



INTERNATIONAL
HELLENIC
UNIVERSITY

Calculation, Insurance and Risk Management for Data Breaches

Patias Emmanouil - Panagiotis

SID: 3301130020

Supervisor: Prof. Vasilis Katos

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

DECEMBER 2015

THESSALONIKI – GREECE

Abstract

Nowadays, information exchange, in any format, is a main process which takes place worldwide, especially due to the abrupt spread of the Internet Billions of Internet users (physical or virtual users) share their information via a chaotic grid, in which information may be transferred through numerous and various distinguished parts such as computers, servers, optical or coax cables, satellites etc. until it reaches the final destination. Information can be stored on a local computer or on a server and be exchanged among network users. It is obvious that we are going to deal with the information protection which is processed, transmitted among users and stored in digital format. This practice of defending information is called Information Security, and incidents where information is stolen by an unauthorized user or system are called Data Breaches, and more often the victims are companies and organizations. The attackers target sensitive and private data that can be valuable or their infringement can cause reputation and operation issues to the organization or company.

As a result, a vital necessity for every organization that stores and processes sensitive or private data is to conduct research about countermeasures that can protect and ensure its overall business operation. However, there are many ambiguous and murky points when an organization does market research or wonders about the security level within the organization and the overall protection that the organization offers with respect to data that it possesses. For that reason, a web application is required, which will advise a company owner or a security manager and will help him or her to clarify all these grey areas about the necessity or not of continuous, dedicated and increasing Information Security policies which would lead to the development of a Data Breach security product whose aim is to maximize an organization's existing security and its confidence.

Also, at this point I would like to thank my supervisor, Professor Vasilis Katos, for his guidance and advice he has provided throughout this dissertation project.

Patias Emmanouil - Panagiotis

8/12/2015

Contents

ABSTRACT	II
CONTENTS	V
1 INTRODUCTION.....	9
2 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS).....	10
2.1 ISMS FRAMEWORK / ISO STANDARDS FOR IT.....	11
2.1.1 <i>ISMS Framework</i>	13
2.1.2 <i>ISO standards for IT</i>	14
2.2 USEFULNESS OF AN ISMS MANAGEMENT.....	16
2.2.1 <i>Management Principles</i>	17
2.2.2 <i>IT: Continuous Development and Maintenance</i>	19
2.2.3 WAYS TO DEPLOY AND IMPROVE SECURE BUSINESS NETWORKS.....	19
2.3 PDCA MODEL FOR ISMS.	23
3 DATA BREACHES AND CYBERSECURITY.....	24
3.1 WHAT DATA BREACH IS AND ITS EFFECTS.....	25
3.2 DATA BREACH – THREAT AGENTS	25
3.2.1 <i>External Factors</i>	26
3.2.2 <i>Internal Factors</i>	27
3.2.3 <i>Partners</i>	28
3.2.4 <i>Threat actions and Hacking Methods</i>	28
3.3 INCOMPLETE DATA SECURITY / COMMON PITFALLS	30
3.4 DISCOVERING A DATA BREACH.....	31
3.4.1 <i>Things that uncover security problems</i>	31
3.4.2 <i>Immediate and Necessary Actions</i>	32
3.4.3 <i>Averting Future Data Breaches</i>	32
3.5 CYBER SECURITY	33
3.5.1 <i>Cybercrime</i>	34

3.5.2	<i>On-line Privacy</i>	35
3.6	DIFFERENCES BETWEEN CYBER SECURITY AND INFORMATION ASSURANCE	37
4	RISK MANAGEMENT – RISK ASSESSMENT	38
4.1	RISK ASSESSMENT – DEFINITION	38
4.2	EFFICIENT RISK ASSESSMENT FUNDAMENTALS	39
4.3	RISK ASSESSMENT CASE STUDY: <i>COMPUTER SOFTWARE COMPANY</i>	40
4.3.1	<i>Stage 1: Commencement</i>	42
4.3.2	<i>Stage 2: Operation and documentation</i>	42
4.3.3	<i>Stage 3: Collecting Data</i>	43
4.3.4	<i>Stage 4: Analysis</i>	43
4.3.5	<i>Stage 5: Final report and assurance that pre-agreed actions are applied</i>	44
4.4	RISK MANAGEMENT: <i>DEFINITION</i>	44
4.4.1	<i>Risk Management Cycle</i>	45
4.4.2	<i>Risk Management: Privacy</i>	46
5	CYBER INSURANCE	47
5.1	CYBER INSURANCE IN GREECE: <i>PERSPECTIVES</i>	48
5.2	SECURITY LIMITATIONS – BLACK MARKET GROWTH	50
5.3	CYBER INSURANCE: <i>EVOLUTION</i>	53
5.4	DATA PRIVACY AND DATA PROTECTION IN GREECE	54
6	DB.EST (DATA BREACH ESTIMATION TOOL)	60
6.1	APPLICATION PRESENTATION	60
6.1.1	<i>Data Breach: probability/risk estimation</i>	61
6.1.2	<i>Data Breach Recovery Cost Calculation</i>	61
6.2	DEMPSTER – SHAFER THEORY	62
6.2.1	<i>Application of the Dempster - Shafer theory to the Data Breach estimation</i>	63
6.2.2	<i>Dempster – Shafer Scenarios / Validation</i>	66
7	CONCLUSION	77

BIBLIOGRAPHY.....	799
APPENDIX: DB.EST.....	80

1 Introduction

This study assesses the impact of Data Breaches on vital business operations and investigates the role of Information Security Management System (ISMS) in Cyber-attack prevention and avoidance. Hence, any procedure and technique that is followed in order to protect information and information systems in general against unauthorized access or modification of information, whether in storage, processing, or transit, and against Denial of Service (DoS) to authorized users, is called Information Security.

This dissertation has three aims: first to present the severity of Data Breaches; second to highlight the necessity for strict Information Security policy and guidance for organizations and businesses; and third, an attempt to estimate the probability of Data Breach events alongside with Recovery Cost for organizations, based on existing security policies. By taking into consideration the fundamental principles of Information Security we try to depict current patterns and types of Cybercrime and also introduce the Online Privacy, which each user should demand and ensure not only during information exchange but also throughout its storage and processing.

Moreover, it's main objective is to clarify the demanding and time consuming required process followed in order to discover, comprehend and decide about the best ways to confront Data Breaches. Thus, by following world-wide Data Breach Investigation reports and Cost of Data Breach studies (Global analysis), we try to provide a tool that offers Data Breach probability estimation as well as Recovery Cost in case of a breach incident by using the data of those studies. Through this application (tool), the user can also learn how each action with respect to information security affects the risk management as well as the size of the risk by answering the specific questions.

In addition, we will analyze and evaluate Risk Assessment and Risk Management procedures and their great contribution to the overall protection and assurance of business operations. Subsequently, an extensive reference is made to an emerging business type: Cyber Insurance, with a particular emphasis on the Greek market prospects but also on

the Black Market of private data and respective legislations. Furthermore, synthesizing the Dempster – Shafer theory of combining evidence, this research analyzes and illustrates and tests the variations of the probability of combined Data Breach events. To validate this theory, three scenarios were created and used as case studies to show how security countermeasures reflect on several Data Breach types. The findings of the research suggest that the effect of staff training, familiarity and reconciliation with Information Security aspects can significantly reduce major Cyber-attack risks as well as the possibility of suffering any type of breach. Theoretical contribution and services of Cyber-Insurance inclusion are also discussed by presenting its main benefits.

Initially, Chapter 2 presents the ISMS Framework and the ISO Standards for Information technology, which is followed by the introduction into the Data Breaches and Cybersecurity with simultaneous analysis of the potential threats and how to avert them in Chapter 3. Subsequently, there is a detailed report about Risk Management and Risk Assessment by presenting a case study in order to highlight their importance in the overall security of an organization. Chapter 5 introduces the term of Cyber Insurance, showing the operating procedures and its prospects in the Greek market and finally in Chapter 6 we use the theory of combining evidence in order to develop an innovative way to estimate the probability of an organization or company suffering a Data Breach event

2 Information Security Management System (ISMS)

Information Security Management System (ISMS) is a significant component of the overall organization's protection and organization's management system. In order to be successful, the ISMS has to plan, implement, operate, supervise, review, maintain and improve Information Security within an organization. Practically, ISMS is the part of the management system which deals with the Information Security issues.

The formation and the implementation of an ISMS for an organization, requests an analytic and detailed way, from which the needs and the detailed strategic and business

goals will emerge. In that way, we can create an integrated ISMS which meets all the important security requirements.

ISMS includes the following fundamental components:

- Management principles
- Resources
- Staff
- Information security process

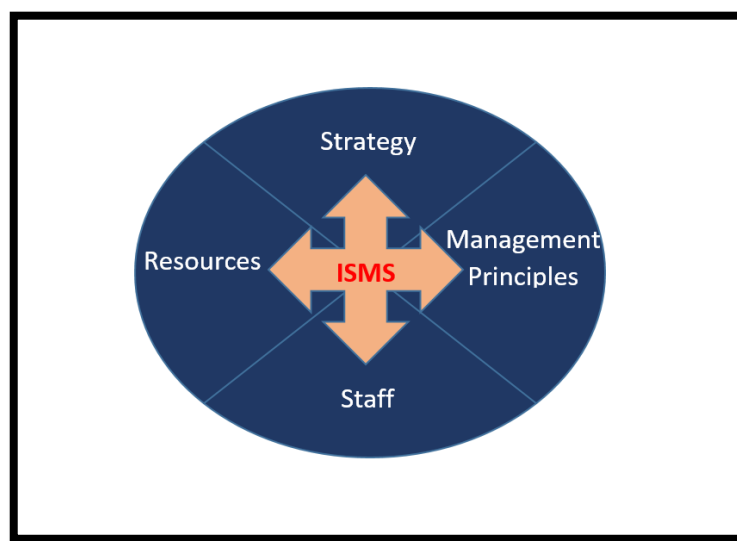


Figure 1: Information Security Management System (ISMS) components.

2.1 ISMS Framework / ISO standards for IT

To start with, we should mention that the overall formation and acceptance of an Information Security Management System (ISMS) constitutes one of the most important strategic issues for an organization. Each organization has to develop and implement an ISMS according to its needs and the future business ambitions. Considering the kind of data and all the security factors, the organization must adopt an adequate ISMS which will provide trust to the users. This can be achieved by applying Security policies, standards and procedures (PSPs) which is the backbone of any stable ISMS. Although

PSPs are the most basic elements of an ISMS, they are also one of the most challenging for many organizations to implement them in an effective way. Therefore, to ensure the effectiveness of ISMS, organizations follow a framework and a structured approach to develop and implement the IT security system.

The main objective of Information Security Management is to apply the most appropriate practices in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In this way, Information Security Management will enable implementing the desirable qualitative characteristics of the services offered by the organization, for instance, availability of services, preservation of data confidentiality and integrity etc. The most significant factors that dictate the security level of the organization is not only its size on itself, but the kind of business and sensitivity of data. These are the factors which determine the security requirements and levels of an organization on a legal, physical and operational level. It is obvious that small businesses with limited IT infrastructure, whose operation does not demand storage and/or processing of personal or confidential data, usually face minor risks or risks with lower likelihood or impact. These organizations are less likely to maintain independent ISMS and usually deal with information security risks ad-hoc or as part of a wider Risk Management process.

On the other hand, larger organizations and organizations such as banks and financial institutes, telecommunication operators, hospital and health institutes and public or governmental bodies have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmost attention and priority to information security risks. So, we conclude that the development and implementation of a separate and independent management process, namely an Information Security Management System, is the one and only alternative [1].

2.1.1 ISMS Framework

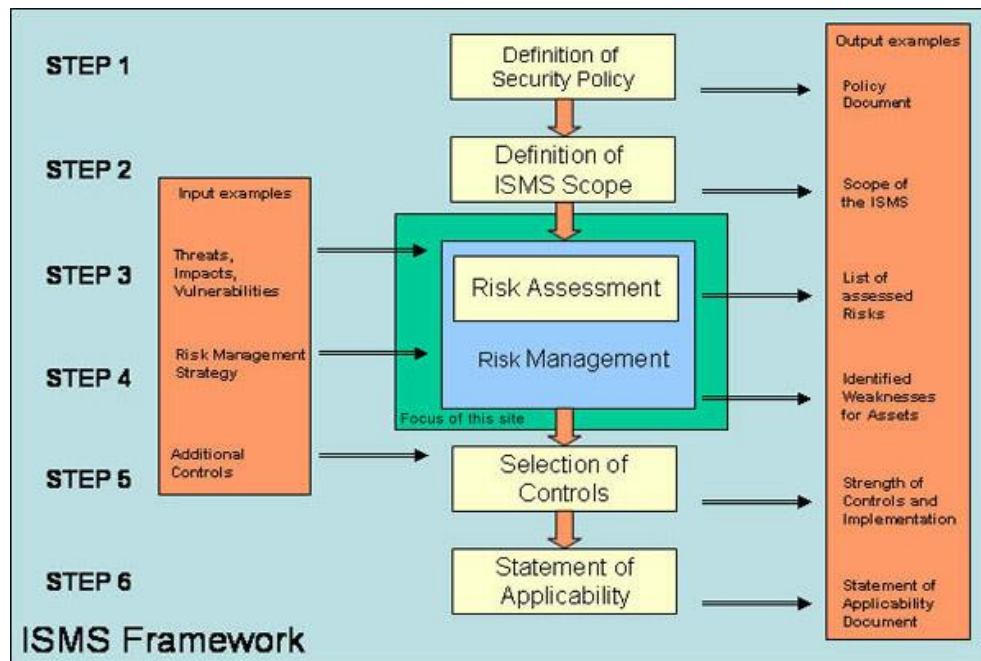


Figure 2: The steps of process development of the information security management system. (source: <http://www.enisa.europa.eu>)

The above figure represents the ISMS framework and the six (6) required steps [1]. These steps are:

- Step 1: Definition of Security Policy,
- Step 2: Definition of ISMS Scope,
- Step 3: Risk Assessment (as part of Risk Management),
- Step 4: Risk Management,
- Step 5: Selection of Appropriate Controls and
- Step 6: Statement of Applicability

Steps 3 and 4 (Risk Assessment and Management process), comprise the heart of the ISMS. These processes are the guidelines of security policy and the targets also. On the other to transform objectives of ISMS into specific plans for the implementation of controls and mechanisms that aim at minimizing threats and vulnerabilities. It is worth

mentioning that steps 3 and 4 are considered as a single entity, namely Risk Management, wherein we will extensively analyze in Chapter 3.

2.1.2 ISO standards for IT

To achieve the appropriate control levels an organization should follow some security standards that include sets of control mechanisms. The optimum option is to adopt some security standards (e.g. ISO 1779), the characteristics and the guidelines that each ISO dictates.

Many standards have been developed in order to emphasize the most important subject areas that organizations or government agencies must pay attention to. Below are presented the most important IT standards and break down their key features.

The most important standards are [2]:

- *ISO 13335*

The ISO 13335 standard "Management of Information and Communications Technology Security" is a general guide for initiating and implementing the IT security management process. It provides instructions but no solutions for managing IT security. The standard is a fundamental work in this area and is the starting point or reference point for a whole series of documents on IT security management. The standard currently comprises the following parts:

- Part 1: Concepts and models for information and communications technology security management
- Part 2: Techniques for information security risk management
- Part 5: Management guidance on network security

The former parts 3 and 4 have been mnately absorbed by the current parts 1 and 2. The ISO13335-2 standard contains various methods for risk analysis. Certification is not intended.

- *ISO 17799*

The aim of ISO 17799 "Information Technology – Code of Practice for Information Security Management" is to define a framework for IT security management. ISO 17799 is therefore primarily concerned with the steps necessary for developing a fully-functioning IT security management and for integrating this securely in the organization. The necessary IT security measures are touched on briefly on the one hundred or so pages of the ISO/IEC 17799 standard. The recommendations relate to the management level and contain almost no specific technical information. Their implementation is one of the many options available for fulfilling the requirements of the ISO 27001 standard.

- *ISO 27001*

Due to the complexity of information technology and the demand for certifications, numerous manuals, standards and national norms for information security have emerged over the past several years. The ISO 27001 "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first international standard for management of information security that also allows certification. ISO 27001 provides general recommendations on around ten pages for, among other things, the introduction, operation, and improvement of a documented information security management system that also takes the risks into account. The controls from ISO/IEC 27002 are referred to in a normative annex. The readers however, are not provided with any assistance for the practical implementation.

- *ISO 27002*

The goal of ISO 27002 (previously ISO 17799:2005), "Information technology – Code of practice for information security management", is to define a framework for information security management. ISO 27002 is therefore mainly concerned with the steps necessary to establish a functioning security management system and anchor it in the organization. The necessary security safeguards are only described briefly in the approximately 100 pages of the ISO standard ISO/IEC 27002.

The recommendations are primarily intended for the management level and do not contain much specific technical information for this reason. The implementation of the security recommendations in ISO 27002 is one of many ways to fulfill the requirements of ISO Standard 27001.

- *ISO 27005*

This ISO Standard "Information security risk management" contains general recommendations for risk management for information security. Among other items, it supports the implementation of the requirements from ISO/IEC 27001. In this case, though, no specific method for risk management is prescribed. ISO/IEC 27005 replaces the previous standard ISO 13335-2. This standard, ISO 13335 "Management of information and communications technology security, Part 2: Techniques for information security risk management", provided guidelines for the management of information security.

