



Module 2 (DP-JV-2): IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Aims & Objectives

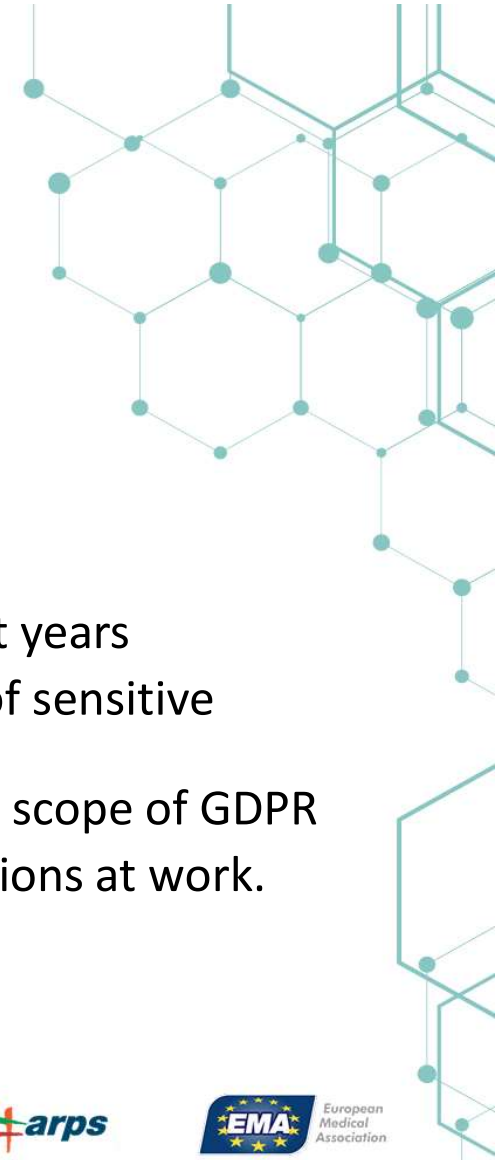


EU Institutions ensure that they have prevention mechanisms for personal breaches. Within this context DPOs will:

- explore the guidelines on personal data breach notification for the EU Institutions and Bodies
- be informed about the measures in case of emergency situation
- be able to understand the risks deriving from technology and
- Be able to understand the basic information regarding current solutions, technologies and controls (technical and organizational).



Learning Outcomes



- 2.1.a. DPOs will be able to recognize emergency cases
- 2.1.b. DPOs will know the basic IT / Information Security terminology
- 2.1.c. DPOs will know the basic definitions regarding Information and Data
- 2.1.d. DPOs will know the basic principles regarding Risk Management
- 2.1.e. DPOs will know the Top Threats to information and systems of the last years
- 2.2.a. DPOs will be able to explain the regulations concerning the handling of sensitive information in work.
- 2.2.b. DPOs will be able to identify the organization's information within the scope of GDPR
- 2.3.a. DPOs will be able to test and configure solutions for emergency situations at work.
- 2.3.a. DPOs will be able to estimate the impact of a data breach
- 2.3.b. DPOs will be able to fill in the Data Breach Notification Form



Terms and Keywords



This training module covers terms and keywords related to the following topics:

Information

Information Security

Risk Assessment

Data Breaches

Antivirus

Firewall

SIEM

Backup

Password Management

Encryption

Anonymization

Pseudonimization

Vulnerability Management

Vulnerability Assessment

Penetration Testing



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Table of contents



Lesson 1 Introduction to Information

Unit 1.1: What is Information

Unit 1.2: Information Data Flows

Lesson 2 Information Security Basics

Unit 2.1: What is Information Security

Unit 2.2: Information Security Management System

Unit 2.3: International Best Practices

Unit 2.4: Known threats and Threat Agents

Unit 2.5: Trends, statistics and examples

Lesson 3 Risk Management

Unit 3.1: Definitions

Unit 3.2: The Risk Management Process

Lesson 4 IT Security Tools & Controls

Unit 4.1: IT Security Tools

Unit 4.2: IT Security Controls

Lesson 5 Data Breaches

Unit 5.1: Introduction

Unit 5.2: Definitions

Unit 5.3: Types of personal data breaches

Unit 5.4: Assessment of impact

Unit 5.5: Notification of a Data Breach

Lesson 6 Other tools for the DPO

Unit 6.1: Official websites of the EDPB and the relevant authorities

Unit 6.2: Reports on current Threat Landscape

Unit 6.3: Reports on Imposed Fines

Unit 6.4: Tools to check if information has been leaked



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Lesson 1

Name: Introduction to Information



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Synopsis



This lesson provides

- an introduction to the basic definitions and differentiations between the terms: Information, Personal Data and Data concerning Health and
- The concept of Data Flows. More specifically, it presents what Data Flows are, what are the requirements regarding the records of processing facilities and which are the basic methods for mapping the data flows.



