton, NY 13902-6000, USA, Received 10 January 1991; Accepted 7 February 1991.

[BCG10]

The Boston Consulting Group: Swimming Against the Tide: How Technology, Media, and Telecommunications Companies Can Prosper in the Economic Reality. http://www.bcg.com/documents/file69160.pdf, Accessed at 2014-10-13.

[Bel10]

Dr. Belovich, Steve G.: IT Security History & Architecture: How Did We Get Into This Mess?. Presented at 5/18/10. Available at: http://www.iqware.us/PDF_presentations/SecurityHistoryArticle2-4-2014.pdf, Accessed at 2014-10-31.

[BeLe72]

Belady LA and Lehman MM.: An Introduction to Growth Dynamics. Proc. Conf. on Statistical Comp. Perf. Evaluation, Brown Univ. 1971, Academic Press, 1972, W Freiberger (ed.), pp. 503 -511.

[Berg10]

Berg, Heinz-Peter: Risk Management: Procedures, Methods And Experiences. RT&A # 2(17), (Vol.1) 2010, June. Available at: http://ww.gnedenko-forum.org/Journal/2010/022010/RTA_2_2010-09.pdf, Accessed at 2014-12-15.

[Bern96]

Bernstein, Peter, L.: Against the Gods: The Remarkable Story of *Risk*, John Wiley & Sons, 1996.

[Bhav08]

Bhavya, Daya: Network Security: History, Importance, and Future. University of Florida, Department of Electrical and Computer Engineering, 26 August 2008. Available at: http://web.mit.edu/~bdaya/www/Network%20Security.pdf, Accessed at

2014-10-31.

[BlMc01]
Blakley, Bob, McDermott, Ellen and Geer, Dan: Information security is information risk management. Proceeding of the 2001 workshop on New Security Paradigms, ACM, New York, USA, 2001, pp. 97 – 104, doi: 10.1145/508171.508187.

[Bon01]
Bontis, Nick: Assessing knowledge assets: a review of the models used to measure intellectual capital. International Journal of Management Reviews, Vol. 3, Iss. 1, March 2001, pp.41-60, DOI: 10.1111/1468-2370.00053.

[Brod01]
Dr. Broderick, J.S.: Information security Risk Management – When Should It be Managed? Information Security Technical Report, Vol. 6, No. 3, 2001, pp. 12-18.

[CaGo03]
Campbell K, Gordon LA, Loeb MP, Zhou L.: The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Computer Security 2003, 11(3), pp. 431-448.

[CaLo89]
Caelli,William, Longley, Dennis and Shain, Michael: Infor-mation Security for Managers. Stockton Press, UK, 1989.

[CaMiRa04]
Cavusoglu H, Mishra B, Raghunathan S.: The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int J Electron Comm 2004;9(1):70e104.

[Car08]
Carey, L.: The evolution of computer virus and anti virus protection. Available at: http://www.identitytheftsecrets.com/the-evolution-of-computer-virusesand-anti-virus-p.html; Accessed at 2014-11-17.

[CCST14]
Committee on Commerce, Science, and Transportation: A “Kill Chain” Analysis of the 2013 Target Data Breach. http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf, Accessed at 2014-12-09.

[Chec13]
Check Point Software Technologies Ltd.: Check Point 2013 Security Report. Available at http://sc1.checkpoint.com/documents/security-report/files/assets/common/downloads/publication.pdf, Accessed at 2014-10-02.

[ChHo06]
Shuchih Ernest Chang and Chienta Bruce Ho: Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, Vol. 106, Iss. 3, 2006, pp. 345 – 361.

[Cisc14]
Cisco 2014: Annual Security Report. http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf, Accessed at 2014-12-20.

[ClAmGh14]
Clemens, M., Amina, K. and Ghada A-S.: Quantifying the Financial Impact of IT Security Breaches on Business Processes: A CPN-based approach. 2014 Twelfth Annual Conference on Privacy, Security and Trust (PST).

[CLUSIF09]
Club de la Securite de l'Information Français: Risk Management-Concepts and Methods. White paper, Methods Commission / Espace Méthodes, 2008/2009. Available at: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-risk-management.pdf, Accessed at 2014-12-18.

[Comf05]
Comfort, Louise, K.: Risk, Security and Disaster Management. Annu. Rev. Polit. Sci. 8, 2005, pp. 335-356, doi: 10.1146/annurev.polisci.8.081404.075608.

[Co-Mu03]
Conray-Murray A.: Strategies & issues: justifying security spending. Available at http://www.itarchitect.com/articles/NMG20020930S0002.html; 2003, Accessed at 2014-09-06.