- *ISO 27006*

ISO Standard 27006 "Information technology - Security techniques - Requirements for the accreditation of bodies providing certification of information security management systems" specifies requirements for the accrediting of certification bodies for ISMS and also handles specific details of the ISMS certification process.

Other standards in the ISO-2700x series

The ISO 2700x series of standards will probably be made up of ISO standards 27000–27019 and 27030–27044 in the long term. All standards in this series handle different aspects of security management and are based on the requirements in ISO 27001. The other standards should contribute to improved understanding and the practical application of ISO 27001.

2.2 Usefulness of an ISMS Management

There are several ways, from a technical perspective, to develop an ISMS. That makes the management of the ISMS a critical as well a challenging sector for the administrators and the people who participate in the overall system operation. So, it is easily implicit that an ISMS must include strict policies and access procedures in order to prevent unauthorized users from gaining access and provoking safety events.

Despite the fact that the implementation of an ISMS depends on organization requirements, there are rules and principles that all ISMS must obey. That will increase the protection and safety level but also the confidence of the organization to deal with

daily operating challenges. Also, it is important to underline that it is difficult to create, implement and maintain an ISMS, unless all the people involved are aware of the thoroughness and the stability of the system. Therefore, for an ISMS to be effective, we must analyze the security needs while considering data sensitivity of each information asset in order to apply the appropriate control mechanisms. It is obvious that not all information needs the same security levels, and therefore we should establish scalar security controls.

As threats and vulnerabilities are increasing and becoming more hazardous than in the past, concurrently an ISMS must continually develop its defensive mechanism and its ability to recover after a security incident, to meet the rapidly changing technical landscape. Last but not least, ISMS must frequently be tested to ensure the organization about its up-to-date protection status or if modifications need to be made.

2.2.1 Management Principles

In this paragraph, some of the most notable management principles are presented, as well as their complexity and the staff training which is required in order to achieve an acceptable and positive management. The discipline on these measures and principles is an important issue that personnel must strictly follow. At this point, we should mention that many times it is a common mistake that expensive and large-scale complex projects are considered as safer and more appropriate and as a consequence they are wrongly chosen by an organization.

Regarding Information Security, we can distinguish some tasks and duties of ISMS management as follows:

1. Information Security: Responsibilities

The higher administration level of every public agency, company or organization is responsible for the proper and unfailing operation with respect to Information Security, taking into account the nature, the objectives and the structure of the organization. Also, it has to assure the outgoing and incoming information, considering the existing legislation of each country.

It is also very important for security managers as well as every manager in any sector of the organization to heed organizations' security and to inform every member of the organization about the usefulness of the Information Security.

2. Information Security: Integration

Similarly, organizations' operations must include and integrate Information Security in all phases, where information is processed and used. For instance, security policy and requirements must not only be taken into account during information exchange and processing, but also in business plan and strategy creation and employee or staff security training.

3. Information security: Management

One of the most important parts of the Information Security System is the management, which has to supervise and administrate the overall security process.

Management includes the following tasks:

Information Security strategy and objectives must be clear and agreed.

- We need to analyze the way and the degree that information security risks could impact organization or company operation and the extent to which we can support it in an offensive incident.
- Information Technology business operations and other functions related to security systems must obtain effectual resources for their uninterrupted operation.
- Periodically, Information Technology Security Strategies must be reviewed in order to control and examine the achievement of objectives. Consequently, we can correct any faults, mistakes and vulnerabilities. In order to achieve this and to operate efficiently, all key-stakeholders must collaborate.
- There must be incentives for the Staff just to motivate them to keep security levels high and think seriously about all issues relating to organization and the overall business operation security. However, over and above that, staff security training and familiarity with all the information security needs and objectives are two of the most important factors in order to maximize and ensure business procedure integration.

4. Realizable Goals and Objectives

One of the main reasons that objectives, goals and total security projects and policies fail is that many times they are excessively ambitious and over-optimistic.

This phenomenon take places not only in the Information Technology fields, but also in many business projects. Therefore, we must adjust security-related measures according to the underlying resources (material as well physical). So, from an empirical perspective, the most sufficient method to establish a security policy for an organization is its step-by-step development with moderate investments in spite of high investments and cost and large range projects. Consequently, one option is to choose the most vulnerable and the most valuable sections of the organization and to secure them first. It can thus be appropriate to implement the necessary level of security initially only within selected areas. Afterwards, we must make plans, schedule and set priorities about the whole system security.

5. Balancing costs: Security - Benefits

One of the most challenging tasks is the balance between the cost for the security measures and the benefits that they can offer to the organization. In order to achieve that, first we have to conduct a risk analysis to find out the most vulnerable aspects, to learn about the high risks in our organization and invest in security systems that can shield them. It is common, that many times inexpensive security solutions are more efficient than costly systems, and therefore we should be very careful and patient when we run a risk analysis and risk assessment approaches.

2.2.2 IT: Continuous Development and Maintenance

Information Security definition and installation is not a process with temporal beginning and end (time-stamps). On a regular basis, we have to control, check and evaluate the overall security system and to make continuous improvements. These control procedures do not only include Information Security system evaluation itself, but also analysis and evaluation of the policies, commitments and users' access privileges.

2.2.3 Ways to deploy and improve secure business networks

It is widely accepted that IT professionals, along with involved organizations, tend to focus on the wireless side of the network with respect to security. That is because Wi-Fi has no physical obstacles and fences. As a result, it is easily understood that a network attacker specialist is able to detect the Service Set Identifier (SSID) of a network and launch an attack anonymously. Alongside, as hackers strive to gain physical access to corporate Local Area Networks (LANs) and Wide Area Networks (WANs), it is equally important to examine the wired network security.

- *Wired Network Security*

1. *Keep the network up-to-date:* Continuously firmware and/or software updates checking on all network infrastructure components. Often password change and review for an insecure functionality and inappropriate configuration. Also the administrator should ensure that network devices (computers or servers OS as well drivers, switch software etc.) are also up-to-date. Similarly, firewall and antivirus must be active and updated.

2. *Network mapping and physical security:* Dedicated staff must have clear comprehension and understanding of the entire network infrastructure and configuration, for instance, Ethernet ports, firewall, servers, computers switches and routers as well as access points and all the connected devices. In the mapping step, we should identify security vulnerabilities and threats but also ways to increase performance and reliability. Besides, scientific software can be used in order to produce a professional and accurate network map. Meanwhile, without strong physical security of the network and the building, many security flaws can emerge.

We should continuously digitally check the Ethernet ports and all the infrastructure components with connectivity ability to avoid security flaws that hackers can exploit.

Similarly, all the wired components and gathering devices, like switch racks, should be located out of sight, locked and secured.

3. *MAC address filtering and 802.1x Authentication:* Unlike wireless networks, which require WPA or WPA2 (PSK) security protocols, wired networks provide a quick and easy authentication and encryption method in which anyone can have access to the network by plugging in a device into a port. Experienced hackers can bypass the MAC address filtering but this can be a first step of security which can prevent someone from exploiting a security hole easily. The 802.1x authentication offers users dynamic authentication to VLANs (group Ethernet ports, wireless access points, and multiple virtual networks among users).

To deploy 802.1X authentication, we need a Remote Authentication Dial-In User Service (RADIUS) server, which basically serves as the user database and is the component that authorizes or denies network access. In conclusion, we should note that Windows Server already has a RADIUS server. If we do not use Windows Server, we can install standalone RADIUS servers.

4. *Encryption (PCs, Servers, Network):* VLANs and 802.1x authentication provide the ability to monitor the VLAN network traffic and capture encrypted files which include sensitive and private data (passwords, emails, salary, personal information etc.). We can encrypt the entire traffic or we can select communications we deem more sensitive than others, using SSL/HTTPS. The sensitive traffic can be served through standard VPN (only during sensitive data transmission) or forced to be used continuously. Moreover, we can also encrypt the entire network, using IPsec protocol since Windows server supports this functionality. However, the encryption process can be an overhead burden on the network and traffic rates can decrease dramatically. Alternatively, Layer2 approach is used instead of Layer3 (IPsec) to improve the overhead and latency disadvantages.

- *Wireless Network Security*

1. *WPA (IEEE 802.11i standard)*: It addresses most of the known WEP vulnerabilities and is intended for wireless enterprise networks. The Extensible Authentication Protocol (EAP), using a secure public-key encryption system, provides access only to authorized network users and also improves data encryption by using the Temporal Key Integrity Protocol (TKIP). Furthermore, a security improvement for WEP which is called Message Integrity Check (MIC), helps network administrators to avoid bit-flip techniques attacks on encrypted network data packets. It determines whether a hacker captured or altered packets, passing between the access point and client.

2. *WPA2*: This implements the obligatory IEEE 802.11 elements standard while it introduces the use of AES (Advanced Encryption Standard) and CCMP (Counter Cipher Mode with Block-Chaining Message Authentication Code protocols. In this way, security becomes tighter for enterprise networks. The secure dynamic keys distribution, takes place after users log in or provide valid digital certificate.

3. *Deploy WPA2 – Enterprise*: It contains RADIUS server installation, encrypted access point configuration and RADIUS server information. Also, we must configure the operating system with the encryption and IEEE 802.1x settings and then connect to the secure wireless enterprise.

- RADIUS Server and EAP

The user who wants to be authenticated is the *supplicant*. The RADIUS server establishing the authentication is the *authentication server* and the device at the AP (PC, laptop, smartphone) is the *authenticator*. Users do not see the encryption keys and keys are not stored on the device. The authentication is port-based so that when a user attempts to connect to the network, communication is allowed through a virtual port for the transfer of login credentials. If authentication is successful, encryption keys are securely passed and the user receives full access.

- EAP

We can choose the EAP among PEAP, TLS and TTLS considering the security level we need and devices (PC, Servers) specifications. [3]

-PEAP (Protected EAP): It authenticates users through the usernames and passwords they enter when connecting to the network. It is one of the easiest EAP types to implement.

- TLS (Transport Layer Security): Although this EAP type requires more time to implement and maintain, TLS is very secure because both client and server validation is done with SSL (secure socket layer) certificates. Instead of connecting to the network with usernames and passwords, end-user devices or computers must have an SSL certificate file. You control the certificate authority and distribute the client certificates.

- TTLS (Tunneled TLS): This version of TLS doesn't require security certificates and reduces network management time. However, because TTLS doesn't have native support in Microsoft Windows, it requires a third-party client.

2.3 PDCA Model for ISMS.

All the IT business processes have a lifecycle which is frequently divided into four (4) phases in order to describe the dynamics of Information Technology and also how the organization should establish and manage the ISMS. These phases comprise the Plan-Do-Check-Act model which is described in detail below.[4]

- *Plan*: We organize the ISMS policy, targets and procedures to balance the management risk. Moreover, we increase the level of Information Security in order to achieve the organization's mission and ambitions.

- *Do*: ISMS implementation and operation plan and policy. We actualize the overall project while adjusting controls and procedures following the most appropriate and innovative approach.

- *Check*: We congregate performance evaluation and analyze the achievement objectives. Finally, we produce and summarize a report to review and appraise the results.

- *Act*: It is designed with a view to taking the appropriate actions to eliminate discovered flaws and weaknesses as well as to improve the current ISMS management and operation.

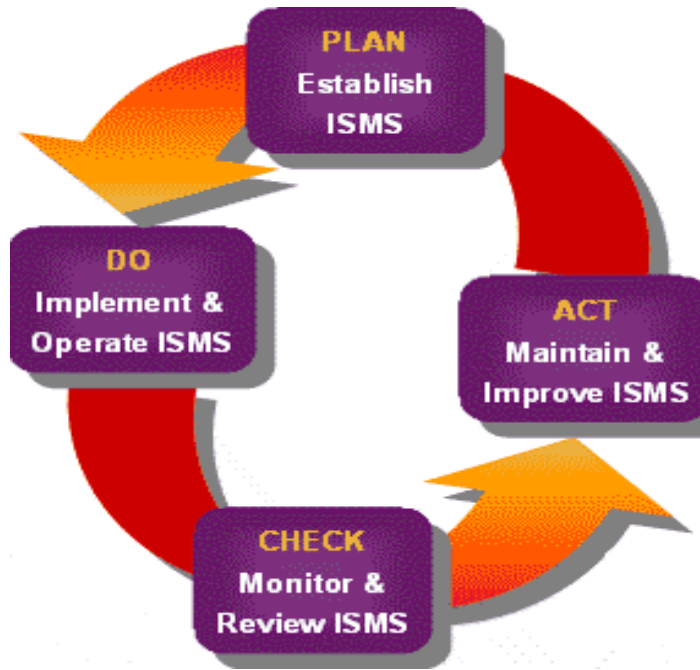


Figure 3: Lifecycle in the PDCA model

Last but not least, we should also mention that ISO 27001 standard includes PDCA model and it can be applied to all the Information Security tasks. Using the PDCA model, we are able to describe the Information Security policy in a simple and clear way.

3 Data Breaches and Cybersecurity

In this chapter, an attempt is made in order to comprehend what exactly Data Breach and Cybersecurity are, what are the greatest threats and the main factors influencing them as well as distinguishing the terms Cybersecurity and Information Assurance. Reference is also made to the ways in which Data Breaches are discovered and the procedures following, after the initial detection.

3.1 What Data Breach is and its effects

There are numerous important factors we should consider while establishing a new business. Especially in large companies, there are several security factors we should consider, in order to take the necessary measures which maximize security level and reliability. By knowing that private data are vitally important in organization running, it is obvious that if sensitive data is leaked from an organization, it may cause irreparable damage. Data Breach is one of the main security risks that most organizations should be armored against. Data breach is the exposure of sensitive confidential or private data to unauthorized personnel or illegal viewing. Sometimes this is reported in literature as Data Split or Data leak. There are several ways that data breaches can happen: from a hacker attack to an employee error and may result in financial, personal or health information loss. We can categorize the effects of Data Breaches as follows:

- *Stealing*: For example: Bank account information.
- *Reputation break-down*: Customers' and contributors' trustiness fades since business is unable to guarantee data security.
- *Revenue reduction*: Even if the Data Breach does not generate extensive technical problems or sensitive data loss, the extended period that your entire network is off can cause remarkable revenue reduction and other significant financial problems.
- *Criminal damage*: Defamation or seeding of false information can result in the ruin of organization reputation in minutes. For instance, customers may be wrongly informed on purpose by hackers through the business website.
- *Copyright damage*: Stealing of intellectual property can be equally important when a Data Breach provides hackers with information that includes business projects, contracts, plans or ideas.

3.2 Data Breach – Threat agents

When we refer to threat agents, we focus on factors which are involved in Data Breach incidents. Often there can be more than one factor involved in any of those incidents and their involvement can be malicious or not malicious, direct or indirect, deliberate or

accidental. Therefore, source identification is one of the most critical and also difficult phases during forensic investigation. This is because if we manage to recognize the persons involved, we will be able to analyze the attack in depth and additionally to implement future defensive strategies and specific methodologies for an effective and straightforward response. Consequently, we can distinguish three main categories of threat factors: External, Internal and Partner [5].

3.2.1 External Factors

They derive from sources outside the organization and its network partners. Examples are hackers, specialized criminal groups but also weather and environmental phenomena such as earthquakes. The following two figures present the types of external factors by percentage of Data Breaches within external and the origin of external factors.

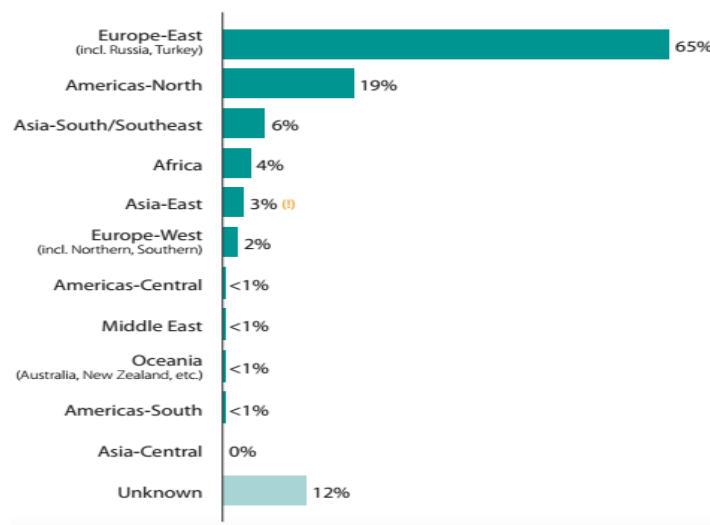


Figure 4: Origin of External Factors (source: Verizon DBIR)

Organized criminal group	58% (1)
Unaffiliated person(s)	40% (1)
Former employee (no longer had access)	2%
Competitor	1%
Unknown	14%
Other	<1%

Figure 5: Types of External Factors (source: Verizon DBIR)

3.2.2 Internal Factors

They derive from within the organization and include organization executives and employees as well as independent contractors and interns etc. The following figure present the types of internal factors by percent of Data Breaches.