Lesson 2

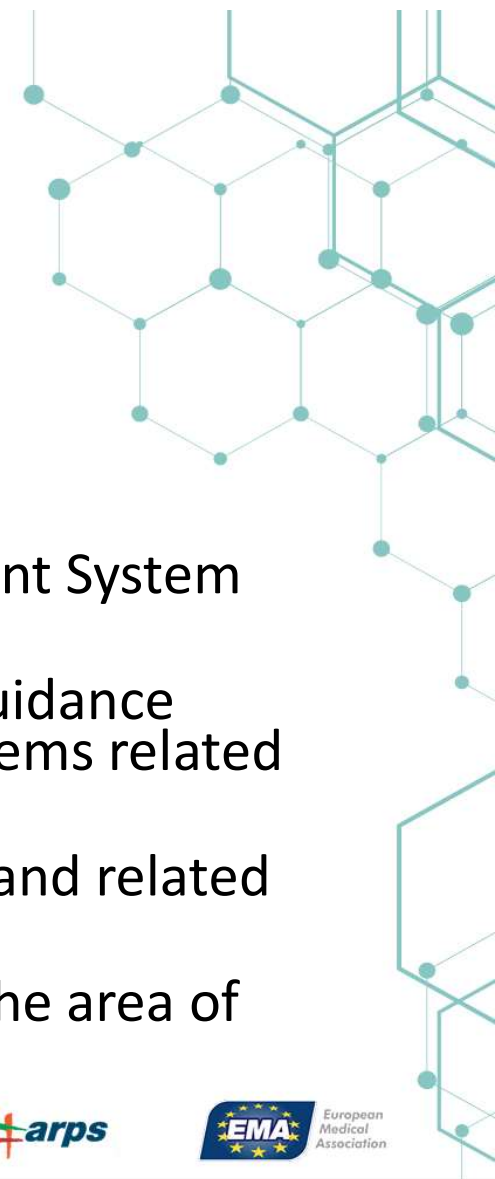
Name: Information Security Basics



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Synopsis



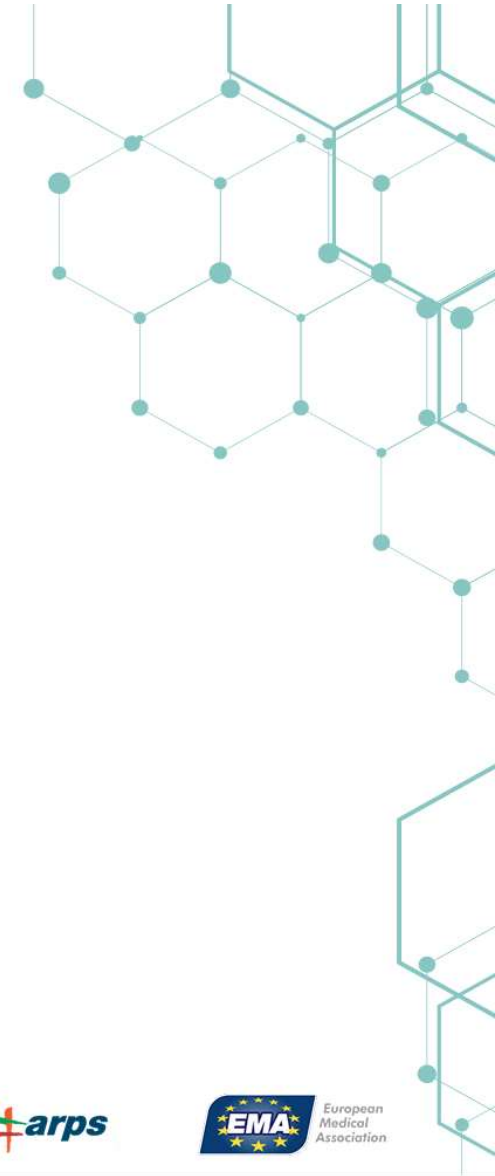
This lesson provides

- An introduction to the term Information Security and its basic characteristics
- Information on the idea of an Information Security Management System (ISMS) and why it is beneficial for an organization
- A list and a short description on various standards providing guidance regarding Information Security Management Systems and Systems related to Privacy
- A list of threat and threat agents, a short description per type and related examples where applicable
- Trends, statistics and examples in general and in particular in the area of Health.



Lesson 3

Name: Risk Management



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Synopsis



This lesson provides

- an introduction to the basic definitions related to the Risk Management Process
- An analysis of the various steps of the Risk Management process in theory as well through a practical example.



Lesson 4

Name: IT Security Tools & Controls



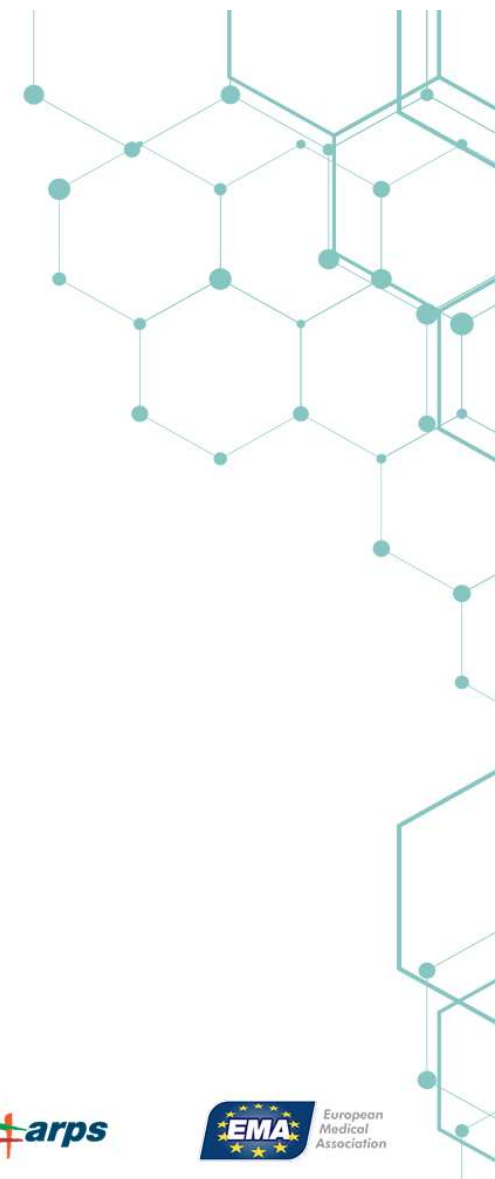
The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Synopsis