[Cox08]
Cox, Louis, Anthony (Tony): Some Limitations of "Risk = Threat X Vulnerability X Consequence" for Risk Analysis of Terrorist Attacks. Risk Analysis, Vol. 28, No. 6, 2008, DOI: 10.1111/j.1539-6924.2008.01142.x

[Croc82]
Crockford, G.N.: The bibliography and history of risk management: Some preliminary observations. The Geneva Papers on Risk and Insurance 7, pp. 169-179, 1982.

[CSI11]
Computer Security Institute: 15th Annual 2010/2011 Computer Crime and security Survey. Available at http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf, Accessed at 2014-10-16.

[Damb10]

Damballa, Inc.: The Command Structure of the Aurora Botnet: History, Patterns and Findings. https://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf, Accessed at 2014-11-28.

[DelE13]

Deloitte and EMC^2: Irish Information Security and Cyber Survey 2013. Available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/cybercrime_survey_risk_2013_deloitte_ireland.pdf, Accessed at 2014-10-14.

[Denn98]

Denning, E.D.: Information warfare and security. United States of America: ACM Press, 1998.

[DHS05]

Department of Homeland Security, Office of Inspector General: Security Weaknesses Increase Risks to Critical Emergency Preparedness and response Database (Redacted). http://www.oig.dhs.gov/assets/Mgmt/OIGr_05-43_Sep05.pdf, Accessed at 2014-11-27.

[DHS09]

Department of Homeland Security: Cyber Threat to the United States, presentation fall 2009, DHS, DTA, HITRAC.

[DiEe85]

Dionne, G., Eeckhoudt, L.: Self-insurance, self-protection and increased risk aversion. Economics Letters 17, pp. 39-42, 1985.

[DiGe13]

Dionne, Georges: Risk Management: History, Definition and Critique (September 6, 2013). Available at SSRN: http://ssrn.com/abstract=2231635 or http://dx.doi.org/10.2139/ssrn.2231635, Accessed at 2014-10-31.

[Dion13]

Dionne, Georges: Risk Management: History, Definition and Critique. CIRRELT Interuniversity Research Centre on Enterprise Networks, Logics and Transportation, March 2013. Available at: https://www.cirrelt.ca/DocumentsTravail/CIRRELT-2013-17.pdf, Accessed at 2014-12-18.

[DiP-C05]

Dillon, Robin, L. and Paté-Cornell, Elisabeth, M.: Including Technical and Security Risks in the Management of Information Systems: A Programmatic Risk Management Model. Systems Engineering, Vol. 8, No. 1, 2005.

[DlEl08]

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M.: Information security: The moving target. Computers & security 28 (2009), pp.189-198 and Elsevier Ltd., 2008, doi:10.1016/j.cose.2008.11.007.

[DosS93]

Dos Santos BL, Peffers K, Mauer DC.: The impact of information technology investment announcements on the market value of the firm. Inf Syst Res 1993;4(1):1e23.

[Econ11]

The Economist: Too good to fail? New challenges for risk management in financial services. A report from the Economist Intelligence Unit, Sponsored by SAS, 2011.

[EMC^{2}13]

EMC Corporation and RSA: The Current State of Cybercrime 2013: An Inside Look at the Changing Threat Landscape. Available at: http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf, Accessed at 2014-11-17.

[EnBr2013]

Encyclopedia Britannica Online: Philosophy of science, 2013. Available at: http://www.britannica.com/EBchecked/topic/528804/philosophy-of-science, Accessed at 2014-10-21.

[ENISA06]

ENISA: Inventory of risk assessment and risk management methods, Version 1.0, 30 March 2006.

[EhBe72]

Ehrlich, J., Becker, G.,: Market insurance, self-insurance and self-protection. Journal of Political Economy 80, pp. 623-648, 1972.

[EtRi02]

Ettredge M, Richardson VJ.: Assessing the risk in e-commerce. In: Proceedings of the annual Hawaii International conference on System Sciences; 2002. pp. 194e194.

[EUPar13]

Europian Parliament: Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts. Directorate General for Internal Policies Policy Department A: Economic And Scientific Policy Industry, Research And Energy.

[FaLiFu04]

Farn, Kwo-Jean, Lin, Shu-Kuo and Fung, Andrew Ren-Wei: A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards & Interfaces 26, 2004, pp. 501-513.

[FaNa05]

Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp and Philip H. Enslow: A Management Perspective on Risk of Security Threats to Information Systems. Information Technology and Management 6, 2005, pp. 203–225.

[FiCa14]

Finkle, Jim and Humer Caroline: Community Health says data stolen in cyber attack from China. Reuters, August 18, 2014.

[Finn00]

Dr. Finne, Thomas: Information Systems Risk Management: Key Concepts and Business Processes. Computers & Security, 19, 2000, pp. 234-242.