Regular employee/end-user	88% (1)
Finance/Accounting staff	23%
Executive/Upper Management	9%
Helpdesk staff	4%
System/network administrator	2%
Software developer	1%
Unknown	1%
Other(s)	1%

Figure 6: Types of Internal Factors (source: Verizon DBIR)

3.2.3 Partners

Partners include any third party sharing a business relationship with the organization. For instance: suppliers, vendors, hosting providers, outsourced IT support etc.

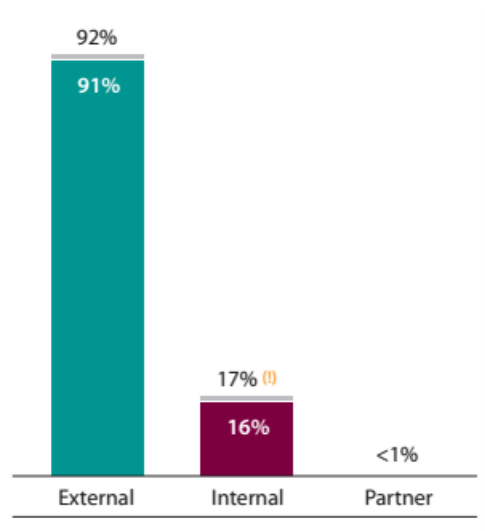


Figure 7: Threat Factors by percentage of Data Breaches. (source: Verizon DBIR)

3.2.4 Threat actions and Hacking Methods

Threat actions present what the threat agent did to cause or to contribute to the Data Breach. The majority of incidents involve multiple threat actions in one or more categories, which are present in the figure below along with the percentage of breaches and compromised records associated with each.

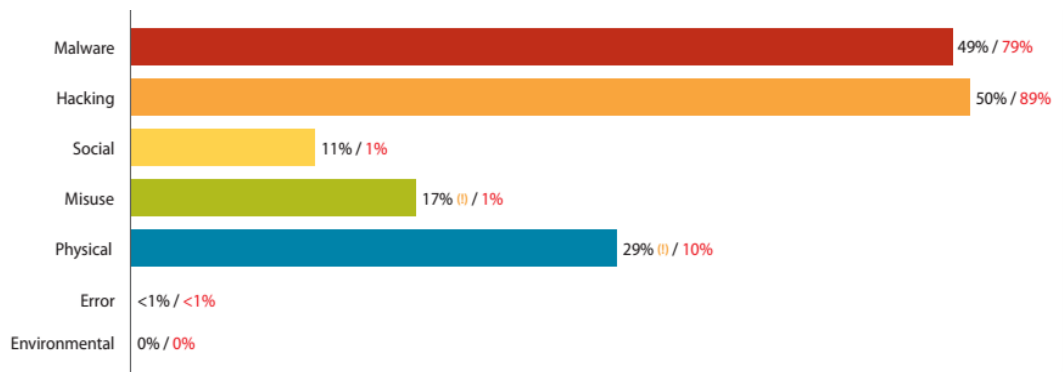


Figure 8: Threat action categories by percentage of Data Breaches and percentage of records. (source: Verizon DBIR)

It is obvious that Hacking and Malware are the most popular threat actions with Physical and Misuse following.

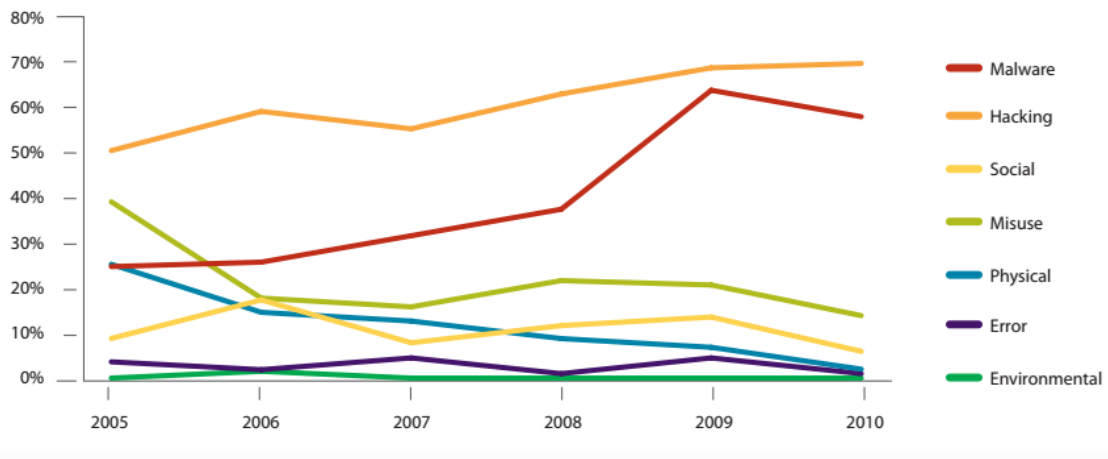


Figure 9: Threat action categories over time by percent of Data Breaches (source: Verizon DBIR)

Meanwhile, there is a variety of hacking methods that hackers use frequently to gain access and/or steal sensitive data and information. The method with the highest use percentage is the Exploitation of backdoor or command/control channel. Using backdoor installation, attackers can bypass security mechanisms to gain access without relying on

legitimate channels. The following figure presents all Types of hacking by percentage of breaches within Hacking.

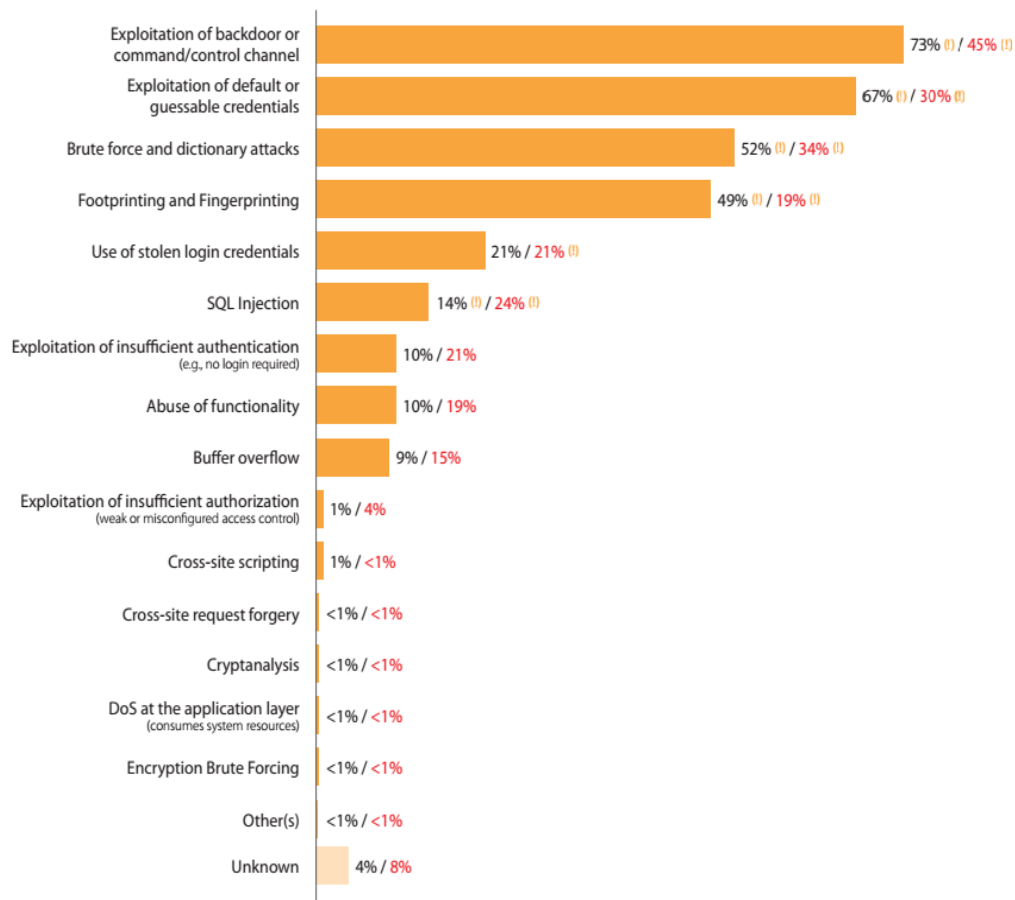


Figure 10: Types of hacking by percentage of Data Breaches within Hacking and percentage of records. (source: Verizon DBIR)

3.3 Incomplete Data Security / Common Pitfalls

Since there are numerous Data Security tools, the complexity among them increases as they can be applied in a wide range of organizations or enterprises such as data base security and administration, information governance, data privacy, data activity monitoring etc. Due to similarities or differences among those security tools, we should

assimilate some common pitfalls just to ensure that our private or sensitive data are protected to a greater extent.

Firstly, we should mention that it is necessary to have an end-to-end data protection solution and to achieve that, we must adopt many levels of automated security processes. These security automations will be able to support overall system failure and redirection as well as load balance capabilities in order not to utilize high CPU resources and security gaps.

Furthermore, Data Security solutions should include Analytics to identify advanced level threats. Appropriate Analytics level can identify, stop and consequently prevent data loss, especially if those tools provide real time analytics. These solutions require specialized architecture and software engineering. Similarly, there is an important need for successful reports with the aim of saving time and forestalling security incidents. Security reports must be assiduous, accurate and up-to-date. So, automated workflows will confirm that your security policies are being observed accurately by the whole system.

3.4 Discovering a Data Breach

According to most studies, organizations discover that they have suffered from a Data Breach days or months after it happened (or even years later), when clients, cooperators or network administrators identify an irregularity. That happens because usually attacks do not bring out functionality issues or other glitches, so it is not so easy for unqualified users or employees to notice that something has gone wrong.

3.4.1 Things that uncover security problems

Undoubtedly, there are few things that can help users to identify a security issue. For instance, slow or non-responsive computers or servers, freeze windows, colleagues' reports about spam e-mails received by company mail servers and strange programs that request for personal information or credentials could be worrying signs that should rouse us. When malware or a virus is discovered on a system, it is necessary to conduct an investigation about contaminated files and generally overall data health. However, the

most worrying fact is that if a company has been compromised by professional attackers, infringement signs will be few or not easily discovered.

3.4.2 Immediate and Necessary Actions

From the time Data Breach is discovered, there is little chances of recovering stolen data and information, so the breach assessment stage is practically the first step in which we can determine what exactly happened and the importance of the incident. The usual process for an organization is to consult their attorney with a view to conducting a forensic investigation in order to identify the attack source and the sectors that have been affected. Then attorneys will define experts who specialize in finding, maintaining and analyzing electronic equipment and data storage devices.

Meanwhile, we should shut down their servers, computers and any device where the breach occurred because this will conserve evidence and will help forensic experts to dive into the problem. Finally, we have to copy and carefully store the access and activity logs from the affected machines as well as to identify the type and the category of information that has been affected (company plans, customers' personal details, employee details and payments).

3.4.3 Averting Future Data Breaches

It is not a short period for a company to recover after it has suffered a Data Breach, but when it get the situation under control, it is time to start working in order to prevent future Data Breaches.

To start with, IT security professionals should establish an up-to-date security plan that will demand the optimum constant practices and measures to shield the company against threats. An impeccably trained staff, ready to act in dangerous situations is the key to eliminating the risk of a Data Breach and its consequences. That means that all employees which use electronic equipment and have access in any level in a company's network must learn how to recognize indications which bring out security flaws.

In conclusion, since no security policy, strategy, software or equipment can provide 100% security, the most important thing for a company is to learn how to respond directly and in an efficient way, to recover from a Data Breach, while it cares continuously about the security technologies and policies upgrade.

3.5 Cyber Security

Just like criminal activities in the physical medium, by the term Cyber Security, we refer to the ability of an organization to protect its existence and to defend against cyber-attacks that take place in Cyberspace¹.

It involves information and system protection from a range of risks and threats such as: Cyber Warfare², Cyber Terrorism³ and Cyber Spying⁴ which could be targeted at sensitive, classified, business or organization secrets and plans or political and military information. Consequently, Cybersecurity plays a significant and first priority tactic in most of the world's government agencies, military forces, multinational corporations and organizations.

¹Cyberspace is "the notional environment in which communication over computer networks occurs. The parent term of cyberspace is "cybernetics", derived from the Ancient Greek κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener for his pioneering work in electronic communication and control science.

²Cyberwarfare is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems.

³Terrorist activities intended to damage or disrupt vital computer systems.

⁴Cyber Spying is a form of cybercrime in which hackers target computer networks in order to gain access to classified or other information that may be profitable or advantageous for the hacker.

3.5.1 Cybercrime

Cybercrime refers to any illegal activity against any computer system, computer network or the Internet and due to diversity of Cybercrime attacks it can be classified into three main categories. :

- Business Offense and Abuse
- Online Scams
- Identify Theft and Fraud

Hereinafter, we analyze these three categories by presenting their subcategories and their characteristics.

1. Business Offense and Abuse includes:

- *Denial-of-Service (DoS)*, which changes a computer's normal response and makes it unavailable to the users or prevents users from efficiently using it.
- *Malicious software*, refers to computer programs (like virus, Trojan horse etc.) which exploit computer systems or computer networks trying to disrupt business operations and gain access to sensitive data.
- *Information Piracy*, which refers to gaining access and stealing Copyright Data (archives, software etc.)
- *Industrial Spying*, which is opponents' illegal collaboration, in order to gain access to sensitive, confidential and financial data, which will provide them with an advantage against a company or organization.

2. Online Scams, includes:

- *Phishing*, which involves entangling participant/s in a computer/electronic communication and making them believe that they are participating in a trustworthy communication in order to gain access to sensitive data and/or personal information.
- *Spear Phishing*, which is a scam and makes an e-mail appear as if it originates from an organization or business that we know. Of course, this is not true, and these e-mails aim at our personal data such as bank account or credit card numbers, passwords etc.

- *Spoofing*, which is the fraudulent procedure in which someone is being tricked into entering personal data in a fake website that looks similar to a well-known one.
 - *Purchase Fraud*, which takes place when someone sells products via e-shops that are never sent to the recipient.
 - *Pharming*, which refers to a technique in which a user can be redirected from a legal to a fraudulent website.
3. Identify Theft and Fraud, includes:
- *Theft of Identity*, which relates to the acquisition of private or personal data (bank account numbers or details, credit card numbers) that can be used illegitimately to carry out banking operations without the victim's knowledge.
 - *Business Theft*, which refers to stealing revenue from a business. This can be done directly through a company's bank account (requires previous *Theft of Identity* step), and involves illegal money transferring.
 - *Theft of Copyright*, which refers to plans, ideas, military or government secrets being stolen in order to obtain competitive advantages among similar organizations.
 - *Theft of Customer Data*, which refers to private or personal customer data/information in order to use them for economic benefit.

3.5.2 On-line Privacy

In this chapter, we will try to distinguish between fraud actions by which attackers try to steal valuable information or data and actions which aim at data normally published through the Internet while we surf on the Web. Consequently, with the term On-line privacy or Internet Privacy we refer to a diversity of methodologies, techniques and factors used to protect communications, personal or sensitive data and classified

information. While E-commerce becomes a famous marketing model and gains market share year by year, on-line privacy and namelessness are important factors that can shield users and decrease the events of personal data violation.

- Cookies, are text files (usually) saved by websites on our computers while we surf the Internet and remain (exist) on that, until we delete the specific folder that include them, or are sessions. A session means that cookies only work when we are on a specific website. Cookies provide information to website owner, for instance how many times a specific customer visits the website, or decide what ads to show, in order to conduct a more targeted advertising campaign. At once, we conclude that cookies play a significant role to normal Internet operation. However, they are visible to unauthorized parties and take part in On-line privacy.

- Social Networking privacy: It is readily understood that due to wide-spread of Social Networking, million personal information of any time are disseminated through the Internet daily.

So, through Social Network platform users share personal information including pictures, date of birth, phone number, home or business address or even marital or relationship status. These kinds of information offer a chance to misrepresent information and create fake profiles, all of which use part of our personal data, aiming to deceive and/or defraud.

- IP addresses, are numerical label addresses which are assigned to each IP-based network device such as computer, smartphone and printer. Through DHCP⁵ administration mechanism, which provides an automated way to distribute and update IP addresses on network devices listed above, communication is feasible.

So, every time we visit a website, our IP address is recorded. Our IP address provides information about our approximate location and specific Proxy services and is the easiest way to disincorporate this information to be known.

⁵Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any new node entering the network. DHCP permits a node to be configured automatically, thereby avoiding the necessity of involvement by a network administrator. Source:technopedia.com

3.6 Differences between Cyber Security and Information Assurance.

First we should point out that these two terms have many differences, although many times we tend to confuse them and consequently use them as synonymous concepts. Cybersecurity, aims at defense and prevention against attacks and also against unauthorized access to computers, networks, servers, software and any kind of data in electronic format, through the Internet. Generally, Cyber Security defined as the protection of data and systems in networks that are connected to the Internet⁶. We can depict Cyber Security as a subset of Information Assurance and afterwards a subset of Information Security which encloses various higher level policies, Risk Management, constraints and discipline, as well as training and strategies. Consequently, we can say that Cyber security's first priority is to defend Information Systems' infrastructure (devices, networks) and thereafter data protection within Cyberspace.