This lesson provides

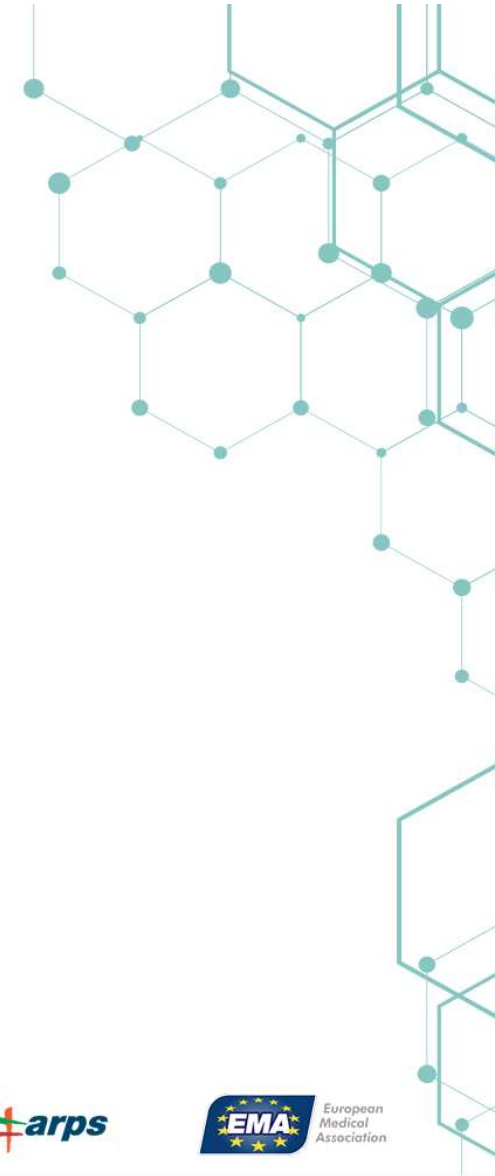
- a description of the most common IT Security Tools and
- a description of the most common IT Security Controls.





Lesson 5

Name: Data Breaches



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

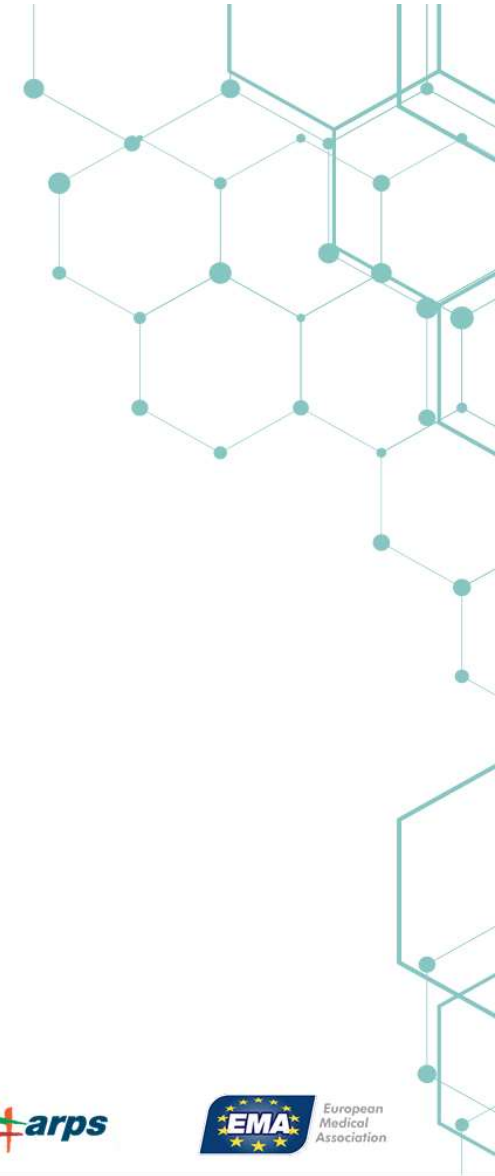


Synopsis



This lesson provides

- an introduction to the requirements regarding Data Breaches
- Description and analysis for the definitions related to Data Breaches
- An introduction to the various types of personal data breaches
- A methodology for the assessment of impact of a Data Breach and
- A template and required information regarding the notification of a Data Breach