[Fisc09]

Fischer, Urs: Risk IT: Based on COBIT. ISACA Guidance and Practices Committee. 2009, Available at: http://www.isaca.org/Knowledge-Center/Standards/Documents/Risk-IT Overview.ppt, Accessed at 2014-12-10 and http://www.isaca.org/Journal/Past-Issues/2009/Volume-5/Documents/jpdf0905-identify-govern.pdf, Accessed at 2014-10-13.

[Flin97]

Flin R.H.: Decision Making Under Stress: Emerging Themes and Applications. Aldershot, Hants, UK: Ashgate, 1997, p. 339.

[Galt10]

Galt Dubbs: Security Threat.
http://www.a-equals-a.com/uploads/3/4/2/4/342487/security_theater.pdf

[GaMc10]

Gatzlaff KM, McCullough KA.: The effect of data breaches on shareholder wealth. Risk manag insur rev 2010;13(1):61e83.

[Garg03]

Ashish, Garg ,Jeffrey, Curtis, Hilary, Halper: Quantifying the financial impact of IT security breaches. Information Management & Computer Security, Vol. 11 Iss 2 pp. 74 – 83.

[Geer11]

Kenneth Geers: STRATEGIC CYBER SECURITY. 2011 NATO Cooperative Cyber Defence of Excellence, Publicher CCD COE, Estonia.

[GeerD11]

Dan Geer, chief information security officer for IN-Q-Tel: Take Heed of Lockheed's Plight, ISSA meeting in Tampa, December 2011.

[GeKa02]

Gelbstein, E. and Kamal, A.: Information security: A survival guide to the uncharted territories of cyber-threats and cyber-security.
http://www.itu.int/wsis/docs/background/themes/security/information_insecurity_2ed.pdf, Accesses at 2014-09-01.

[Gelb06]

Gelbstein, E.: Information security for policy makers: what it means- why it matters- what to do about it? Available at: http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf; Accessed at 2014-10-06.

[GeSo01]

Gerber, Mariana and Rossouw von Solms: From Risk Analysis to security Requirements. Computer & Security, 20, 2001, pp. 577-584.

[GeSo05]

Gerber, Mariana and Rossouw von Solms: Management of risk in the information age. Computer & Security, 24, 2005, pp. 16-30.

[GoCoDr09]

Gorman, S., Cole, A. and Draezen, Y.: Computer spies breach fighter-jet project. Wall Street Journal, April 21, 2009.

[GoEk08]

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S. and Mück, T: Integration of an Ontological Information Security Concept in Risk-Aware Business Process Management. Proceedings of the 41st Hawaii International Conference on System Sciences, 2008.

[GoLoZh11]

Gordon LA, Loeb MP, Zhou L.: The impact of information security breaches: has there been a downward shift in costs? J Computer Security 2011;19(1): pp 33-56.

[Gorm09]

Gorman, S.: Electricity grid in US penetrated by spies. Wall Street Journal, April 8, 2009.

[GoSh09]

Goel, S. and Shawky, H.A.: Estimating the market impact of security breach announcements of firm values. J Info & Mang 2009: 46, pp. 404-410.

[HaNi03]

Harrington, S., Niehaus, G.R..: Risk Management and Insurance. Irwin/McGraw-Hill, USA, 2003.

[Heck05]

Heckman Rocky: Attackers Classification to Aid Targeting Critical Systems for Threat Modelling and Security Review. http://www.rockyh.net/papers/AttackerClassification.pdf, Accessed at 2014-09-10.

[Herz03]

Herzog, Peter V., ISECOM: OSSTMM 2.1: Open-Source Security Testing Methodology Manual. http://isecom.securenetltd.com/osstmm.en.2.1.pdf, Accessed 2014-09-20.

[HKMA03]
Hong Kong Monetary Authority: Supervisory Policy Manual, TM-G-1, General Principles for Technology Risk Management, V.1 – 24.06.03.

[HKSAR08]
The Government of the Hong Kong Special Administrative Region: An Overview of Information security Standards. http://www.infosec.gov.hk/english/technical/files/overview.pdf, Accessed at 2014-11-27.

[HoD'A03]
Hovav A, D'Arcy J.: The impact of denial-of-service attack announcements on the market value of firms. Risk management insurance rev 2003;6(2):97e121.

[HoD'A04]
Hovav A, D'Arcy J.: The impact of virus attack announcements on the market value of firms. Information System Security 2004;13(3):32e40.

[How14]
Howard, Philip, N.: Data Breaches in Europe: Reported Breaches of Compromised Persona; Records in Europe, 2005-2014. Center for Media, Data and Society, Working Paper 2014.1, School of Public Policy, Central European University, October 2014.