On the other hand, whilst Cyber Security is a term recently introduced, Information Assurance is a well – known and popular security procedure which focuses on digital and non-digital information and data, such as hard disks. Thereupon, Information Assurance offers the certainty to an organization, that IT system will perform appropriately and disincline unauthorized users to access it. Eventually, we can provide the following inclusive definition about Information Assurance: *‘Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.*

These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities’⁷

⁶ PC Magazine's Encyclopedia

⁷ NIST (National Institute of Standards and Technology) Guideline for Identifying and Information System as a National Security System – August 2003

4 Risk Management – Risk Assessment

Risk Assessment and Risk Management are two of the most important procedures in order to ensure the integrity and the business continuity process. This chapter presents the fundamentals and the lifecycle of these methods but also refers to Risk Management privacy.

4.1 Risk Assessment – Definition

Risk Assessment is the procedure of identifying variables that can affect an organization in a negative way and as a result decrease or even ruin organization and business running. In multinational corporations and large companies, usually Risk Assessments are conducted by Chief Risk Officers (CRO) and can be divided into two main categories / techniques: Quantitative and Qualitative.

1. *Quantitative Risk Assessment:*

Numerical Values are assigned as a probability of an event taking place as well as the consequence that it can cause. These values are used in order to calculate the Risk Factor for an incident. Afterwards, Risk Factor values are translated into an amount of money.

2. *Qualitative Risk Assessment:*

This category does not include any numerical factors, numerical probabilities or loss provision. It is used more often than the Quantitative approach just to rank the risks regarding their dangerousness.

This category includes the *Fraud Risk Assessment* subcategory, at which we conduct an evaluation of potential events of fraud that could impact an organization's security standards, including employees and client information, financial data and business plans and strategies. Also, *Security Risk Assessment* contains a potential breaches evaluation

at organization's information protection, material assets and generally the overall security level within an organization. In order to achieve this, we need to take into account an organization's main operations, applications, infrastructure and employees' actions in daily operations.

4.2 Efficient Risk Assessment Fundamentals

In order to produce useful results, Risk Assessment process should follow four (4) basic principles or steps.

1) *Transparent establishment throughout Risk Assessment process.*

To verify that resources and obligations are secured, supervision and accountability are considered as critical procedures, while they can ensure that strict and continuous actions will take place in a case of an incident.

2) *Setting specific objectives at the beginning and at the end of Risk Assessment phase.*

Risks are measured in scope for the risk assessment while the definition of objectives has a critical role in successful Risk Assessment.

3) *Defining and Rating Risk Scales in relation to organization objectives.*

Generally, risks are measured in terms of probability of occurrence, and probability scales should reflect the units of measure used for company objectives which can mirror various types such as: financial, people etc. Likewise, the timescale used to assess risk probability should coincide with the organization's objectives timescale.

4) *A view of risk portfolio is modulated to support decision making.*

Although risks are estimated individually in relation to the targets they impact, we should bring together a risk portfolio which at present detects interdependencies between risks within the organization. Possible correlations in which high risk exposure may be disclosed to one risk, could cause variations (positive or negative) to another risk.

Last but not least, through view of risk portfolio, summarization of risks may be spotted as well as helps organizations assimilate discrete events' effects and determine where to develop automated responses to risks.

4.3 Risk Assessment Case Study: *Computer Software Company*

We consider a company that uses risk assessment to verify that information controls comply with all the predefined requirements and take place due to an organization's effort to achieve more secure e-commerce operations, as well as to pick up information system integration among customers, administrators and suppliers. By using a combination of *Quantitative* and *Qualitative* techniques, the overall process tries to exploit experts' knowledge in order to exclude flavorless recommendations while ensuring the maximum security levels in the entire company. The implementation of the process recognizes and records all the security controls (related to assessment), identifies current risks and additional controls needed to minimize these risks.

Company characteristics: This provides its customers with Software solutions about (accounting, payrolls etc.), Networking Software, Consulting and Support Services. Also, it is a multinational company with a vast private network and it uses thousands of in-house servers to conduct many daily operations. Furthermore, Support Services include thousands of daily connections to clients in order to provide those services, as well as connections with partners and other suppliers. It is obvious that the nature of all these operations increases the risks for a Data Breach event, which makes information protection a challenging process.

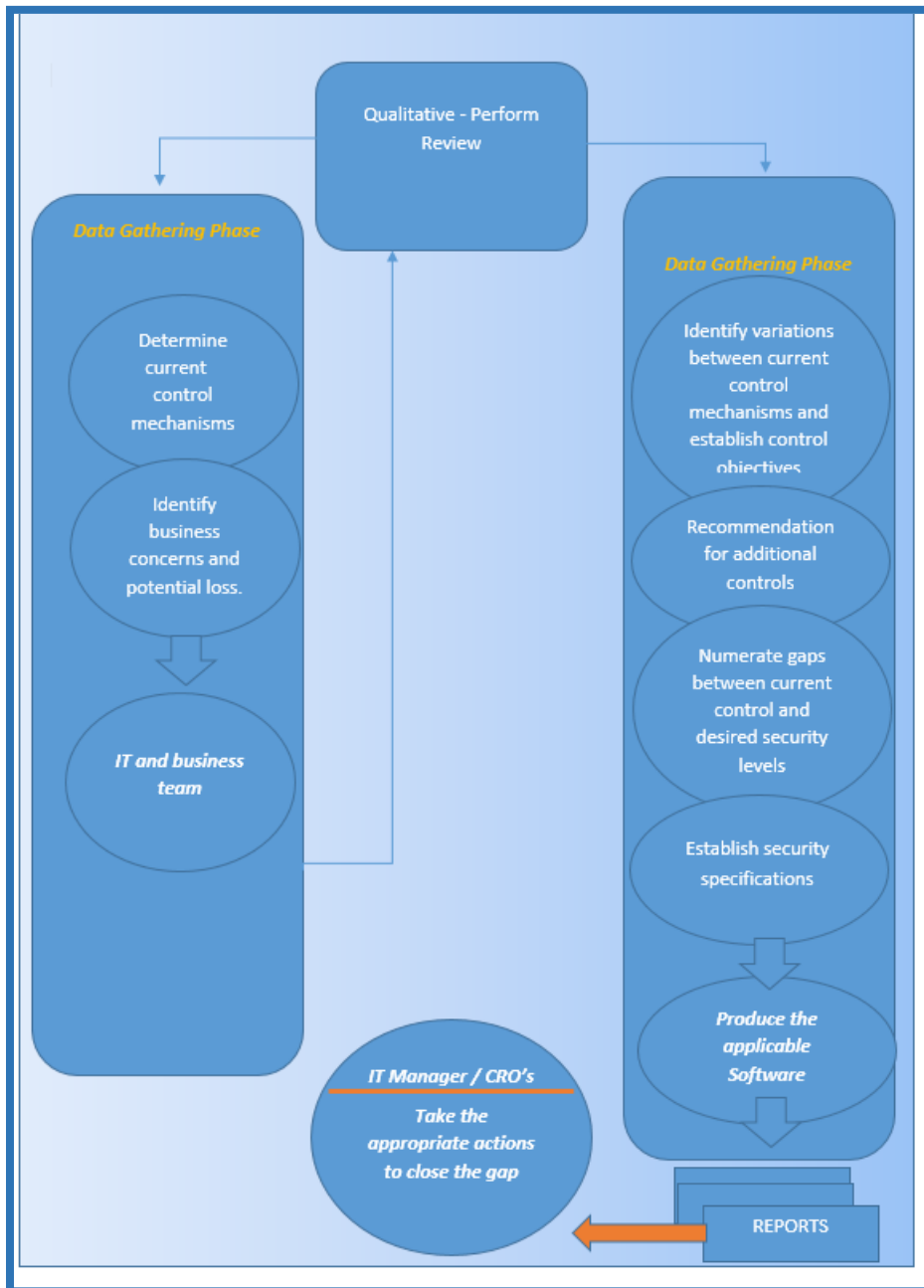


Figure 11: Qualitative – Perform – Review (Procedures)

4.3.1 Stage 1: Commencement

Company policy organization demands IT security collaboration in order to initiate Risk Assessment under the importance of the procedures and the certain time frame. The most important processes indicated by managers and the ideal running frequency is on an annual basis with the exception of extremely critical and frequently changing instances. Certainly, managers can request Risk Assessment if they consider it necessary. The following types of activity are associated with Risk Assessment:

- New Software development.
- New Software procurement (by cooperators).
- Existing System -Improvement of Security Features (Software, Databases, Hardwar units, Network infrastructure etc.)

When the decision to run a Risk Assessment is taken, CRO managers create a team of IT and business experts with the aim of aggregating important data. Moreover, a permanent staff team are responsible for: Quality Reviews, Result analysis and Overall Process Supervising.

4.3.2 Stage 2: Operation and documentation

In this phase, a questionnaire is used to gather information concerning security controls, policies, value of important tasks and thereafter compare that information with the default security controls and policies. To do that, the company has developed specific software in order to automate the comparison procedure by taking into account many significant factors. In the event where software identifies points that does not comply the predefined control requirements, automatically accesses a specifically database that includes suitable control solutions (developed by CRO, security managers and other security experts) and searches for the optimum solution.

4.3.3 Stage 3: *Collecting Data*

During this stage, a questionnaire developed by specialists is completed by employees' teams to specify the current security controls and to assess their operations. Experts can advise and assist those teams in order to help in production of detailed, quality and productive results. The main categories of questions relate to:

- Policy implementation
- Authorization and authentication procedures
- Hardware / Physical Security
- Incident Break / Loss Response
- Confidentiality
- Configuration Management
- Database / Warehouse Design and Security

4.3.4 Stage 4: *Analysis*

After the quality review stage is finished, the Analysis Group derive questionnaire answers about current control level and use them as input to the specific software, in order to compare current control with the predefined security requirements and policies. In the event that a scan detects gaps and security control does not comply with company requirements, the software recommends control techniques to maximize security level, cover current gaps and eventually, comply with security control requirements. Furthermore, scanning control techniques can have multiple security levels which depend on strength type and the stiffness we choose to conduct the whole Risk Assessment initially.

4.3.5 Stage 5: *Final report and assurance that pre-agreed actions are applied.*

In this phase, reports are produced by the overall Risk Assessment process including Risk Analysis report, which include current compliance with predefined security standards and advice for the organization of security integration. Also, reports include graphs and figures for all the main procedures or applications aberration between current security controls and introduced or suggested by organization security managers which establish the security policy.

Besides, reports estimate the average cost for each suggested security measure (employee training, software implementation and improvement, certifications etc.) As IT Security Managers are responsible for making improvements to a company's Information Security System, there are many tools that can assist them to achieve the best possible result. Nonetheless, reports are created and published periodically just to evaluate the overall company's progress and the effectiveness of measures taken to increase the overall security as well as to prevent any negative effect on any other production and operation process.

4.4 Risk Management: *Definition*

The overall Data protection for an organization is based on Risk Management due to its high criticality as it can assure that all data, and especially sensitive, private and confidential data, are properly edited and privacy is respected. Also, Risk Management is an explicit necessity in most Data Protection legislations. These risks consist of two individual categories:

- Hazardous / Harmful events
- Incidents that could probably trigger harmful events

Possible harmful events that must be avoided include illegal access to personal data, arbitrary changes in policy and/or processing, undesirable changes and/or deletion of personal data, legal processes Denial of Service. Generally, we can say that the word Risk

has many meanings and is used to describe dangers and threats to an organization, company, business or a physical person. From a business perspective, when we make estimations about Risk, we should take into account and analyze the following:

- Types of threats for the organization
- The more significant parts of the organization that we must draw our attention to
- The possibilities for a risky event to take place
- The consequences if the threats occur and finally: The appropriate actions which can decrease the chances of a threat occurrence.

4.4.1 Risk Management Cycle

Based on Risk assessment, we are able to establish convenient policy solutions by selecting effective mechanisms and techniques to implement them, and at the same time we have to face daily emergence of new threats and risks. Due to these continuity, changes it is necessary to conduct periodically risk assessment by considering the effectiveness of the control mechanisms and the privacy policies that had previously put into practice.

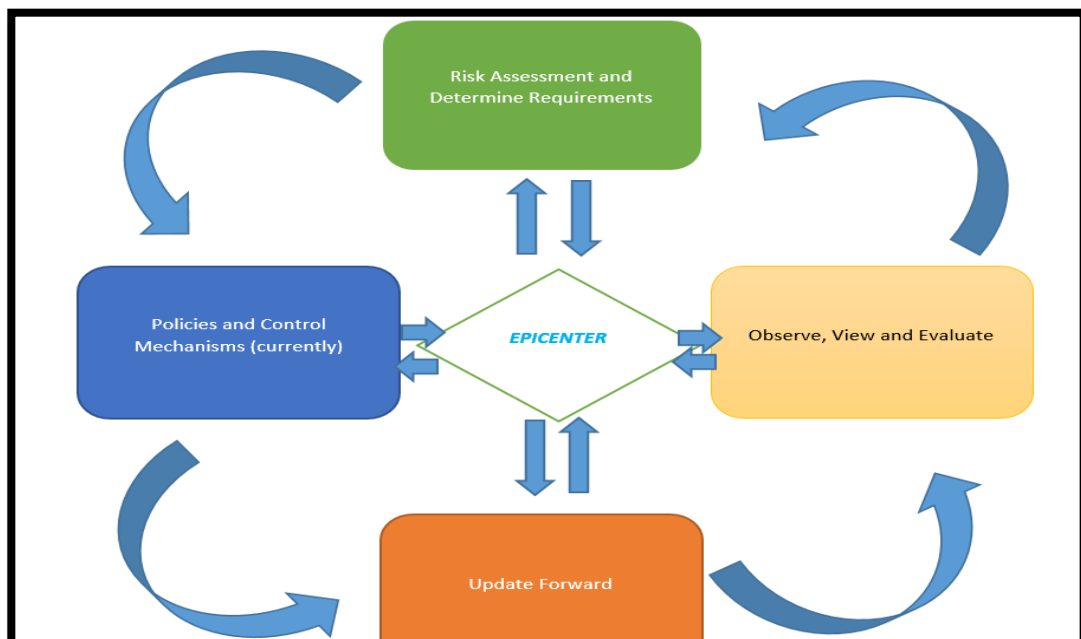


Figure 12: Risk Management Cycle

This continuity process is called Risk Management Cycle and it is presented in the following figure.

4.4.2 Risk Management: *Privacy*

This safest way to obtain coherence and high level confidence is to use Risk Management during the procedure selection establishment. In order to go ahead and assess risks and threats, first we have to classify them, based on their importance. High importance risk and threat events, are high up in the ranking, and then we estimate their probability of occurrence. Once the risks have been assessed, they can be processed depending on their urgent requirements. Subsequently, we can provide the following process in order to analyze the foregoing procedure:

- 1) Personal or Sensitive data process.
- 2) Risky events that can affect these data
- 3) Possible threats involved
- 4) Similar threats (if they exist)
- 5) Techniques to defend those risks or heal them

Because of the continuity of this process, supervising it is obligatory in order to provide updates constantly in case where important changes take place.

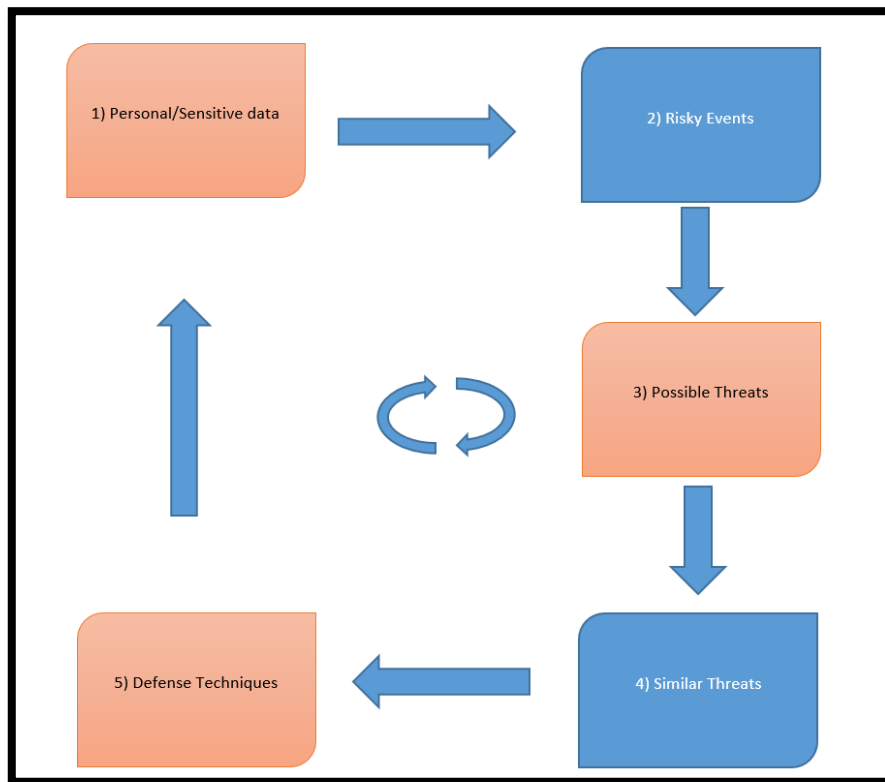


Figure 13: Privacy: processes

5 Cyber Insurance

The Global Insurance market today is increasing sharply, due to soaring Data Breach incidents and private/sensitive data (in digital format) daily increment. The highest percentage of Cyber Insurance market share belongs to the U.S.A. (90%, \$2 billion). This chapter discloses the way that Cyber Insurance companies offer cyber insurance services to private clients, companies or organizations that need to secure sensitive data and Internet transactions in order to increase their trust and confidence. It also presents the current situation and the perspectives in this business field, while presenting the sharp Black Market growth.