Lesson 6

Name: Other tools for the DPO



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Synopsis

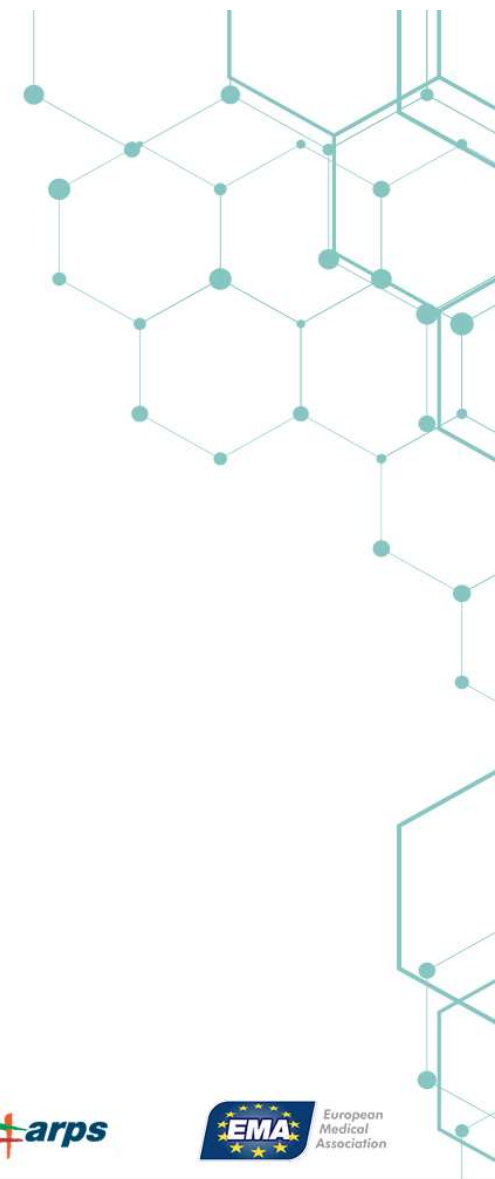


This lesson provides

- A list of official websites of authorities and other institutions that could provide assistance and guidance to the DPO
- Reports on current Threat Landscape
- Reports on Imposed Fines
- Tools to check if information has been leaked



Bibliography



(Autoriteit Persoonsgegevens (AP), 2020)

(THE EUROPEAN PARLIAMENT AND THE COUNCIL, 2016)

(Information Commissioner's Office (UK), 2019)

(Australian Red Cross Lifeblood, 2016)

(Fisher, 2013)

(Krebson Security, 2016)

(ISO, 2013)

(ISO, 2018)

(ISO, 2013)

(ISO, 2016)

(ISO, 2019)

(BSI, 2017)

(EuroPriSe GmbH - European Privacy Seal, 2020)

(EuroPriSe GmbH, 2017)

(NIST, 2013)

(ENISA, 2009)

(Government Accountability Office (GAO), 2005)

(NIST, 2020)

(Synopsis, Inc., 2019)

(Lennon, 2014)

(NIST, 2020)

(ENISA, 2016)

(PANDA Security, 2016)

(SecureWorks Inc., 2020)

(The AV Institute, 2020)

(NIST, 2020)

(Hackmageddon, 2020)

(Insurion, 2020)

(Parker, 2019)

(ARMIS, 2020)

(NIST, 2016)

(AV Institute, 2020)

(AV Institute, 2020)

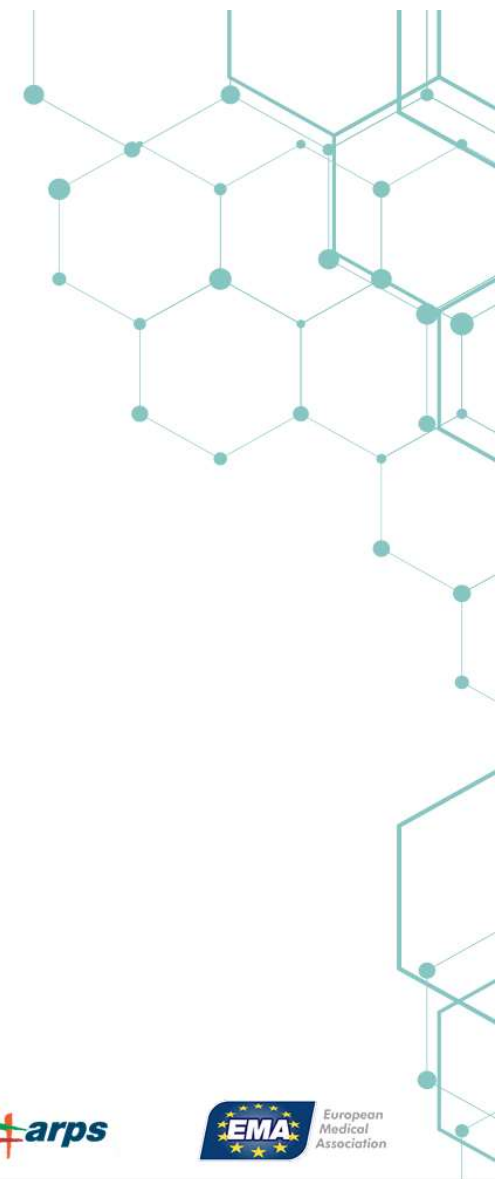
(Australian Cybersecurity Center, 2020)



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Bibliography



(Faiwarning, 2019)

(Verizon, 2019)

(ISO, 2009)

(ISO, 2018)

(AV-Comparatives, 2019)

(Gartner, 2019)

(Quinstreet Inc, 2020)

(Info Security Memo, 2020)

(SolarWinds Worldwide, LLC, n.d.)

(101 Computing Net, 2018)

(Office of the Government Chief Information Officer, 2020)

(OWASP, 2020)

(NIST, 2020)

(ENISA, 2017)

(European Data Protection Board, 2018)

(ENISA, 2013)

(European Data protection Supervisor, 2018)

(Information Commissioner's Office (ICO), 2020)

(Information Commissioner's office - Ireland, 2019)

(European Data Protection Board, 2020)

(ENISA, 2020)

(Symantec, 2020)

(PWC, 2018)

(Oracle, 2019)

(KPMG, 2020)

(European Data Protection Board, 2020)

(CMS, 2020)

(Hunt, 2020)



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Tutor's bio page

Mrs. Chrysa Psyllaki

- Organization: Skybridge
- Job placement: Researcher
- Specialty: European issues and projects

- ChrysoulaPsyllaki holds a BA in International and European Studies from the Department of International and European Studies, University of Piraeus, and currently is completing a master's in International and European Policies on Education, Training and Research Department of International and European Studies, University of Piraeus. As a student she has participated in many research groups, she has drafted newsletters and has presented papers in scientific conferences of the University of Piraeus. She performed an internship in the European Parliament Office in Greece. Moreover, she has been working as an administrative officer in the Laboratory of Education, Policy, Research, Development and Interuniversity Cooperation. She is involved in EU-funded projects



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



Thank you for your attention!