[Hub09]
Hubbard, Douglas, W.: The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons, 2009.

[Hump02]
Humphreys, Edward: Information Security Risk Management: Handbook for ISO/IEC 27001. http://shop.bsigroup.com/upload/Standards%20&%20Publications/publications/BIP0076-Chapter1.pdf, Accessed at 2014-11-24.

[Hump11]
Humphreys, Edward: Information security management system standards. Datenschutz und Datensicherheit - DuD 35 (1), 8 March 2011, pp. 7–11. doi:10.1007/s11623-011-0004-3.

[HuMyK-M12]
Humayum, Z., Myung, S.K. and Kweku-Muata, O-B.: Financial Impact of Information security Breaches and Breached Firms and their Non-Breached Competitors, WP # 0015IS-299-2012, University of Texas at San Antonio, 2012.

[Hutc12]
Hutchings, Alice, Australian Government, Australian Institute of Criminology: Computer security threats faced by small businesses in Australia. Trends & issues: in crime and criminal justice, No. 433, February 2012. Accessed at:
http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi433.pdf,

Accessed at 2014-10-07.

[IDT]
International Center for Invincible Defense: Invincible Defense Technology. http://www.invincibledefense.org/technology.html, Accessed at 2014-09-04.

[III14]
Insurance Information Institute, Hartwig, Robert P.: Cyber Risks: The Growing Threat. Available at: http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf, Accessed at 2014-12-20.

[ISACA14]
ISACA, Sanchez, Jeffrey: Prevention of Data Breach. ISACA's North America, ISRM Conference 2014.

[Jam13]
James A. Lewis: Raising the bar for Cybersecurity. , CSIS, Center for Strategic & International Studies, Technology & Public Policy, 12 February, 2013. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, Accessed at 2014-10-14.

[Jun99]
Jung C, Han I and Suh B.: Risk analysis for electronic commerce using case-based reasoning. John Wiley & Sons, Ltd, International Journal of Intelligent Systems in Accounting, Finance & Management 8, 1999, pp. 61-73.

[Kam14]
Kamala, Harris, D.: California Data Breach Report. Attorney General, California Department of Justice, October 2014. Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf, Accessed at 2014-11-26.

[Kasp13]
Kaspersky Lab.: Global Corporate IT Security Risks: 2013. Available at http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf, Accessed at 2014-10-15.

[Kers12]
Kersteman, Wouter: Security Management System's Usability Key to Easy Adoption. http://us.sourcesecurity.com/news/articles/co-4108-ga.8554.html, Accessed at 2014-08-22.

[Kle93]
Klein, G.A.: A recognition primed decision making (RPD) model of rapid decision making: In Decision Making in Action: Models and Methods, ed. G Klein, J Orasanu, R Calderwood, CE Zsambok, Norwood, NJ: Ablex, 1993, pp 138–147.

[Knig21]

Knight, F. H.: Risk, Uncertainty, and Profit. Boston: Hart, Schaffner & Marx, 1921.

[Kum11]

Kumar, Mohit: Coca-Cola Norway Hacked by Greek Hacking Scene (GHS). The Hacker News, 07 December, 2011. Available at: http://thehackernews.com/2011/12/coca-cola-norway-hacked-by-greek.html, Accessed at 2014-11-17.

[Lad02]

Ladyman, James: Understanding Philosophy of Science. Taylor & Francis Group, e-Liabrary, 2002. Available at: http://srbiau.ac.ir/Files/Ladyman,%20Understanding%20Philosophy%20of%20Science.pdf, Accessed at 2014-09-16.

[LaWa14]

Layton, R. and Watters, P.A.: A methodology for estimating the tangible cost of data breaches. J Inf Sec and Applications 2014:19, pp.321-330.

[Lew13]

Lewis, James, A.: Raising the Bar for Cybersecurity. CSIS, Center for Strategic & International Studies, Technology & Public Policy, 12 February, 2013. Available at: http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, Accessed at 2014-10-14.

[Litt63]

Émile Maximilien Paul Littré: Dictionnaire de la langue française ("Le Littré"), 1863–1873.

[LoMa92]

Loderer CF, Mauer DC.: Corporate dividends and seasoned equity issues: an empirical investigation. J Financ 1992;47(1):201e25.

[Loud02]

Loudon T.V: Geoscience after IT: Part A. Defining Information Technology, its significance in geoscience, and the aims of this publication. Available at: http://core.ac.uk/download/pdf/63429.pdf, Accessed at 2014-11-13.

[Lyyt90]

Lyytinen, Kalle: Information Systems and Critical Theory: A Critical Assessment, University of Jyväskylä, Department of Computer Science,Working Paper WP-13, July 1990.