5.1 Cyber Insurance in Greece: *Perspectives*

There is a small number of companies that offer Cyber Insurance services in Greece. Most of these companies provide Data Breach Incidents Management solutions as well as Information Loss and Recovery tools, providing financial compensation and data recovery. Due to legislations dealing with Data Privacy and Data Breach incidents obligatory acknowledgment to the competent authorities, but also to their clients or persons whose personal data and details were lost, there was a large and sudden market increase in the U.S.A. In the same manner, similar legislations are expected in the European Union that will impose the mandatory Data Breach events acknowledgment to the appropriate authorities within a period of 24 hours and also to the clients whose data was lost. Apart from this, this legislation will impose fines on the corresponding organizations or companies up to 2% of their overall turnover. Current estimations refer to ten billion dollars (\$10 billion) about the Data Insurance market in the U.S.A. until 2020 and twenty billion dollars (\$20 billion) in 2025, according to Allianz.

As a result and pursuant to Lloyd's study, which estimates that approximately one billion dollars (€1 billion) of Greece's GDO⁸ are in danger of Cyberattacks, we expect a gradual increase in this market perspective for the years to come. [6] Furthermore, Kaspersky Lab make public a study which states that in 2013, 96% of Greek companies confronted digital security issues, but also the most recent ways and methodologies that every organization and company can use to shield itself against those hazardous incidents. Last but not least, we should mention that on an international level, a Data Breach incident can cost an average of 720 thousand dollars to a medium size company or organization, which is able to reach up to 2.5 million dollars for a large size company or organization in case of targeted and successful attack.[7] [8]

Two of the most common ways that attackers try and manage to gain access and steal personal and private data are: Backdoor Trojan, and Phising, as we mentioned in Chapter

⁸ **Gross domestic product (GDP)** is a measure of the size of an economy.

2, and as a consequence, the human factor plays a critical role in the organization's overall protection.

In addition, Kaspersky's research includes the following about the threats for the Greek companies.

- 87% of Greek companies faced internal security issues (mainly due to carelessness of employees).
- 39% of cases, attributable data leaks due to human factor of company employees and executives.
- 18% of cases, attributable to the inappropriate use of mobile devices (smartphone, laptop, tablet).

Table 1: Top 20 countries with the highest risk of computer infection via Internet. (source: CyRM)

a/a	Country	% of unique users
1	Azerbaijan	56.29 %
2	Kazakhstan	55.62%
3	Armenia	54.92%
4	Russia	54.50%
5	Tajikistan	53.54%
6	Vietnam	50.34%
7	Moldova	47.20%
8	Belarus	47.08%
9	Ukraine	45.66%
10	Kyrgyzstan	44.04%
11	Sri Lanka	43.66%
12	Austria	42.05%
13	Germany	41.95%
14	India	41.90%

15	Uzbekistan	41.49%
16	Georgia	40.96%
17	Malaysia	40.22%
18	Algeria	39.98%
19	GREECE	39.92%
20	Italy	39.61%

5.2 Security Limitations – Black Market Growth

Since the technology emerged in the early 40's, and electronic information (digital information since the 80's) began to prevail, security risks and threats involved with these types of information started to appear alongside. Technologies and techniques dealing with defense and protection such as Anti-virus software, Spyware, Firewalls, attack prevention or detection software and activity log systems began to develop steadily to provide protection even in high risk and difficulty attacks. Even so, there is no security solution or tool to provide 100% security against all types of threats and also it is almost certain that such a solution will never appear. This is reasonable because while new threats and risks appear, security software are updated to discover these new threats, so it is easily understood that since attackers try to detect and exploit just one vulnerability in a specific system, security software specialist or developers try to guess what the attacker will think up to gain access to or steal information from a system.

At the same time, increasing value of personal or business information has been approached by cyber criminals for the obvious reason: more and more information and data are stored in digital format, uploaded and processed throughout the Internet. Organizations and companies spend more and more funds to increase the level of security they offer, they conduct market research to evaluate the most appropriate security solutions and install them hopefully to achieve maximum security and reliability.

Undoubtedly, Cyber-attacks costs are increased dramatically for organizations or companies while the volume of data they store and process continually increases. The fact is that Cyber-attacks cost global business over \$300bn a year.

Table 2: Estimated loss of business revenues to cyber attacks
(source: Grant Thornton IBR 2015)

Union /Region	(Sep 2014 – Sep 2015) in Billion Euros
E.U	62.3
North America	61.3
Asia Pacific	81.3

Meanwhile, the Black Market can provide integrated services for illegal use and cyberattack inception. According to a great deal of recent research, a weekly duration Denial of Service (DoS) attack can be bought by anyone for only 150€. These incidents aggravate the size of risk, turning any inexperienced and unsophisticated person to conduct low–cost attacks against specific targets in a very simple way, from any computer they want. Apart from that, the lack of legislation in many countries (dealing with cyber criminality) provides impunity to cyber criminals.

Here follow some figures that provide us with some accurate and detailed data about personal data worth in the underground market.

Table 3: Estimated per card price, in €, for stolen payment card data
(source: McAfee Labs)

Payment Card Number with CVV2	U.S.A	U.K	Canada	Australia	E.U

Software-generated	5€-8€	20€-25€	20€-25€	21€-25€	25€-30€
With Bank ID Number	15€	25€	25€	25€	30€
With Data of Birth	15€	30€	30€	30€	35€
With FULLZ ⁹ info	30€	35€	40€	40€	45€

Payment card data is the most notable stolen data type which is usually sold in the Black Market. The most cost effective solution is a software-generated solution valid number that is created by using some algorithms (Generators) which are able to produce account numbers and CVV2 number and expiration dates “randomly”. For each additional piece of information, the price increases progressively, because criminals can achieve better access to sensitive information. A “full information packet” is called FULLZ.

Another underground market category is accounts that offer Payment Services to the owners. Of course, in this category prices rise according to each account balance. The following table provides information about price ranges in this category.

⁹ A slang term that criminals who steal credit card information use to refer to a complete set of information on a prospective fraud victim. Fullz include, at a minimum, the victim’s name and billing address; credit card number, expiration date and card security code; and Social Security number and birthdate. (*Investopedia.com*)

Table 4: Accounts about payment services (source: McAfee Labs)

Payment Service Account Balance	Estimated Price / account
400€ - 1000€	20€ - 50€
1000€ - 2500€	50€ – 120€
2500€ - 5000€	120€ – 200€
5000€ - 8000€	200€ - 300€

Apart from these categories, cybercriminals sell bank login credentials in order to provide access to Web Banking services. In this way, illegal owners of these credentials can transfer stolen funds of bank accounts on a global scale. Pursuant to McAfee, 2200€ accounts sell for 190€. E.U. accounts with the ability to transfer illegitimate funds varies from 900€ to 16000€ for account balances about 700€ to 10000€.

5.3 Cyber Insurance: *Evolution*

Cyber Insurance and Cyber Liability are two terms that were introduced during the late 90's to satisfy market needs and emerging issues around the use of the Internet. The policies and the products offered were too expensive and limited compared with current similar solutions. The first companies that adopted Cyber Insurance products were world-renowned companies that were active in the Internet Business field like Google, Yahoo etc., whose Cyber Insurance policies include property and liability coverage. It is generally accepted that the Cyber Insurance sector has not been developed greatly and this is due to many factors such as: Cyber Insurance products are quite expensive for the majority of the SME's type business, Cyber Insurance lawsuits are compound and manipulative and last but not least, more of the companies' or organizations' security managers have not realized the severity of Data Breach incidents and the Cyber Insurance products' real value, necessity and utility. Moreover, many companies or organizations wrongly suppose that underlying conventional Insurance policies are sufficient and they offer legal coverage in a case of Data Breach incident.

Because of the foregoing, most of the countries had to develop appropriate legislations in order to protect the increasing digital data format. These legislations obligates companies and organizations that store and/or process personal or sensitive data to discipline and correspond in these privacy policy principles.

As expected, Cyber Insurance and Security legislations have undergone major and significant changes since their first emergence in order to align with the evolution of the Information Technology.

5.4 Data Privacy and Data Protection in Greece

The main Data Protection legislation for the Protection of Individuals with regard to the Processing of Personal Data in Greece is Law 2472/1997. This legislation implements E.U. Directive 95/46/EC and has been modified by the posterior *Data Protection Law*. Below we can see all the existing legislation and meaningful information about Data Privacy Laws in Greece [8]. *Data Protection Authority and Registration Requirements*

1. Authority. Hellenic Data Protection Authority (the “Data Protection Authority”).

1.1Registration. The data controller must notify the Data Protection Authority in writing of the creation and operation of a file or the commencement of processing. The notification must contain:

- the details of the data controller;
- address of all files and places where processing takes place;
- description of the purpose of the processing of personal data;
- the nature of the personal data;
- categories of data subjects;
- duration of processing;
- recipients or categories of recipients to whom personal data are
- announced or transferred; and

- any transfer and the purpose of such transfer of personal data to third countries.

2. *Protected Personal Data*

2.1 *Personal data* is information relating to the data subject. Information of a consolidated statistical nature not enabling the identification of data subjects is not considered as personal data.

2.2 *Sensitive personal data* is data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, social welfare and sexual life, criminal prosecution or convictions, as well as membership in related associations.

3. *Data Collection and Processing*

3.1 *Application.* The Data Protection Law applies where personal data is processed by a data controller or processor established in Greece, in a place where Greek law applies pursuant to public international law, and/or where the data controller is not established in the EU, but uses equipment situated in Greece to process personal data for purposes other than transit. The data controller is responsible for compliance with the Data Protection Law.

3.2 *Processing.* Processing of personal data is only permitted where the data subject has notice and has provided consent to such processing, except where processing is necessary:

- for the execution of a contract to which the data subject is party or for the adoption of measures further to the data subject's request during the pre-contractual stage;
- for compliance with a legal obligation by the data controller;
- in order to protect the vital interests of the data subject, if s/he is physically or legally incapable of giving her consent;
- for the performance of a task carried out in the public interest or in the exercise of public function by a public authority or assigned by it to the data controller or a third party; or
- for the purposes of a legitimate interest pursued by the data controller or a third party or third parties where such an interest prevails over rights and interests of data subjects and their fundamental freedoms are not affected.

3.3 *Notification.* Additionally, notification of the data subject is not necessary where processing:

- is carried out for purposes directly or indirectly related to an employment relationship or works contract or provision of services in the public sector and is necessary for the fulfillment of an obligation imposed by law or for the performance of obligations arising under these relationships where the data subject has been previously notified;
- relates to clients or suppliers provided that data is not disclosed to third parties;
- is administered by unions, companies, associations of persons and political parties and relates to personal data of their members or companies provided they have given their consent and the data is not transferred or disclosed to third parties;
- involves medical data and is carried out by doctors or other persons providing medical services provided the data controller is bound by medical confidentiality or other professional/legal confidentiality and data is not disclosed to third parties;
- is administered by lawyers, notaries public, fee-paid land registrars and court bailiffs and relates to the provision of legal services; provided the controller and its members are bound by a duty of confidentiality and the data is not transferred or disclosed to third parties; or
- is carried out by the judicial authorities in the interests of justice.

3.4 *Sensitive Data.* Under the Data Protection Law, processing of sensitive data is prohibited, except with the prior approval of the Data Protection Authority. Such approval may be granted in the form of a license under specific circumstances, namely where:

- the data subject has consented in writing;
- processing is necessary to protect the vital interests of the data subject or third-party interest provided by law, if the data subject is incapable of giving her consent;
- processing relates to data published by the data subject or is necessary for the recognition, exercise or defense of a right in court or before a disciplinary body;

- processing relates to health matters and is carried out by a health professional under a duty of confidentiality where needed for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services;
- processing is carried out by a public authority and is necessary for national security, criminal or correctional policy and aids detection of offenses, criminal convictions or security measures, protection of public health or exercise of public control of fiscal or social services;
- processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained; or
- processing concerns data relating to public figures, provided that such data are in connection with a public office or the management of third party interests and is carried out solely for journalistic purposes. The license is only granted where processing is absolutely necessary to ensure the right to information on matters of public interest, as well as literary expression and provided that the rights to privacy and family life are not infringed.

4 *Data Transfer*

4.1 Without further requirements being necessary, data transfer is permitted within the European Economic Area (EEA).

4.2 Outside the EEA, data transfer is permitted to countries that the Data Protection Authority has granted a license based on a finding that those countries' laws provide an adequate level of protection to personal data.

4.3 Countries with an adequate level of protection also include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

4.4 A license is not required to transfer data to countries that the European Commission has deemed to have adequate levels of protection; however, transfer of data to such countries requires a transfer form be completed informing the Data Protection

Authority of the transfer absent a license. The data controller should provide evidence of Safe Harbor certification where applicable.

4.5 Transfers outside the EU to a country that does not ensure an adequate level of protection will be allowed after a license has been granted by the Data Protection Authority provided that one or more conditions occur:

- the data subject has consented;
- transfer is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent;
- transfer is necessary for the conclusion of a contract between the data subject and the data controller or between a third party and the data controller for the benefit of the data subject;
- transfer is necessary for the performance of pre-contractual measures at the request of the data subject;
- transfer is necessary to safeguard a superior public interest, especially the performance of a cooperation agreement with public authorities of another country where the data controller provides adequate safeguards for the protection of the data subject's privacy and rights;
- transfer is necessary for the establishment, exercise or defense of a right in court;
- transfer is made from a public register, which provides information to the public and is accessible by any member of the public who can demonstrate a legitimate interest; or
- where the data controller ensures that personal data and the rights of the data subject are adequately protected.

A license is not required where standard contractual clauses are in place, which would also need to be submitted and would be accepted provided there is no deviation from the standard terms. Although not included in the Data Protection Law, the Data Protection Authority also examines binding corporate rules for the purposes of approving intra-group transfers.

The Data Protection Law specifies that, if data processing is carried out on the data controller's behalf by a processor, there must be a written assignment. The assignment must provide in its terms that the processor will abide by the

data controller's instructions as regards the data processing and will also comply with the confidentiality requirements.

5 *Data Security*

Processing of data must be confidential and carried out by persons acting on instructions from the data controller or processor.

The data controller is required to select persons with relevant professional qualifications, which provide adequate guarantees of technical knowledge and integrity. The data controller must additionally implement appropriate technical and organizational methods for the security of data in order to protect data from accidental or unlawful destruction or loss, alteration or unauthorized disclosure, and any other type of unlawful processing.

6 *Breach notification*

There are no requirements under the Data Protection Law requiring notification in the event of a breach; however, the Act for the Protection of Personal Data and Privacy (Law 3471/2006 Article 12) in the Electronic Communications Sector does have breach notification requirements that apply to providers of electronic communications.

7 *Enforcement and Penalties*

7.1 The DPA may impose sanctions and penalties after an investigation undertaken either on its own initiative or pursuant to a complaint from another party.

7.2 If there is a breach of the data protection rules, the DPA may impose administrative sanctions on the data controller or any of its representatives.

Such sanctions include:

- an order that the violation cease within a specified time limit;
- fines ranging from approximately €1,000 – €140,000; and
- in the event of more serious or repeated violations, a temporary or permanent revocation of the data controller or processor's license to process data and/or an order requiring the data controller to delete the data.

7.3 *Criminal sanctions* may apply for certain actions, including failure to notify the DPA that a file is being established, for failure to notify the DPA of any change to the conditions of processing that formed the basis for the permit or for breach of the permit. Criminal penalties may also apply for unlawfully interfering with personal data file, altering or affecting a personal data file in a harmful manner or disclosing or making a personal data file accessible to unauthorized persons. Criminal penalties also apply to the

unauthorized party who accepts or affects the personal data. Criminal sanctions may consist of imprisonment of up to three years and a financial penalty ranging from approximately €3,000 to €30,000.

7.4 *Civil liability* may result where a natural person or legal entity should have been aware that damage to another was likely. Civil recoveries could include an order of injunctive relief on behalf of the data subject, full compensation for damage to property and compensation for moral damages of at least €6,000 (unless a lesser amount is claimed).

6 DB.Est (Data Breach Estimation tool)

In this chapter, the DB.Est (*Data Breach Estimator*) is presented, which is a web application that enables the user to estimate the risk for his/her organization to suffer a Data Breach by answering a group of specific questions. Hereafter the application allows to user to calculate the Recovery Cost from a breach incident as well as to find out how each action or/and measure with respect to security, can affect the above mentioned metrics.

6.1 Application presentation

In order to provide as accurate results as possible, the specific questions have been created taking into account the most precise and recent global surveys/research about Data Breach occurrences. [10] [11]

6.1.1 Data Breach: probability/risk estimation

The following questions are extracted from the previously mentioned research to estimate a company's risk exposure to a Data Breach.