Credits

- Author/Authors: Chrysoula Psyllaki
Researcher, Skybridge
- Technical and scientific reviewers:



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 1, unit 2-4

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Introduction to Information

What is Information?

Definitions

Before the analysis of the specifics regarding Information security in the context of the GDPR within an organization in the Health Area, it is crucial that some basic terms are clarified and agreed upon.

The first Term is Information. The following description is derived from ISO 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

“Information is an asset that, like other important business assets, is essential to an organization’s business and, consequently, needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information can be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which it is transmitted, it always needs appropriate protection.”

The above term is very generic and encompasses all types and categories of information. Some examples of information may be:



The Medical Record
of a patient



The maintenance log of
the generator



The employee
master file



The software managing
the patient information



The temperature log
of the storage area



The work contracts of
the administrative staff



The fire Escape plan for each
floor of the Hospital




As shown by the definition and the examples, a lot of things may be called information, in various forms and mediums, and a subset of them could be labeled as Personal Data based on the relevant definition from GDPR (Article 4 – Definitions).

Based on this definition:

“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

Regarding the examples of information in the context of an organization in the Health Area, the following can be classified as personal data.

The icon  has been affixed in all the cases of personal data:



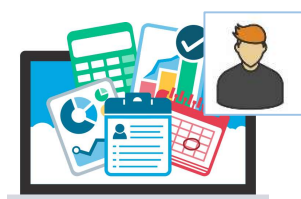
The Medical Record
of a patient



The maintenance log of
the generator



The employee
master file



The software managing
the patient information



The temperature log
of the storage area



The work contracts of
the administrative staff



The fire Escape plan for each
floor of the Hospital



All the above examples are cases, where personal information exist. From these cases, some can be further categorized as data concerning health (Definition from GDPR, Article 4)

“‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”

Or

Personal Health Information (Definition from ISO 27799:2016 – 3 Terms and Definitions).


“information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: To provision of health services to the individual and that may include:

- a) information about the registration of the individual for the provision of health services;
- b) information about payments or eligibility for health care in respect to the individual;
- c) a number, symbol, or particular assigned to an individual to uniquely identify the individual for health purposes;
- d) any information about the individual that is collected in the course of the provision of health services to the individual;
- e) information derived from the testing or examination of a body part or bodily substance;
- f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

Note 2 to entry: Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymized, the identity of the individual who is the subject of the information cannot be ascertained from the information.”

And regarding the examples of information in the context of an organization in the Health Area, the following can be classified as data concerning health.

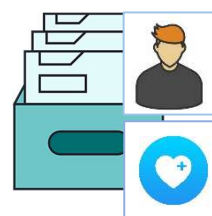
The icon  has been affixed in all the cases of data concerning health:



The Medical Record
of a patient



The maintenance log of
the generator



The employee
master file



The software managing the patient information



The temperature log of the storage area



The work contracts of the administrative staff



The fire Escape plan for each floor of the Hospital

The following image, summarizes the above regarding information, personal data and personal data concerning health:



It should be noted that, in every case organization there will be multiple categories of information and multiple instances of personal data. Especially in organizations in the Health area, there will be



information in all of the above categories (Non personal information, Simple Personal Data, Personal Data Concerning Health and others).

Value of Data concerning Health

The data concerning health is very valuable.

The value of the data is multifold.

It is critical for the operation of the healthcare organization and if the information is corrupted or lost, the organization cannot operate effectively.

Moreover, if the information in question is lost then the fines imposed are considerable.

This is shown also by the following example:

Haga fined for insufficient internal security of patient records

News item / July 16, 2019

Category:
Security of personal data,
Healthcare providers and the AVG,
Medical file

The Haga Hospital does not have the internal security of patient records in order. This is the conclusion of a study by the Dutch Data Protection Authority (AP). This investigation followed when it appeared that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person. The AP imposed a fine of 460,000 euros on Haga Hospital for insufficient security.

(Source: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers>)

On the other side, this type of information is valuable to the malicious actors. The following image depicts the reasons why this is so, based on the Research: Why healthcare information is valuable. - KPMG infographic. (PRNewsFoto/KPMG LLP)