[Mand14]

Mandiant: Beyond the Breach. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf, Accessed at 2014-12-19.

[MAS13]
Monetary authority of Singapore: Technology Risk Management Guidelines, Lune 2013.

[McAL13]
McAfee Labs Report: 2013 Threats predictions. http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf, Accessed 2014-09-26.

[Meez12]
Mezzofiore, Gianluca: Teampoison Hackers 'Phone Bomb' MI6 over Terror Detentions. IBTimes, 12 April, 2012. Available at http://www.ibtimes.co.uk/teamp0ison-phone-bombs-m16-agents-anonymous-hackers-327090, Accessed at 2014-10-06.

[MeHe63]
Mehr, R.I., Hedges B.A.: Risk Management in the Business Enterprise. Irwin, Homewood, Illinois, 1963.

[MeHu12]
Mekovec, R. and Hutinski, Ž: The role of perceived privacy and perceived security in online market. https://bib.irb.hr/datoteka/583343.Rad.pdf, Accessed at 2014-09-24.

[Meun07]
Meunier Pascal: Classes of Vulnerabilities and Attacks. http://homes.cerias.purdue.edu/~pmeunier/aboutme/classes_vulnerabilities.pdf, Accessed at 2014-11-20.

[Micr11]
Microsoft Corporation: Microsoft Security Intelligence Report: Global Threat Assessments for 117 countries/regions. Microsoft, 2011.

[MOD10]
Ministry of Defence, UK: strategic Trends programme: Global Strategic Trends – Out to 2040. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33717/GST4_v9_Feb10.pdf, Accessed at 2014-10-06.

[MOD14]
Ministry of Defence, UK: strategic Trends programme: Global Strategic Trends – Out to 2045. Available at: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2014/Global_Strategic_Trends_-_Out_to_2045.pdf, Accessed at 2014-11-25.

[Nav12]
Navigant: Information Security & Data Breach Report. April 2012. Available at: http://www.privacyandsecuritymatters.com/files/2012/05/Navigant.pdf, Accessed at 2014-10-08.

[Naz09]

Nazario, Jose, Arbor Networks: Politically motivated Denial of Service Attacks. Cryptology and Information Security Series, Ebook: The Virtual Battlefield: Perspectives on Cyber Warfare, V.3, pp.163-181, 2009.

[NIST13]

NISTIR 7298, Revision 2: Glossary of Key Information Security Terms. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, Accessed at 2014-09-23.

[NIST11]

National Institute of Standards and Technology, U.S. Department of Commerce: Information Security. Computer Security Division, Information Technology Laboratory, Gaithersburg, MD 20899-8930, September 2011.

[NIST98]

National Institute of Standards and Technology: Special Publication 800-18.Guide For Developing Security Plans for Information Technology Systems. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

[NSBA13]

National Small Businesses Association: 2013 Small Business Technology Survey.
http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey2013.pdf, Accessed at 2014-11-17.

[Orm03]

Ormerod, Paul: Sunday times article. Available at: http://www.paulormerod.com/current.html; 2003, Accessed at 2014-08-11.

[Owen98]

Owens S.: Information security management: an introduction. British Standards Institution, London, 1998.

[OxEnDic89]

Simpson, J.A. and Weiner, E.C.S.: Oxford English Dictionary. Oxford: Clarendon Press, Oxford, New York, Oxford University Press, 1989.

[Pass12]

Passeri, Paolo: Timeline of Cyber War Between Bangladesh and India (PartII). Hackmageddon, 26 March, 2012. Available at http://hackmageddon.com/tag/indishell/, Accessed at 2014-10-06.

[Pat10]

Patel N.: The effect of it hack announcements on the market value of publicly traded corporations. Duke J Econ 22 (2010).

[PDA12]

Parental Drug Association: An Incomplete History of Risk Management. https://store.pda.org/TableOfContents/Risk_Assessment_Ch01.pdf, Accessed at 2014-10-31.

[PIAC12]
Public Interest Advocacy Centre, Lawford, J. and Lo, J.: Data Breaches: Worth Noticing?. PIAC, Suite 1204, Ottawa, Ontario, ISBN 1-895060-63-X.

[PiMePa14]
Pirounias, S., Mermigas, D., and Patsakis, C.: The relation between information security events and firm market value, empiricall evidence on recent disclosures: An extension of the GLZ study. J Inf Sec and Applications 2014:19, pp. 257-271.

[PoDe09]
Pourquery, Pierre and De Mulder, Johan: Operational Risk management: Too Important to Fail. The Boston Consulting Group, February 2009.

[Pon12]
Ponemon Institute LLC: Aftermath of a Data Breach Study. http://www.experian.com/assets/data-breach/brochures/ponemon-aftermath-study.pdf, Accessed at 2014-12-20.