- *Question 1:* Company/Organization Location
- *Question 2:* Type of organization / company
- *Question 3:* Type of Information processed / Information Sensitivity
- *Question 4:* Presence of a Chief Information Security Officer (CISO) or a Security Manager
- *Question 5:* Permissions / Privileges for limit access to sensitive data (Scalable Security Model)
- *Question 6:* How would you describe your Employees' Security Training Level?
- *Question 7:* User account review & control (e.g Mandatory password change periodically)
- *Question 8:* Are there any password requirements/restrictions in order to create an account?
- *Question 9:* Does the organization use any encryption tools (cryptologic tools, tokenization)?

6.1.2 Data Breach Recovery Cost Calculation

The following questions are extracted from the previous mentioned researches to calculate the Recovery Cost from for a company, in case of a Data Breach.

- *Question 1:* What is your company type?
- *Question 2:* What type of information does the company store / process?
- *Question 3:* What is your company sector of operation?

- Question 4: What is your company development model for Data storage and processing?
- Question 5: How many records are stored in your database [aggregate, with respect to employees, customers or patients]?

6.2 Dempster – Shafer Theory

In addition, to help the user comprehend and consider the risk exposure level and its implication, we include the Dempster – Shafer Theory in order to create some types of Data Breaches and produce more accurate estimations than a simple estimation probability [11]. In the 70's, Shafer developed the Evidence Theory, just to extent the Probability Theory. Meanwhile, we will explain how the Evidence Theory works, what is its denotation and its semantics.

.

We assume a variable q and the total of all possible values S . Hence we consider that: “Variable q has a value in the mass M ”, M is a subset of S . The variable q can be assumed as an arbitrary parameter that takes Numeric or non-Numeric values. The mass S it is called “frame of discernment” of variable q . The $P(S)$ (the power-set of S) can be considered as the sum of the events of which each one corresponds to one specific sentence. That model uses the known method of assigning a number between zero (0) and one (1) to present the degree of support in a potential, based on the available evidence. This is accomplished by a function m which is called Basic Probability Assignment and represents the amount of Belief in each subset of value S (the amount of belief in a value or combination of values S). The base assign probability m is a function $P(S)$ (power-set of S) on $[0,1]$ such that:

- 1) $m(\emptyset) = 0$
- 2) $\sum_{A \subseteq E} m(A) = 1$

Of course, the $m(A)$ amount, counts the belief(persuasion) directly to A , but does not take into account the overall belief in A based on the beliefs of its subsets. So, we define

another function of belief (*Belief function*) or (*Credibility measure*) $Bel(A)$ or $Cr(A)$ as following:

$$Bel(A)=Cr(A)=\sum_{B \subseteq A} m(B) \quad (1)$$

Similarly we define a *Plausibility Measure*, denoted as $Pl(A)$:

$$Pl(A) = 1 - Cr(\sim A)$$

Reasonable, it can be proved that:

$$Pl(A)=\sum_{A \cap B \neq \emptyset} m(B) \quad (2)$$

6.2.1 Application of the Dempster - Shafer theory to the Data Breach estimation.

In order to apply the Dempster – Shafer theory to the Data Breach estimation case we define the following events:

- Convention Data Breach (Low Risk Data Breach) (C)
- High Risk Data Breach (H)
- No Data Breach (N)

So, we have the following possible events for a Data Breach in which we assign a possible mass by consulting the global surveys we mentioned before (5.1):

Table 5: Power – set probabilities mass assignation to the events.

EVENT	MASS
No-one is possible	0
C (Conventional Data Breach)	0.2
H (High Risk Data Breach)	0.23
N (No Data Breach)	0.12
CH (either Conventional Data Breach or High Risk Data Breach)	0.15
CN (either Conventional Data Breach or No Data Breach)	0.08
HN (either High Risk Data Breach or No Data Breach)	0.12
CHN (one of three (3) events are possible to take place)	0.1

From the above Table X, we have:

Belief in A:

Example:

$$(1) \quad \text{bel}(\{C\}) = m(\{C\}) = 0.2$$

$$\text{bel}(\{C,H\}) = m(\{C\}) + m(\{H\}) + m(\{C,H\}) = 0.2 + 0.23 + 0.15 = 0.58$$

So, overall we have the results in the table below:

Table 6: Belief functions: results

	C	H	N	CH	CN	HN	CHN
m(A)	0.20	0.23	0.12	0.15	0.08	0.12	0.1
bel(A)	0.20	0.23	0.12	0.58	0.40	0.47	1.0

Plausibility of A: pl(A)

Example:

$$(2) \text{pl}(\{C,H\}) = m(C)+m(H)+m(C,H)+m(C,N) \\ +m(H,N)+m(C,H,N) = 0.2 + 0.23 + 0.15 + 0.08 + 0.12 + 0.1 = 0.88$$

So, overall we have the results in the table below:

Table 7: Plausibility functions: results

A	C	H	N	CH	CN	HN	CHN
m(A)	0.20	0.23	0.12	0.15	0.08	0.12	0.1
pl(A)	0.53	0.60	0.48	0.88	0.77	0.80	1.0

Belief Interval of A, is the definition of A with respect to certainty associated with a given subset [bel(a) pl(a)]. For instance, the belief interval of (C,N) is [0.15, 0.88].

Table 8: Plausibility and Belief functions: results (aggregated)

A	C	H	N	CH	CN	HN	CHN
m(A)	0.20	0.23	0.12	0.15	0.08	0.12	0.1
bel(A)	0.20	0.23	0.12	0.58	0.40	0.47	1.0
pl(A)	0.53	0.60	0.48	0.88	0.77	0.80	1.0

The probability A takes values between bel(A) and pl(A) and also bel(A) represents the evidence we have for A directly. So, prob(A) *cannot be less than this value*.

Conclusively, with Dempster – Shafer theory we have the ability to give a degree of certainty of our beliefs.

- A *small* difference between bel(A) and pl(A) (belief and plausibility) reveals a *Certainty* about our belief.
- A *large* difference between bel(A) and pl(A) (belief and plausibility) reveals an *Uncertainty* about our belief.

However, even with a zero (0) difference (interval) between $bel(A)$ and $pl(A)$, our conclusion is *probably* right, *not definitely* right.

6.2.2 Dempster – Shafer Scenarios / Validation

In order to validate the Dempster – Shafer in DB.Est (Data Breach Estimator) application in practice, we will examine some scenarios, in which an organization or company (User) fills the question form we mentioned in Chapter 5.1.1. The reason why we chose a Latin America based company to conduct the validation scenarios is that according to data of global surveys, organizations and companies in Latin America have the highest risk of suffering Data Breach incidents. Also, the Healthcare industry is a sector targeted by such malicious attacks.

➤ Scenario 1: Questions - Answers

Table 9: Scenario (1) Completed Form

<i>Question</i>	<i>Answer</i>
Question 1: Company/Organization Location.	Latin America
Question 2: Type of organization / company.	Healthcare
Question 3: Type of Information processed / Information Sensitivity.	Patient Data / Healthcare Info
Question 4: Presence of a Chief Information Security Officer (CISO) or a Security Manager.	No

Question 5: Permissions / Privileges for limited access to sensitive data (Scalable Security Model).	Lax Security Model
Question 6: How would you describe your Employees' Security Training Level?	Moderate
Question 7: User account review & control (e.g. Mandatory password change periodically).	N
Question 8: Are there any password requirements/restrictions in order to create an account?	Minimum Length restriction (only).
Question 9: Does the organization use any encryption tools (cryptologic tools, tokenization)?	No

So, by consulting global surveys we mentioned before, we assign the following mass probabilities to the following events (5.2.1):

Table 10: Scenario (1) Power – set probabilities mass assignment to the events.

EVENT	MASS
None is likely	0
C (Conventional Data Breach)	0.2
H (High Risk Data Breach)	0.23
N (No Data Breach)	0.12
CH (either Conventional Data Breach or High Risk Data Breach)	0.15
CN (either Conventional Data Breach or No Data Breach)	0.08
HN (either High Risk Data Breach or No Data Breach)	0.12

CHN (one of three (3) events are likely to take place)	0.1
--	-----

Applying the Dempster – Shafer theory, we have the following results presented in the table below.

Table 11: Scenario (1) Plausibility and Belief functions: results (aggregated)

A	C	H	N	CH	CN	HN	CHN
m(A)	0.20	0.23	0.12	0.15	0.08	0.12	0.1
bel(A)	0.20	0.23	0.12	0.58	0.40	0.47	1.0
pl(A)	0.53	0.60	0.48	0.88	0.77	0.80	1.0

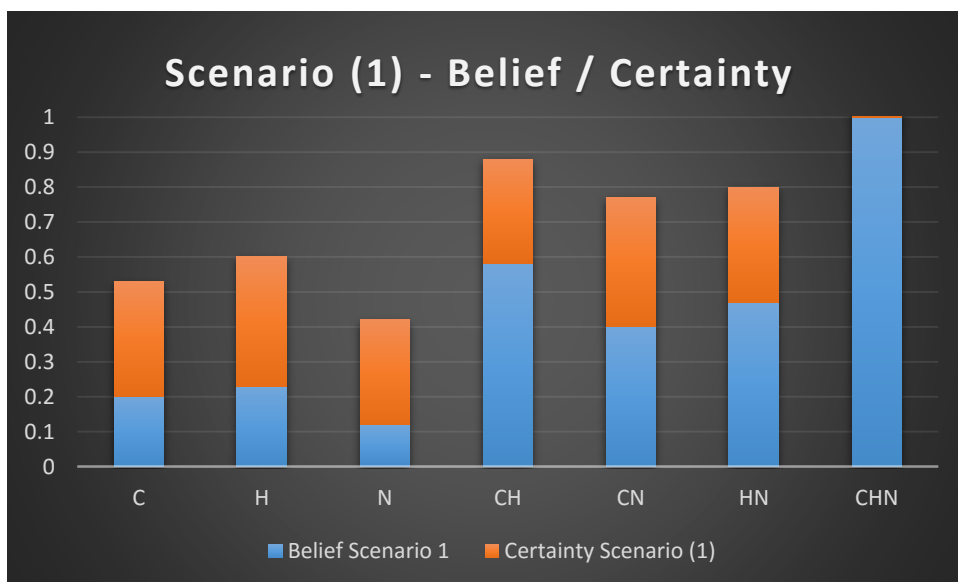


Figure 14: Scenario (1) Belief bel(a) / Certainty for each Data Breach event type

Figure 14 deals with Belief and Certainty about Scenario (1). It highlights the Belief values compared to Certainty about each Data Breach Type.

The orange bar shows the Certainty (the lower the value, the higher the Certainty) and the blue depicts the Belief (bel(A) represents the evidence we have for A directly). So, prob(A) cannot be less than this value. As we can observe, it is likely for a Data Breach to occur but more worrying is that High Risk Data Breach is more likely than Conventional Data Breach to happen, which means that the organization or company can suffer irreparable damage. The highest bel(A) (probability) value belongs to CHN (one of three (3) events are likely to take place) as it was expected, followed by CH (Conventional or High Risk Data Breach) with a Certainty similar to the other breach events. Conclusively, it is obvious that with these lax security measures we cannot ensure data integrity and achieve high level of information security. This is why No Data Breach event type bel(A) has quite low values as well as low Certainty.

➤ *Scenario 2: Questions –Answers*

Table 12: Scenario (2) Completed Form
 (*differences, compared to the previous scenario)

Question	Answer
Question 1: Company/Organization Location.	Latin America
Question 2: Type of organization / company.	Healthcare
Question 3: Type of Information processed / Information Sensitivity.	Patients Data / Healthcare Info
Question 4: Presence of a Chief Information Security Officer (CISO) or a Security Manager.	No

Question 5: Permissions / Privileges for limited access to sensitive data (Scalable Security Model).	Strict Security Model*
Question 6: How would you describe your Employees' Security Training Level?	Well-enough level*
Question 7: User account review & control (e.g. Mandatory password change periodically).	Yes*
Question 8: Are there any password requirements/restrictions in order to create an account?	Required use of numbers and characters (only)*
Question 9: Does the organization use any encryption tools (cryptologic tools, tokenization)?	No

Table 12 shows the answers after several changes in the organization's security policy and planning. Those changes affect the mass we assign to the events as follows:

Table 13: Scenario (2) Power – set probabilities mass assignment to the events.

EVENT	MASS
None is likely	0
C (Conventional Data Breach)	0.16
H (High Risk Data Breach)	0.10
N (No Data Breach)	0.40
CH (either Conventional Data Breach or High Risk Data Breach)	0.10
CN (either Conventional Data Breach or No Data Breach)	0.07

HN (either High Risk Data Breach or No Data Breach)	0.08
CHN (one of three (3) events are likely to take place)	0.09

Applying the Dempster – Shafer theory, we have the following results presented in the table below.

Table 14: Scenario (2) Plausibility and Belief functions: results (aggregated)

A	C	H	N	CH	CN	HN	CHN
m(A)	0.16	0.10	0.40	0.10	0.07	0.08	0.09
bel(A)	0.16	0.10	0.40	0.36	0.63	0.58	1.0
pl(A)	0.42	0.37	0.64	0.60	0.90	0.84	1.0

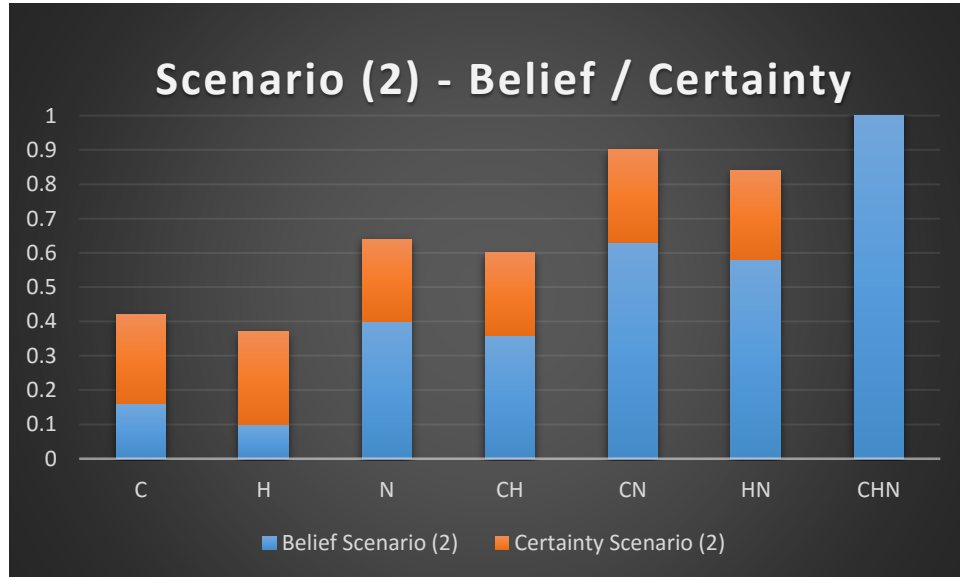


Figure 15: Scenario (2) Belief bel(a) / Certainty for each Data Breach event type

In this Scenario (2), by adopting the significant policy/rules described in Table 12, the Belief probability of not suffering from a Data Breach (N) significantly increases and also there is great Certainty for this to happen. Moreover, in contrast to Scenario (1), it is

likely to suffer a Conventional breach instead of High Risk Data Breach, which is a very important achievement. Combined breach events (including N) have the highest Belief bel(a) probability values and more Certainty than C or H events. So, we conclude that we managed to reduce the probability of a High Risk Data Breach event while at the same time we increase the probability of not being breached or not suffering a breach of vital importance. So, at the next Scenario (3) we will try to further increase safety levels, by implementing stricter security measures and policies

➤ *Scenario 3: Questions –Answers*

Table 15: Scenario (3) Completed Form (**differences, compared to the previous scenario*)

<i>Question</i>	<i>Answer</i>
Question 1: Company/Organization Location.	Latin America
Question 2: Type of organization / company.	Healthcare
Question 3: Type of Information processed / Information Sensitivity.	Patients Data / Healthcare Info
Question 4: Presence of a Chief Information Security Officer (CISO) or a Security Manager.	Yes*
Question 5: Permissions / Privileges for limited access to sensitive data (Scalable Security Model).	Strict Security Model
Question 6: How would you describe your Employees' Security Training Level?	Excellent level*
Question 7: User account review & control (e.g. Mandatory password change periodically).	Yes*

Question 8: Are there any password requirements/restrictions in order to create an account?	All the above (or a combination of the above) -Minimum Length restriction - -Required use of numbers and characters- -Required use of special characters-
Question 9: Does the organization use any encryption tools (cryptologic tools, tokenization)?	Yes

Table 15, shows the answers after several changes in the organization’s security policy and planning. Those changes affect the mass we assign to the events as below:

Table 16: Scenario (3) Power – set probabilities mass assignment to the events.

EVENT	MASS
None is likely	0
C (Conventional Data Breach)	0.12
H (High Risk Data Breach)	0.04
N (No Data Breach)	0.60
CH (either Conventional Data Breach or High Risk Data Breach)	0.05
CN (either Conventional Data Breach or No Data Breach)	0.06
HN (either High Risk Data Breach or No Data Breach)	0.04
CHN (one of three (3) events are likely to take place)	0.09

Applying the Dempster – Shafer theory, we have the following results presented in the table below.