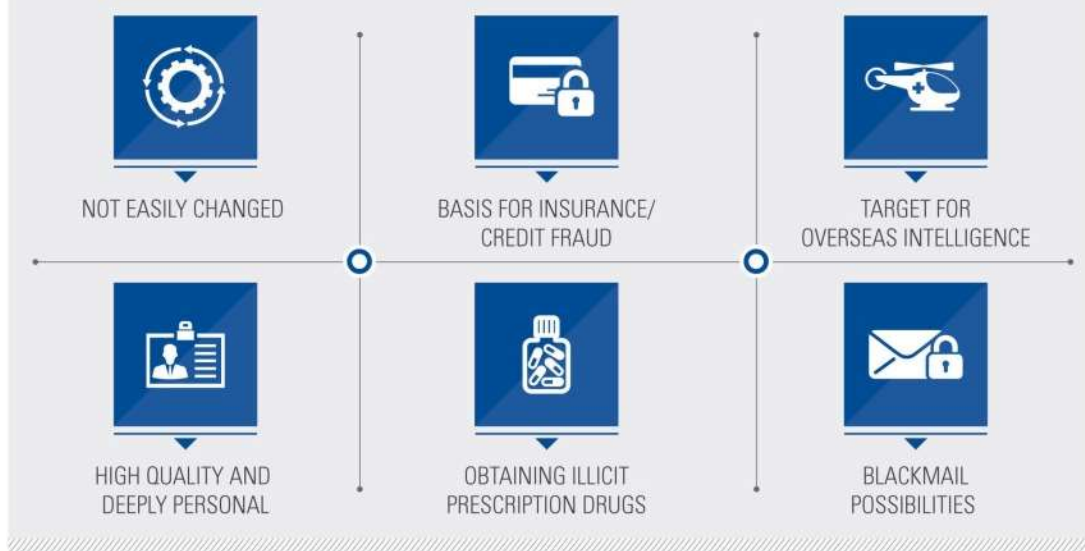
HEALTHCARE INFORMATION IS **10** TIMES MORE VALUABLE



ON THE **BLACK MARKET**
THAN **SOCIAL SECURITY**
& **CREDIT CARD** INFORMATION.



WHY ?





Information Data Flows

The first step that an organization must undertake in every GDPR compliance project, as demonstrated in the previous paragraph, is to identify the information processed within its operation and map it to the relevant category.

Only then, can the organization, for the information categorized as personal data based on the above definitions, proceed with the rest of the steps regarding GDPR compliance.

This identification step is the first one of a process called “Mapping Data Flows” and is used as a basis for the following:

- Definition of the applicability scope for GDPR
- Identification of the categories of personal data processed by the organization
- Conducting the Data Protection Impact Assessments where needed
- Conducting Risk Assessment
- Identification of the interested parties
- Maintaining the Records of processing activities
- Identifying the impact of a data breach
- Implementing protection measures
- and others.

What is an (Information) Data Flow?

An information Data Flow depicts the lifecycle of each instance of personal data. It shows the Personal Data being processed, the type of processing, the purpose of processing, the Personal Data recipients (internal and external), the measures implemented, the relevant constraints etc.

By mapping all this information per each instance of personal data, the organization becomes aware of the quantity and quality of the processed personal data and has an overview of the entire process.

Records of processing activities

GDPR in article 30, Records of processing activities, mandates the creation and maintenance of records of processing activities for specific cases (enterprises or organisations employing more than 250 persons or “when the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1)*)”

* GDPR - Article 9. Processing of special categories of personal data. (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.”

An organization operating in the Health area, most likely falls under the categories described above, and thus needs to keep these records of processing activities as mandated by GDPR and the applicable supervisory authority.



The minimum information requested for the records of processing authorities by the GDPR is (Source: GDPR - Article 30, Records of Processing Activities):

“1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).”

Some supervisory authorities, e.g. the Greek Data Protection Agency,

https://www.dpa.gr/portal/page?_pageid=33,211400&_dad=portal&_schema=PORTAL, the

Information Commissioner's office (UK), [https://ico.org.uk/media/for-](https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx)

organisations/documents/2172937/gdpr-documentation-controller-template.xlsx and others, have



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



published document templates for the recording of processing activities. These templates usually request information superseding the minimum mentioned in the GDPR.

Methods for mapping data flows

Possible methods for the mapping of the data flows are the following (Source: Information Commissioner's Office (UK), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how5>)

- Questionnaires – these can be distributed within these areas of the organisation processing of personal data may be processed. The purpose of these questionnaires it to retrieve information from the people that are directly involved with the processing of personal data.
- Direct meetings with key business functions. These interviews – meeting facilitate the collection of comparable and reliable information since the facilitator is there to ensure uniformity.
- Review of policies, procedures, contracts and agreements. This will help in the verification between intended and actual data processing activities.

There is also, a variety of tools that advertise that can be used during the data mapping process. These tools can be divided I the following two categories:

- a) Automatic discovery tools – These are tools that could be installed in a computer network and could search within the information contained within for specific formats of data (e.g. Credit Card Numbers, National Identification Numbers etc). These tools exhibit the following constraints:
 - a. They can only identify data that fit to a specific predetermined format
 - b. They can only identify digital information that is readable (e.g. they cannot identify information in pictures or products of scanned physical files). This also means that any information not in digital format (e.g. paper documents) will not be identified.
- b) Tools for recording the processing activities – These are tools that have a structure able to document the information required by the GDPR in Article 30, as shown above.

The organization should have all this information in mind before selecting the preferred method. Practice has shown, that a combination of the above mentioned methods is deemed as most effective. Since this way, the organization can collect reliable, comparable and actual information relating the processing of personal data from the people involved in the actual processing while at the same time reducing the effort and resources invested in the process.

The results of the data mapping process are documented in the relevant file and it is maintained in perpetuity. This record may be requested by the Supervisory authority.

Lesson 1 Introduction to Information

Unit 1: What is Information

Question 1.:

Which of the following is Information?

(Select all that apply)



Question 2.:

Where would you expect to find personal information in this scene?