[Pon13a]
Ponemon Institute LLC: The Post breach Boom. http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf, Accessed at 2014-10-10.

[Pon13b]
Ponemon Institute LLC: Is Your Company Ready for a big Data Breach? http://www.experian.com/assets/data-breach/brochures/databreach-preparedness-study-v3.pdf, Accessed at 2014-12-15.

[Pon13c]
Ponemon Institute LLC: 2013 Cost of Data Breach Study: Global Analysis. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf, Accessed at 2014-12-19.

[Pon14]
Ponemon Institute LLC: 2014 Cost of data Breach Study: United States. Available at: http://essextec.com/sites/default/files/2014%20Cost%20of%20Data%20Breach%20Study.PDF, Accesses at 2014-12-27.

[Popp05]
Popper, Karl: The Logic of Scientific Discovery. Logik der Forschung, first published 1935 by Verlag von Julius Springer, Vienna, Austria, Taylor & Francis Group e-Liabrary, 2005. Available at: http://strangebeautiful.com/other-texts/popper-logic-scientific-discovery.pdf, Accessed at 2014-12-04.

[PWC10]
PricewaterhouseCoopers: Information Security Breaches Survey 2010: technical report. Available at: http://pwc.blogs.com/files/isbs-2010-report-final.pdf, Accessed at 2014-10-27.

[PWC13]
PricewaterhouseCoopers: 2013 Information Security Breaches Survey: technical report. https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf, Accessed at 2014-10-20.

[PWC14a]
PricewaterhouseCoopers: US cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey. Available at: http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf, Accessed at 2014-11-14.

[PWC14b]
PricewaterhouseCoopers: 2014 Information Security Breaches Survey. http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf, Accessed at 2014-12-19.

[Räm11]
Rämänen, Jussi: Perceived security in mobile authentication. Master's Thesis, Aalto University, School of Electrical Engineering, Espoo, August 23, 2011.

[RaSn91]
Rex Kelly Rainer, Jr., Charles A. Snyder and Houston H. Carr: Journal of Management Information Systems, Vol. 8, No. 1 (Summer, 1991), pp. 129-147 Published by: M.E. Sharpe, Inc., Article Stable URL: http://www.jstor.org/stable/40397977, Accessed at 2014-12-17.

[Raym00]
Raymond, Jean-François: Traffic Analysis: Protocols, attacks, design issues and Open Problems. http://freehaven.net/anonbib/cache/raymond00.pdf, Accessed at 2014-09-10.

[RBS12]
Risk Based Security, Inc.: Data Breach QuickView: An Executive's Guide to data Breach Trends in 2012. https://www.riskbasedsecurity.com/reports/2012-DataBreachQuickView.pdf, Accessed at 2014-10-08.

[Renn85]
Renn, Ortwin: Risk analysis: scope and limitations. Regulating industrial risks : science, hazards and public protection. London : Butterworths, 1985. - ISBN 0-408-00740-0. Available at: http://elib.uni-stuttgart.de/opus/volltexte/2010/5479/, Accessed at 2015-01-07.

[Riz14]
Rizomiliotis, Panagiotis: Cryptography Lecture 1. Info-Sec-Lab. Available at https://evdoxos.ds.unipi.gr/modules/document/file.php/TEMSEC142/Lectures%202014-2015/Lecture_1_crypto_papei.pdf, Accessed at 2014-11-12.

[Roma14]
Roman, Jeffrey: Top Data Breaches of 2014 Infographic: Lessons Learned from Year's Top Incidents. DataBreach Today, December 30, 2014.

[RoSc04]
Rosenberg, Joshua, V. and Schuermann, Til: A General Approach to Integrated Risk Management with Skewed, Fat-Tailed Risks. Federal Reserve Bank of New York Staff Reports, no. 185, May 2004.

[Ross99]
Rossouw von Solms: Information security management: why standards are important, Information Management & Computer Security, Vol. 7, Iss 1, 2009, pp. 50-58.

[RuGa91]
Rusell, D., Gangemi, G.T.: Computer security basics. United States of America: O'Reilly & Associates, Inc.; 1991.

[RyJe03]
Julie J.C.H Ryan and Theresa I. Jefferson: The Use, Misuse, And Abuse Of Statistics In Information Security Research. The George Washington University. Available at: http://attrition.org/archive/misc/use_misuse_abuse_stats_infosec_research.pdf, Accessed at 2014-10-09.

[SaAl11]
Saleh, Mohamed, S. and Alfantookh, Abdulkader: A new comprehensive framework for enterprise information security risk management. Applied Computing & Informatics, 6 June 2011, doi:10.1016/j.aci.2011.05.002.