Table 17: Scenario (3) Plausibility and Belief functions: results (aggregated)

A	C	H	N	CH	CN	HN	CHN
m(A)	0.12	0.04	0.60	0.05	0.06	0.04	0.09
bel(A)	0.12	0.04	0.60	0.21	0.78	0.14	1.0
pl(A)	0.32	0.22	0.25	0.40	0.96	0.88	1.0

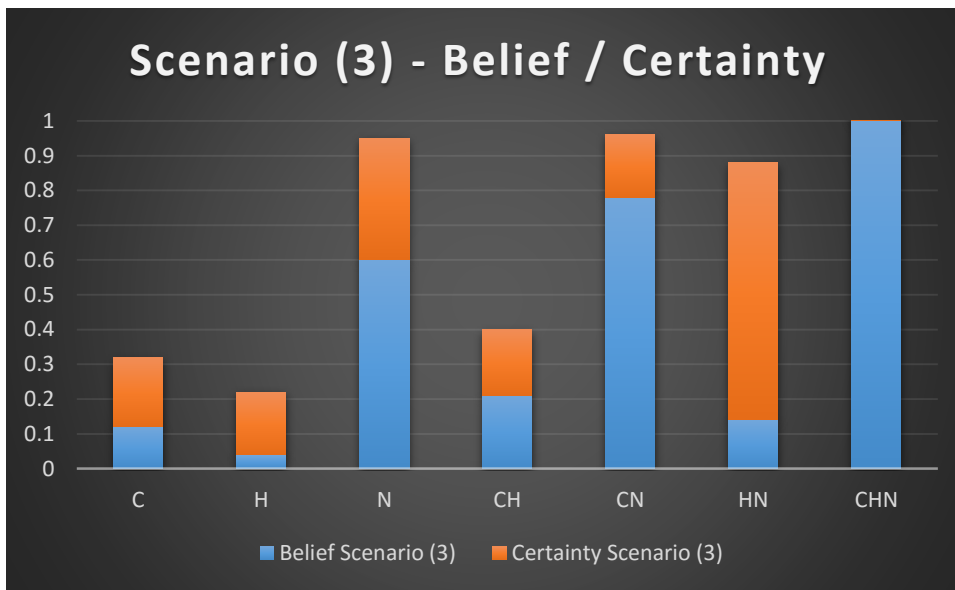


Figure 16: Scenario (3) Belief bel(a) / Certainty for each Data Breach event type

Figure16 shows a bar chart following the adoption of the most stringent measures and policies in order to reduce the probability of any Data Breach type. As we observe, the Belief pl(A) probability value for No Data Breach case (N) has sharply increased, but as expected, it has no high Certainty because we cannot eliminate the possibility of a Data Breach occurring. Nevertheless, the probability of a High Risk Data Breach (H) and (HN) has been minimized (also in H case, with high Certainty). So, we can be assured that in the event of a Data Breach, it is more likely that a conventional breach will occur (Low Risk Data Breach), which will not significantly affect the vital business operations of the organization or company.

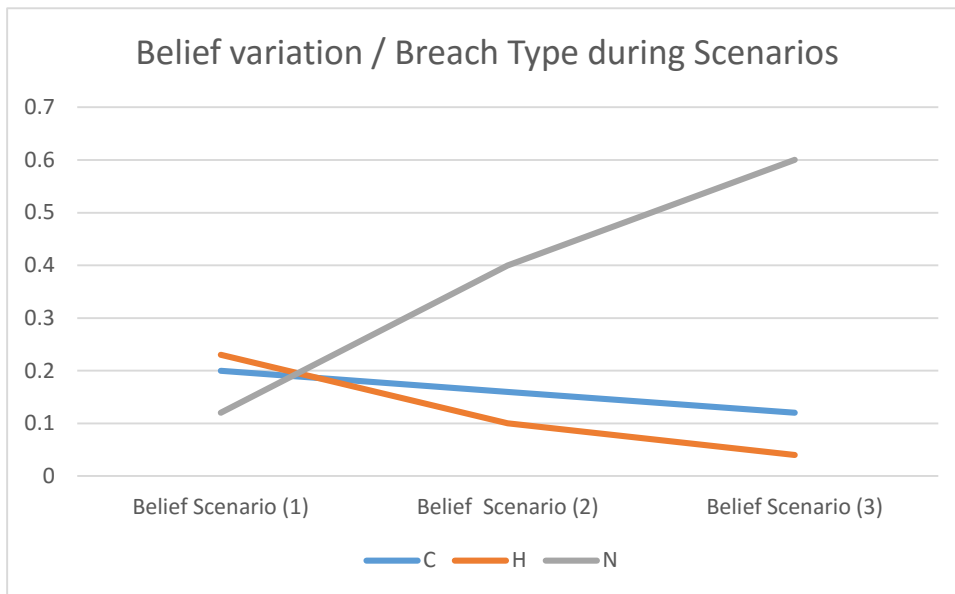


Figure 17: Belief variation for each Data Breach type (C, H and N) over Scenarios.

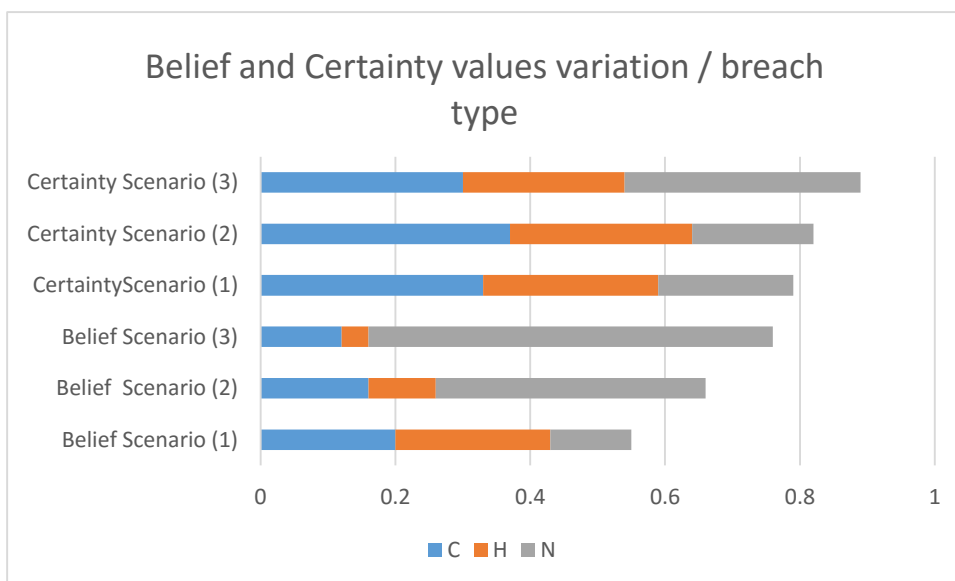


Figure 18: Belief and Certainty variation for each Data Breach type (C, H and N) over Scenarios.

Figure 17 and Figure 18 show the Belief variation from Scenario (1) to Scenario (2) and then to Scenario (3) as a result of the change that occurred in the security measures of the

organization in order to increase the protection and ensure the integrity of data which may be processed or be stored by the organization. From these figures it is clear that No Data Breach type probability has risen sharply without significant Certainty reduction. Moreover, probabilities of High Risk Data Breach and Conventional Data Risk have been greatly reduced.

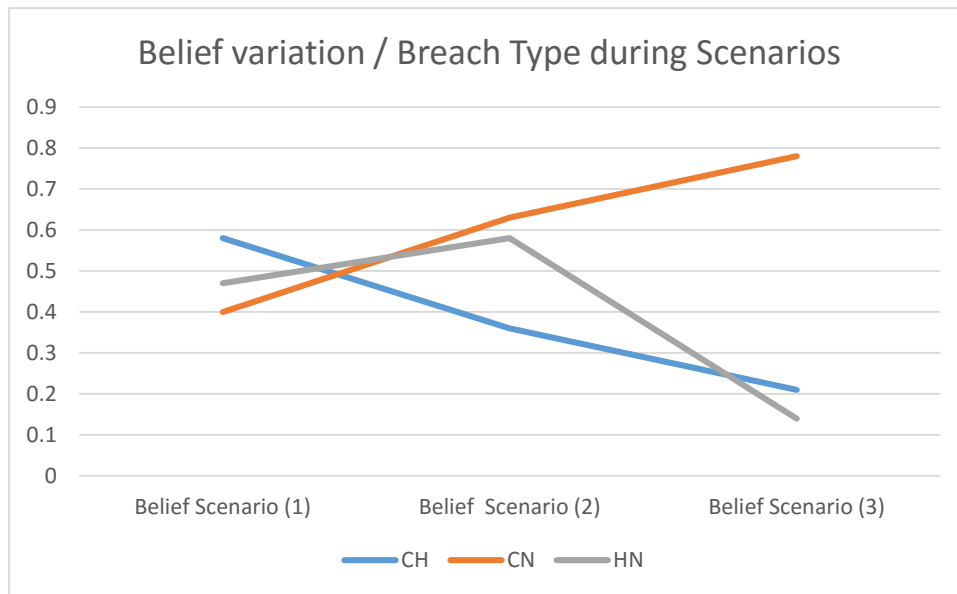


Figure 19: Plausibility variation for each Data Breach type (CH, CN and HN) over Scenarios.

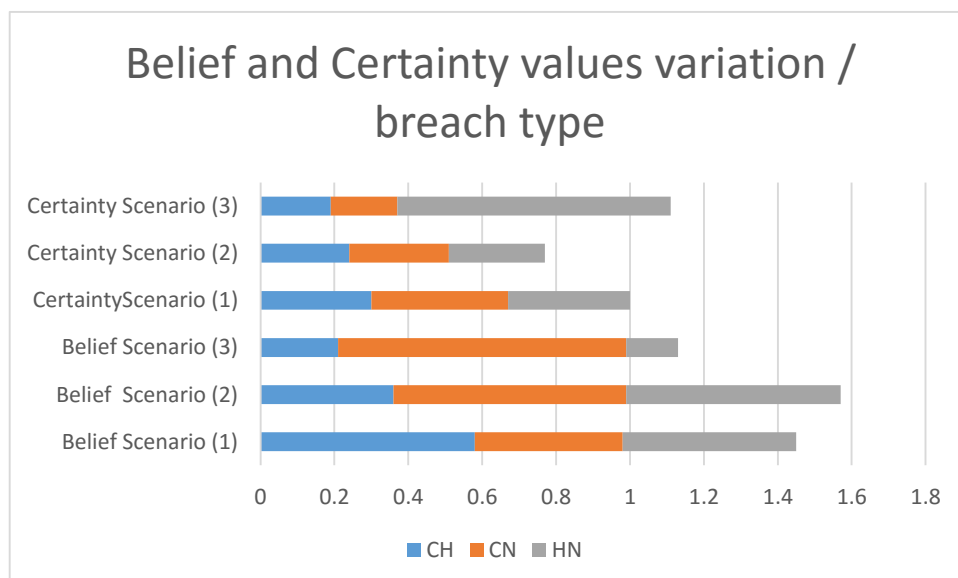


Figure 20: Belief and Certainty variation for each Data Breach type (CH, CN and HN) over Scenarios.

Figure 19 and Figure 20 show the Belief variation from Scenario (1) to Scenario (2) and then to Scenario (3) following the adoption of the most stringent measures and policies in order to reduce the probability of any Data Breach type and at the same time to increase the protection and ensure the integrity of data which may be processed or be stored by the organization. From Figure 19 it is clear that we manage to significantly reduce the probability of CH (Conventional or High Data Breach). But also, we should mention that Scenario (2) HN (High or No Data Breach) type *still presents a strong probability of occurring*. This is due to the necessity and the importance of the security countermeasures we did not include in Scenario (2) (e.g. encryption tools, Chief Information Security Officer (CISO)).

7 Conclusion

This dissertation tried to provide a different approach to the way that Data Breach event probability is estimated. By introducing the ISMS while indicating ways to deploy and improve secure business networks, it presents the severity of Data Breach events and their consequences as well as analyzing the Cybersecurity fundamentals. Moreover, it studies two of the most important methods of maintaining a high level of Information Security by presenting their lifecycles and their phases: Risk Management and Risk Assessment. After researching the Greek but also the global Cyber Insurance market, the current situation is presented but also the perspectives and the future trends this field. Consequently, by applying the combining evidence probability to various Data Breach events, we manage to introduce a more accurate and combined estimation method that highlights the most important security measures and their contribution to the overall security strategy of an organization or a company as well as testing their performance and comparing different scenarios. Results showed that moderate Information Security measures are able to increase organization confidence against common threats and vulnerabilities by decreasing Conventional Data Breach events. Nevertheless, strict,

contemporary and devoted security measures are mandatory for an organization to ensure its integrity against High Risk Data Breaches and protect its reputation.

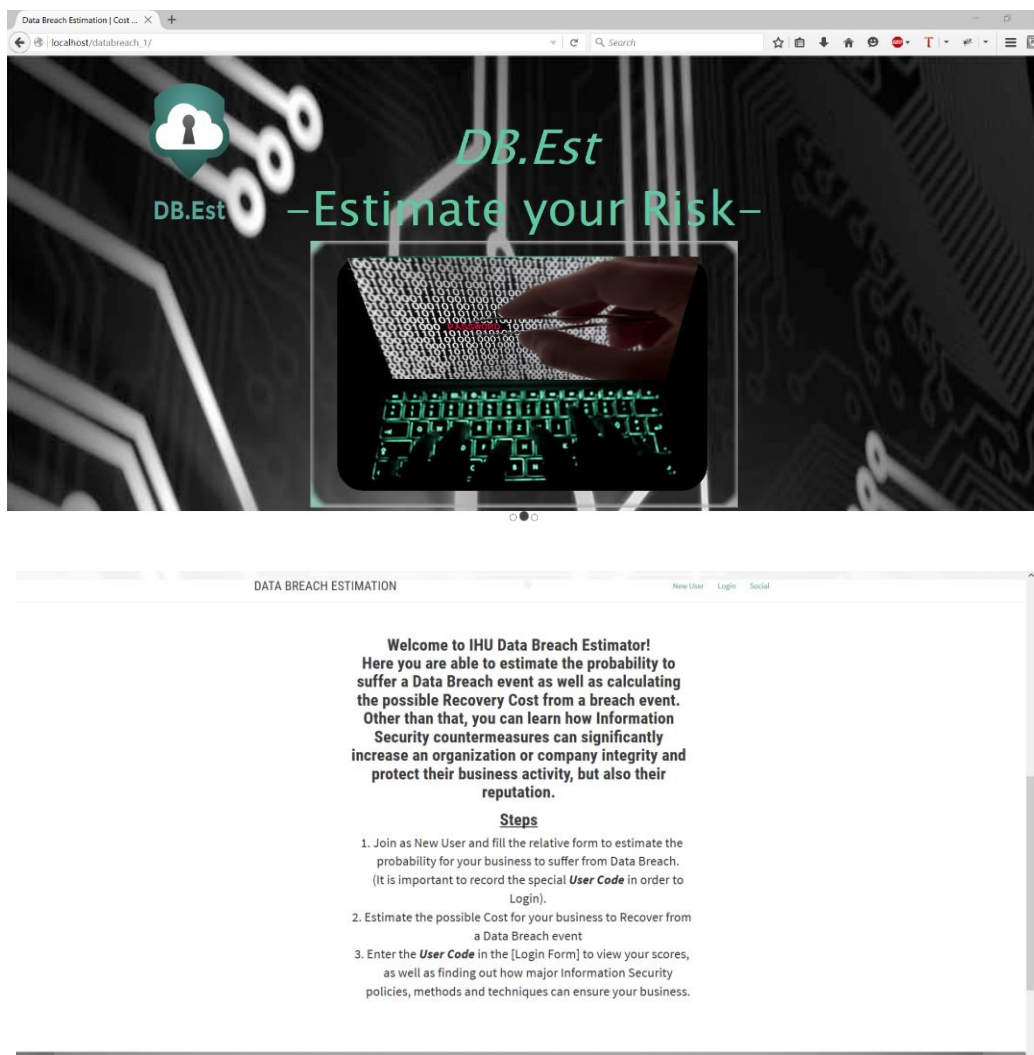
Bibliography

- [1] European Union Agency for Network and Information Security
<http://www.enisa.europa.eu>
- [2] BSI- Standard 100-1, Information Security Management Systems.
<http://www.bsi.bund.de/grundschutz>
- [3] Real World Business Technology
www.tomsitpro.com
- [4] <http://perspectives.avalution.com>
- [5] Data Breach Investigation Reports 2011(DBIR) (Verizon)
- [6] asfalistikomarketing.gr
- [7] <https://report.kaspersky.com/>
- [8] Myth 2: The Greek companies do not face incidents of violation systems & data loss. Nikos Georgopoulos CyRM
- [9] 2015 International Compendium of Data Privacy Laws, BakerHostetler
- [10] Kaspersky Lab – Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series
- [11] Ponemon - 2014 Cost of Data Breach Study: Global Analysis
- [12] Application of Dempster-Shafer theory in condition monitoring applications:
Chinmay R. Parikh, Michael J. Pont1 and N. Barrie Jones
Research Group Department of Engineering University of Leicester, UK

Appendix: DB.Est

DB.Est (Data Breach estimation tool): *User Manual & sample source code*

1) index.html



index.html : *Sample source code:*

```
<div class="navbar-header">
    <button type="button" class="navbar-toggle" data-
toggle="collapse" data-target=".navbar-ex1-collapse">
    <span class="sr-only">Toggle navigation</span>
    <span class="icon-bar"></span>
    <span class="icon-bar"></span>
    <span class="icon-bar"></span>
</button>

<!--Replace text with your app name or logo image-->
<a class="navbar-brand" href="#">Data Breach Estimation</a>

</div>
<div class="collapse navbar-collapse navbar-ex1-collapse">
    <ul class="nav navbar-nav">
        <li><a onclick="$('header').animateScroll({padding:71});" <a
href="newuser.php">New User</a></li>
        <li><a onclick="$('.detail').animateScroll({padding:71});" <a
href="loginForm.php">Login</a></li>
        <li><a
onclick="$('.social').animateScroll({padding:71});">Social </a></li>
    </ul>
</div>
</div>
```

2) newuser.php

DATA BREACH ESTIMATION

Choose the model that characterize your organization more. ▾

How would you describe your Employees' Security Training Level?