(Select all possible spots that may have personal information)

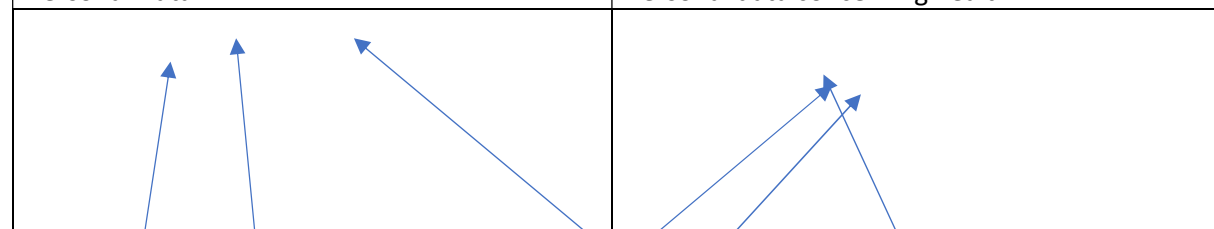
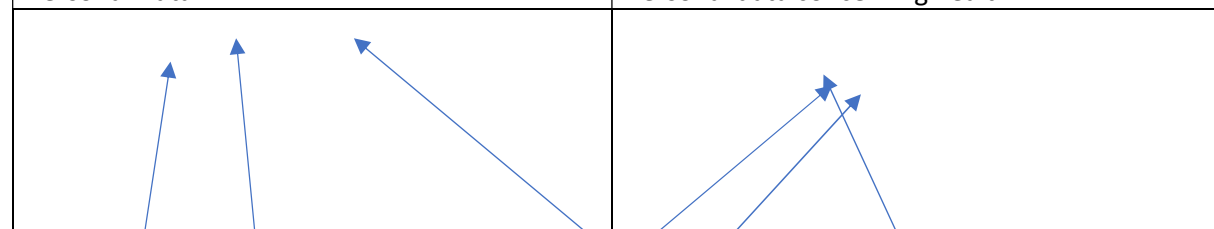


Correct answer



Question 3.:

Which of the following are personal data and which are personal data concerning health?

Personal Data	Personal data concerning health
	

Bank transactions with employees

Medical Records of patients

Insurance claims for

patients

The shift schedule

Medical opinions

The hourly rates of contractor and

permanent staff



Unit 2: Information Data Flows

Question 4.:

What are Personal Data Flows?

1. The flows depict the personal data processed by the organization throughout their entire life cycle within the organization
2. The flows show the amount of work the data protection officer has to do
3. The flows depict the requirements set by GDPR
4. The flows show who is responsible for every piece of information within the organization.

Question 5.:

Why is performing Personal Data Flows mapping important for an organization?

1. By mapping all this information per each instance of personal data, the organization becomes aware of the quantity and quality of the processed personal data and has an overview of the entire process. What is known can be managed also.
2. The file with the data flows is needed in order to conduct Risk Assessment
3. The file of the data flows will tell the DPO what he/she needs to do
4. The file of the data flows is mandatory and must be provided to all data subjects.

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 2, unit 1-6

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Information Security Basics

What is Information Security

The following definition is derived from ISO 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

“Information security: Information security ensures the confidentiality, availability and integrity of information. Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.

Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific information security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization’s business processes.”

Since as shown by the above definition, information security is the protection of the confidentiality, availability and integrity of information, it is also important that these definitions are provided.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

For example, the database of Blood Donor Information, should only be accessible by specific authorized individuals, entities, or processes (internally or externally). A failure regarding this feature would lead to the processing of the related personal information (some of them data concerning health) by unauthorized entities with a possible negative impact to the freedom of the data subjects.

BLOOD SERVICE APOLOGISES FOR DONOR DATA LEAK

FRIDAY 28TH OCT 2016

The Australian Red Cross Blood Service is apologising to donors for an error which allowed a back-up copy of an online enquiry database to be accessed by an unauthorised person.

Blood Service Chief Executive Shelly Park said today that on 26 October the Blood Service became aware that a file containing donor information was placed in an insecure environment by a third party that develops and maintains the Blood Service’s website.

This file contained registration information of 550,000 donors made between 2010 and 2016. The file was part of an online application to give blood and information such as names, addresses, dates of birth and some personal details are included in the questionnaire.

(Source: <https://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak>).

Integrity: property of accuracy and completeness.

For example, in case of patient records, the information contained within the records should be accurate and compete. Or in the case of the Associated Press, contents of the tweets send out from its official twitter account were altered leading to a loss of \$136 billion in equity market value.



This chart shows the Dow Jones Industrial Average during Tuesday afternoon's drop, caused by a fake A.P. tweet, inset at left.

By **Max Fisher**

April 23, 2013 at 11:31 p.m. GMT+3

At 1:07 p.m. on Tuesday, when the official Twitter account of the Associated Press sent a [tweet](#) to its nearly 2 million followers that warned, "Breaking: Two Explosions in the White House and Barack Obama is injured," some of the people who momentarily panicked were apparently on or near the trading floor of the New York Stock Exchange.

At 1:08, the Dow began a [perilous but short-lived nosedive](#). It dropped about 150 points, from 14697.15 to 14548.58, before stabilizing at 1:10 p.m., when news that the tweet had been erroneous began to spread. By 1:13 p.m., the level had returned to 14690. During those three minutes, the "fake tweet erased \$136 billion in equity market value," [according to Bloomberg News' Nikolaj Gammeltoft](#).

(Source: <https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/>)

Availability: property of being accessible and usable on demand by an authorized entity.

For example, in the case of a Hospital, the information of a patient needs to be available to the patient's doctor when he needs it in order to form his diagnosis regarding the patient.