[Sal98]
Salus, Peter: Net Insecurity: Then and Now (1969–1998). Sane '98 Online. 19 November 1998. Available at www.nluug.nl/events/sane98/aftermath/salus.html, Accessed at 2014-09-16.

[SaNe13]
SafeNet: A New Security Reality: The Security Breach. Available at http://www2.safenet-inc.com/securethebreach/downloads/secure_the_breach_manifesto.pdf, Accessed at 2014-10-25.

[SANS02]
SANs Institute, Chan Tuck Wai: Conducting a Penetration Test on an Organization. SANS Institute InfoSec Reading Room, 2002.

[SANS06]
SANS Analyst Program, Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R. and Mancini, S.: Penetration Testing: Assessing Your Overall security Before Attackers Do. SANS Institute InfoSec Reading Room, June 2006.

[Sch14]
Schneiderman, Eric, T.: New York State Attorney General: Information Exposed: Historical Examination of Data breaches in New York State. Available at: http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf, Accessed at 2014-10-17.

[Schn99]
Schneier, Bruce: Attack Trees: Modeling security threats. *Dr. Dobb's Journal of Software Tools 24*, 12, December 1999, pp. 21-29. Available at: https://www.schneier.com/paper-attacktrees-ddj-ft.html, Accessed at 2014-11-08.

[Schn07]
Schneier, Bruce: In Praise of Security Theater. Schneier on Security, 25 January 2007. https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html, Accessed at 2014-09-15.

[Schw12]
Schwartz, Mathew J.: Anonymous-Based attacks Took Nasdaq Website Offline. InformationWeek, DarkReading, February 16, 2012.

[Schw14]
Schwartz, Mathew J.: Sony Hack: More Theories Emerge: Additional Evidence Suggests Insiders, Hacktivists. DataBreach Today, December 30, 2014.

[SeHo05]
Seacord, Robert C.; Householder, Allen D.: A Structured Approach to Classifying Security Vulnerabilities. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2005_004_001_14474.pdf, Accessed at 2014-11-13.

[ShWa07]
Shenkir, W.G. and Walker, P.L.: Enterprise Risk Management: Tools and Techniques for effective implementation. http://www.stjohns.edu/sites/default/files/documents/academics/tobin/enterprise_tools_and_techniques.pdf, Accessed at 2014-08-22.

[SiWi09]
Siponen, Mikko and Willison, Robert: Information security management standards: Problems and solutions. Information & Managemnt 46, 2009, pp. 267-270.

[Slov99]
Slovic, Paul: Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. Risk Analysis, Vol.19, No. 4, 1999, pp.689-701.

[Snee14]

Sneed, Harry, M.: Software Engineering I - Software Project Management for Wirtschaftsinformatiker. Lecture discussions 2014-2015, Universität Regensburg, Lehrstuhl für Wirtschaftsinformatik I.

[Soph13]

Sophos: Security Threat Report 2013: Neue Plattformen und sich wandelnde Bedrohungen. http://www.sophos.com/de-de/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf, Accessed at 2014-10-14.

[Soph14]

Sophos: Security Threat Report 2014: Smarter, Shadier, Stealthier Malware. https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf, Accessed at 2014-10-01.

[SpBa10]

Spears, Janine, L. and Barki, Henri: User Participation in Information Systems Security Risk Management. MIS Quarterly, Vol. 34, No. 3, September 2010, pp. 503-522.

[SSE99]

SSE-CMM,: Model description Document, Version2.0. Available at: http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/SSAIRBSP/SSECMMv2Final.pdf, Accessed at 2014-12-17.

[SSI13]

Space Security Index: Space Security Index 2013: Executive Summary. http://swfound.org/media/109727/SSI_Executive_Summary_2013.pdf, Accessed at 2014-11-03.

[StGoFe02]

Stoneburner, Gary; Goguen, Alice; and Feringa, Alexis: Risk management Guide for Information Technology Systems. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf, Accessed at 2014-11-24.

[Stol00]

Stoll, C.: The cuckoo’s egg: tracking a spy through the maze of computer espionage. United States of America: Pocket; 1st edition, 2000.

[Str11]

Stroie Elena Ramona: Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. Chinese Business Review, ISSN 1537-1506, December 2011, Vol. 10, No. 12, 1106-1110.

[Stul08]

Stulz, René, M.: Risk Management Failures: What Are They and When Do They Happen? Journal of Applied Corporate Finance, Vol. 20, Iss. 4, 16 December 2008, pp. 39-48.

[Suby13]

Suby, Michael, (ISC)²®, The (ISC)² Foundation, Booz Allen Hamilton and Frost & Sullivan: The 2013 (ISC)^2 Global Information Security Workforce Study. Available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf, Accessed 2014-11-15.