Choose the level that characterize your Employees more. ▾

User account review & control (e.g. Mandatory password change periodically).

Choose Yes/No. ▾

Are there any password requirements/restrictions in order to create an account?

Choose the requirement/restriction type (if there is). ▾

Does the organization use any encryption tools (cryptologic tools, tokenization)

Choose Yes/No. ▾

submit

newuser.php: *Sample source code*

```
//select the Data Base
```

```
mysql_select_db("databreach_1");
```

```

//create userCode randomly

function generateRandomString($length = 10) {
    $characters=
'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = "";
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[rand(0, $charactersLength - 1)];
    }
    return $randomString;
}

//call function and parse result on $userCode
$userCode=generateRandomString($length = 10);

//insert into DataBase

$ins=mysql_query("INSERT INTO `estimation_1`
(location, userCode, organizationType, infoType, ciso, permissions,
securityTrainingLevel, accountControl, passwordRestrictions,
encryptionTools)
VALUES ($loc', '$userCode', '$orgType', '$infoType', '$ciso',
'$permissions', '$securityLevel', '$accountControl',
'$passwordRestrictions',
'$encryptionTools' )",$conn)

or

die(mysql_error());

```

```
//GET data from mySQL DB and print them

$getData = 'SELECT estimation_1.id, estimation_1.location,
estimation_1.organizationType, estimation_1.infoType, estimation_1.ciso,
estimation_1.permissions, estimation_1.securityTrainingLevel, estimation_1.acountControl,
estimation_1.passwordRestrictions, estimation_1.encryptionTools

FROM estimation_1

ORDER BY estimation_1.id DESC

LIMIT 1;';
```

3) newuser.php (submit)

DATA BREACH ESTIMATION

Choose Yes/No

Are there any password requirements/restrictions in order to create an account?

Choose the requirement/restriction type if there is

Does the organization use any encryption tools (cryptologic tools, tokenization)?

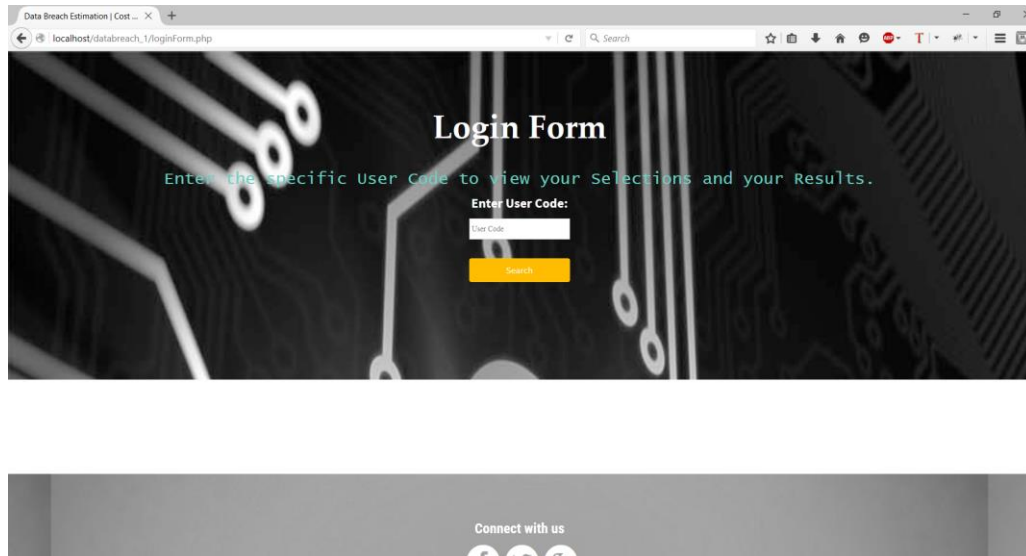
Choose Yes/No

submit

User code:
oZvQXFyIQU

Use this code to enter in the Login form.

4) loginForm.php



loginForm.php: *Sample source code*

```
<div class="collapse navbar-collapse navbar-ex1-collapse">
    <ul class="nav navbar-nav">
        <li><a onclick="$('header').animateScroll({padding:71});" <a
href="newuser.php">New User</a></li>
        <li><a onclick="$('.detail').animateScroll({padding:71});" <a
href="loginForm.php">Login</a></li>
        <li><a
onclick="$('.social').animateScroll({padding:71});">Social </a></li>
    </ul>
</div>
</div>
</nav>
<!-- HEADER
<header style="height:700px">
```

```
<h2 id="calc">Login Form</h2>
```

```
<div class="question" >Enter the specific User Code to view  
your Selections and your Results. <a href="index.php?help=2&width=475"  
class="jTip" id="two" rel= "Help & Information"></a>
```

```
</div>
```

```
<div class="login">
```

```
<form action="" method= "post">
```

```
<label>Enter User Code: </label><br/>
```

```
<input id="userCode" name="userCode" placeholder="User Code"  
type="text">
```

```
<br/><br/>
```

```
<input name="submit" type="submit" value="Search">
```

```
</form>
```

```
</div>
```

```
</header>
```

```
<?php
```

```
include ('loginSearch.php');
```

```
?>
```

5) loginSearch.php: *Sample source code*

```
<?php
```

```
session_start();
```

```

        $error="";
if(isset($_POST['submit'])){
if(empty($_POST['userCode'])){

                                echo $error = "You have not enter a User Code";

                                }

else

        {
        $userCode=$_POST['userCode'];

        $conn = mysqli_connect("localhost", "root", "", "databreach_1");

        if($conn === false){
        die("ERROR: Could not connect. " . mysqli_connect_error());
                                }

        //protect MySQL injection for Security issues
        $userCode = stripslashes($userCode);
        //$userCode = mysql_real_escape_string($userCode);
        $conn=@mysqli_connect("localhost","root","");

        mysqli_select_db("databreach_1");

```

```

// SQL query to fetch information of registered users and finds user match.
$query = mysql_query("select * from estimation_1 where userCode='$userCode'",
$conn);

$est = mysql_query("select estimation_1.breachEst from estimation_1 where
userCode='$userCode'", $conn);

$rows = mysql_num_rows($query);

if(mysql_num_rows($query)== 0){
    echo "Invalid User Code";
}

else
{
    echo "<table>";

    while($rows = mysql_fetch_array($query)){
        /*** 1 LOCATION ***/
echo "<tr>";

        if($rows['location']=== '0.15')
echo '<td><th>Location:</th><th> Europe</th></td>';

        if($rows['location']=== '0.33')

echo '<td><th>Location:</th><th> North America</th></td>';

```



```
if($rows['location']=== '0.16')
```

```
    echo '<td><th>Location:</th><th> Asia</th></td>';
```

```
if($rows['location']=== '0.25')
```

```
    echo '<td><th>Location: </th><th>Asia Pacific</th></td>';
```

```
if($rows['location']=== '0.4')
```

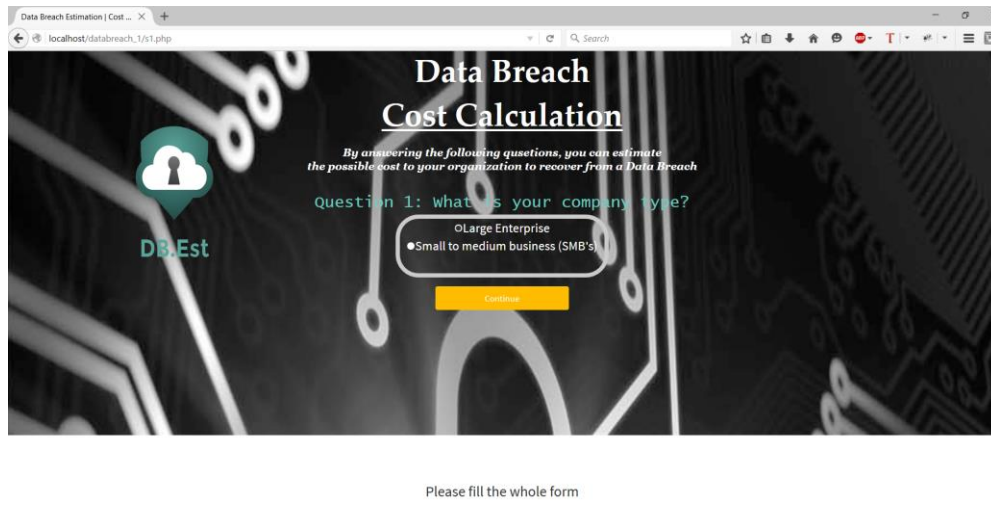
```
    echo '<td><th>Location:</th><th> Latin America</th></td>';
```

```
if($rows['location']=== '0.13')
```

```
    echo '<td><th>Location: </th><th>Middle East and Africa</th></td>';
```

```
echo "</tr>";
```

6) s1.php



s1.php: Sample source code

```
<header>
```

```
<h2 id="calc">Data Breach </h2><h2 id="calc2"> Cost Calculation</h2>
```

```
<div class="container">
```

```
<div class="row">
```

```

```

```
<div class="costQuest" style="font-size:24px">By answering the following  
quesitions, you can estimate <br> the possible cost to your organization to recover from a  
Data Breach</div> <br/><br/>
```

```
<div class="question" >Question 1: What is your company type?
```

```
<a href="index.php?help=2&width=475" class="jTip" id="two" rel=  
"Help &amp; Information"></a>
```

```
</div>
```

```

<form method="post" action="">
  <div class="answer" >

      <input type="radio" name="companySize" value="61000">Large
Enterprise</input><br/>
      <input type="radio" name="companySize" value="7000">Small to medium business
(SMB's)</input><br/><br/>
  </div>
  <br/>
  <input type="submit" name="submit" value="Continue"/>

```

7) test.php: *Sample source code*

```

<?php
    //Check if PHP session has already started
    if (session_status() == PHP_SESSION_NONE) {

        session_start();

        /***** QUESTION 1 *****/

        if (isset($_POST['companySize'])){

            header("Location: s2.php?");

            $comSize =$_POST['companySize'];

            $_SESSION['arr'][]=$comSize;

```

```

        $arr=$_SESSION['arr'];

    }

    //Check if an answer has been selected
/*else{
        echo "<script type='text/javascript'>alert('failed!')</script>";
    }*/

/***** QUESTION 2 *****/

    if (isset($_POST['infoType'])){

        header("Location: s3.php");

        $infoType =$_POST['infoType'];
        $_SESSION['arr'][]=$infoType;
        $arr=$_SESSION['arr'];

    }

/*else{
        echo "Please fill the whole form.";
    }

*/

.....

$conn=@mysql_connect("localhost","root","");

```

```

//DataBase name selection
mysql_select_db("databreach_1");

//Insert to table : estimation_2
    $ins=mysql_query("INSERT INTO `estimation_2`
        (companySize,infoType,    sectorOfOperation,    storageModel,
numOfRecords)
VALUES ('$arr[0]', '$arr[1]', '$arr[2]', '$arr[3]', '$arr[4]','$conn)

        or

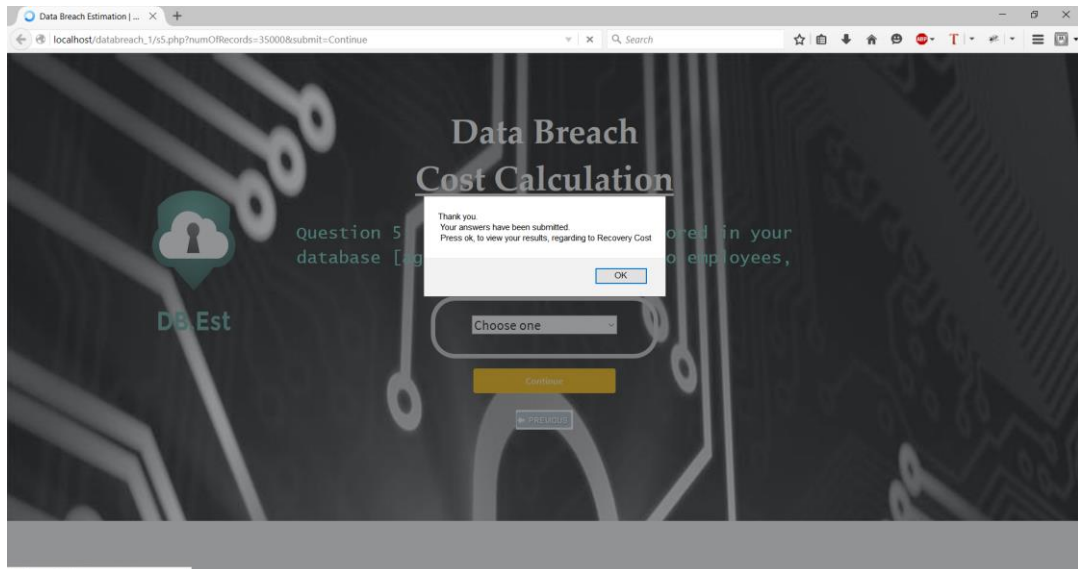
        die(mysql_error());

//message after succesfull submit
echo '<script type="text/javascript">';
    echo 'alert("Thank you. \n Your answers have been submitted. \n Press ok, to
view your results, regarding to Recovery Cost");';

//redirect to the appropriate file
echo 'window.location.href = "costSum.php"';
echo '</script>';

```

8) s5.php



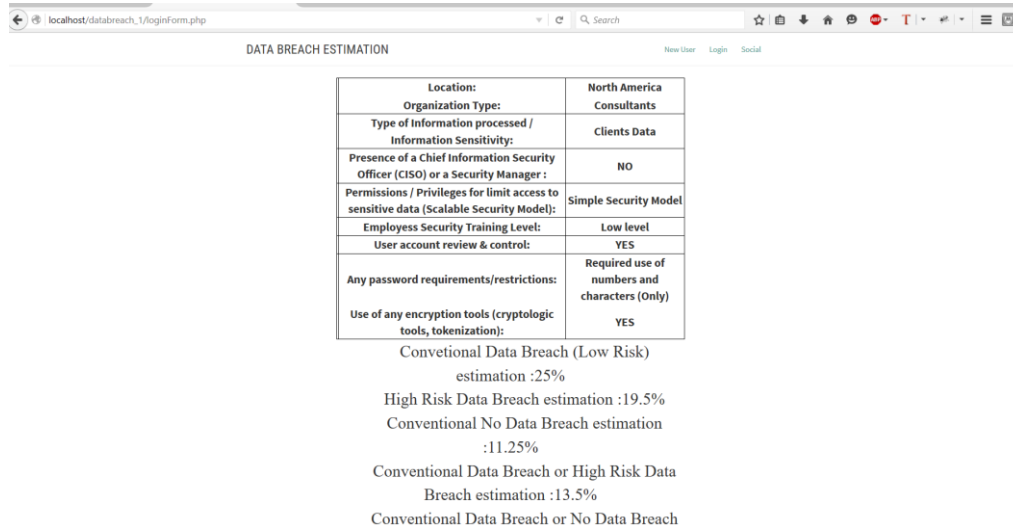
9) costSum.php

The screenshot shows a web browser window with the URL `localhost/databreach_1/costSum.php`. The page title is "Recovery Cost" and the subtitle is "Estimated Total Recovery Cost - Based on your selections". Below the title, there is a table with two columns: "Question" and "Selection". The table contains four rows of data: "Company Type: Large Enterprise", "Organization Type: Medical Records", "Sector of operation: Financial", and "Data storage and processing model: In-house Storage". Below the table, the text "Estimated Total Recovery Cost :77353€" is displayed.

Question	Selection
Company Type:	Large Enterprise
Organization Type:	Medical Records
Sector of operation:	Financial
Data storage and processing model:	In-house Storage

Estimated Total Recovery Cost :77353€

10) loginForm.php (search)



DATA BREACH ESTIMATION

Location:	North America
Organization Type:	Consultants
Type of Information processed / Information Sensitivity:	Clients Data
Presence of a Chief Information Security Officer (CISO) or a Security Manager :	NO
Permissions / Privileges for limit access to sensitive data (Scalable Security Model):	Simple Security Model
Employess Security Training Level:	Low level
User account review & control:	YES
Any password requirements/restrictions:	Required use of numbers and characters (Only)
Use of any encryption tools (cryptologic tools, tokenization):	YES

Convetional Data Breach (Low Risk) estimation :25%

High Risk Data Breach estimation :19.5%

Conventional No Data Breach estimation :11.25%

Conventional Data Breach or High Risk Data Breach estimation :13.5%

Conventional Data Breach or No Data Breach