[Symn14]

Symantec Corp.: Internet Security Threat Report 2014, Trends, Volume 19, published April 2014. https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, Accessed at 2014-10-01.

[Teh14]

Tehan, Rita, Congressional Research Service: Cybersecurity: Authoritative Reports and Resources, by Topic, 14 October, 2014. Available at: https://www.fas.org/sgp/crs/misc/R42507.pdf, Accessed at 2014-10-13.

[TeAs10]

Teymouri, Maryam and Ashoori, Maryan: The impact of information technology on risk management. Procedia Computer Science 3 (2011), pp. 1602-1608. Published by Elsevier Ltd., doi:10.1016/j.procs.2011.01.056

[Toh11]

Tohidi, Hamid: The Role of Risk Management in IT systems of organizations. Procedia Computer Science 3, 2011, pp.881-887.

[trc14]

Identity Theft Resource Center: Data Breach Category Summary. IDT911, trc, 14 October 2014.

[Trus13]

Trustwave: 2013 Global Security Report. Available at: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf, Accessed at 2014-10-07.

[UKG12]

United Kingdom Government: 10 Steps to Cyber Security. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf, Accessed at 2014-10-14.

[UMB12]

Umbrella: Evolving IT Security Strategies in a World of Growing Breadth. http://info.umbrella.com/rs/opendns/images/WP-Umbrella-Defense-in-Breadth.pdf, Accessed at 2014-09-04.

[Ver13]

Verizone: 2013 Data Breach Investigations Report. Available at: http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf, Accessed at 2014-10-17.

[WeSaRo09]
Wei Ming Khoo, Saad Aloteibi and Ross Anderson: Hunting the vulnerabilities in large software: the OpenOffice suite. http://www.cl.cam.ac.uk/~wmk26/openoffice/openoffice9.pdf, Accessed at 2014-08-22.

[Vaas12]
Vaas, Lisa: Hackers snatch $6.7m in South African cyber bank robbery. NakedSecurity, January 20, 2012.

[Ver12]
Verizon: 2012 Data Breach Investigations Report. Available at http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf, Accessed at 2014-10-17.

[Ver14]
Verizon: 2014 Data Breach Investigations Report. Available at: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf, Accessed at 2014-11-27.

[Wake14]
Wakefield, Jane: eBay faces investigations over massive data breach. BBC News, May 23, 2014.

[Wang10]
Wang, Victoria: Facts of Figures – Technological System Crime. Available at: http://hocc.swansea.ac.uk/system/files/Technological%20System%20Crime.pdf, Accessed at 2014-10-07.

[Ware79]
Ware. Willis: Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. Rand Online. 10 October 1979. Available at www.rand.org/pubs/reports/R609-1/R609.1.html, Accessed at 2014-11-22.

[WiHe64]
Williams, A., Heins M.H.: Risk Management and Insurance. McGraw Hill, New York, 1964.

[WiHe95]
Williams A., Heins M.H.: Risk Management and Insurance. McGraw-Hill, New York, 1995.

[Wiki14]
Wikipedia: Data breach. Available at: http://en.wikipedia.org/wiki/Data_breach, Accessed at 2014-11-13.

[WSec13]

WhiteHat Security: Website security Statistics Report, May 2013. Available at: https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf, Accessed at 2014-10-16.

[YaHu11]

Yayla AA, Hu Q.: The impact of information security events on the stock value of firms: the effect of contingency factors. J Inf Tech 2011;26(1):60e77.

[YaYu13]

Yan (Lindsay) Sun and Yuhong Liu: Security of Online Reputation Systems: Evolution of Attack and Defenses. Department of Electrical, Computer and Biometrical Engineering, University of Rhode Island. IEEE Transactions on Information Forensics and Security, special issue on Privacy and Trust Management in Cloud and Distributed Systems, Vol 8, No. 6, pp.936-948, June 2013. http://egr.uri.edu/wp-uploads/nestlab/Security-of-Online-Reputation-Systems-Evolution-of-Attacks-and-Defenses.pdf, Accessed at 2014-10-13.

[Yong13]

Yong Ed: Chinese project probes the genetics of genius**:** Bid to unravel the secrets of brainpower faces scepticism. Nature, 14 May 2013.

Affirmation

I hereby affirm that I have written the submitted master thesis in all parts on my own. Cited sources of literature are perceptibly marked where fragments of text have been used and are also listed at the end of this thesis. Regarding the parts that are in quotation marks are those taken as in the original source which is mentioned in all cases. To the best of my knowledge, I have not used parts of text from sources that are not included.

Regensburg, 26 February 2015

Myrsini Athinaiou
Martikelnummer (University of Regensburg): 1718030
Student Number (University of Piraeus): mte1301