In a “major incident” alert posted to its Web site, the National Health Service’s Lincolnshire and Goole trust said it made the decision to cancel surgeries and divert trauma patients after a virus infected its electronic systems on Sunday, October 30.

! MAJOR INCIDENT - UPDATE

MAJOR INCIDENT – APPOINTMENTS CANCELLED

A virus infected our electronic systems on Sunday October 30 and we have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it.

All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday November 2 with a small number of exceptions as follows:

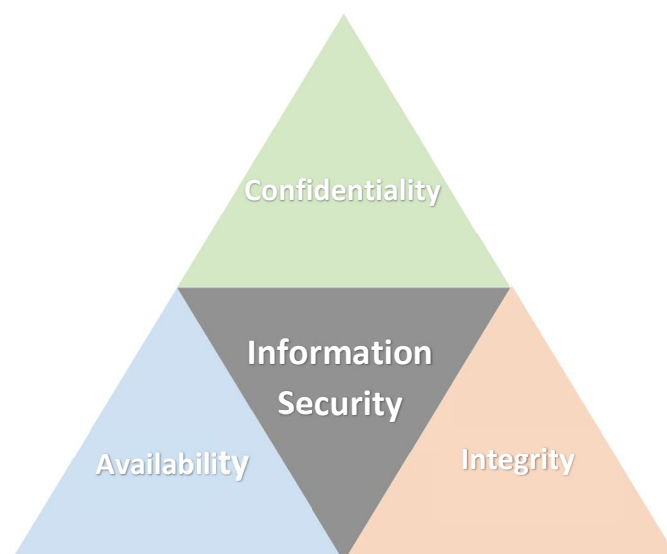
- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics

A portion of the alert posted to the NHS's home page.

“We have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it,” the NHS said, of the unspecified malware infection. “All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday, Nov. 2 with a small number of exceptions.”

(Source: <https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/>)

These three characteristics are often referred to as the CIA triad. In order to achieve information security all three characteristics have to be achieved, to the degree that is compatible with the needs and expectations of the organization.





Information Security Management System

The best practice in order to achieve and maintain a uniform and predefined level of information security within an organization is to implement an Information Security Management System.

The following description is derived from ISO 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

“A management system uses a framework of resources to achieve an organization’s objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

- a) satisfy the information security requirements of customers and other stakeholders;
- b) improve an organization’s plans and activities;
- c) meet the organization’s information security objectives;
- d) comply with regulations, legislation and industry mandates; and
- e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

Why an ISMS is important

The following contains an overview of the need and the benefits from the implementation of an ISMS as described in ISO 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

“Risks associated with an organization’s information assets need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization.

The adoption of an ISMS is expected to be a strategic decision for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization. The design and implementation of an organization’s ISMS is influenced by the needs and objectives of the organization, the security requirements, the business processes employed and the size and structure of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirements of all of the organization’s stakeholders including customers, suppliers, business partners, shareholders and other relevant third parties.

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code,



computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards, the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and can be ineffective without being supported by appropriate management and procedures within the context of an ISMS.

Integrating security into a functionally complete information system can be difficult and costly. An ISMS involves identifying which controls are in place and requires careful planning and attention to detail. As an example, access controls, which can be technical (logical), physical, administrative (managerial) or a combination, provide a means to ensure that access to information assets is authorized and restricted based on the business and information security requirements.

The successful adoption of an ISMS is important to protect information assets allowing an organization to:

- a) achieve greater assurance that its information assets are adequately protected against threats on a continual basis;
- b) maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness;
- c) continually improve its control environment; and
- d) effectively achieve legal and regulatory compliance.”

As mentioned above, at the core of ISMS design and implementation, resides the Risk Management Process. The Risk Management process will allow the organization to assess the risks regarding Information Security and plan for the treatment of the ones evaluated as unacceptable. These plans (Risk Treatment Plans) will contain the organizational or technical Information Security Controls selected by the organization. (More details on risk management will be provided in the further in this document.)



International Best Practices

ISMS Standards

There are various publications containing internationally recognized best practices regarding the design, implementation, maintenance and improvement of an Information Security Management System. Some of these publications are the following:

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

(Source: <https://www.iso.org/standard/54534.html>)

ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. The control objectives and controls from ISO/IEC 27001:2013, Annex A shall be selected as part of this ISMS process as appropriate to cover the identified requirements. (Source: ISO 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary).

The controls populating Annex A, cover the following categories:

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security – (6 controls)
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)



A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance (8 controls)

ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls.

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It is designed to be used by organizations that intend to:

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines.

(Source: <https://www.iso.org/standard/54533.html>)

ISO 27002, provides guidance on the implementation of the controls contained in Annex A of ISO 27001 as described in the previous paragraph.

ISO 27799:2016. Health informatics — Information security management in health using ISO/IEC 27002.

ISO 27799:2016 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.

ISO 27799:2016 provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing ISO 27799:2016, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

It applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is always be appropriately protected.



ISO 27799:2016 and ISO/IEC 27002 taken together define what is required in terms of information security in healthcare, they do not define how these requirements are to be met. That is to say, to the fullest extent possible, ISO 27799:2016 is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, International Standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that ISO 27799:2016 describes.

The following areas of information security are outside the scope of ISO 27799:2016:

- a) methodologies and statistical tests for effective anonymization of personal health information;
- b) methodologies for pseudonymization of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic);
- c) network quality of service and methods for measuring availability of networks used for health informatics;
- d) data quality (as distinct from data integrity).

(Source: <https://www.iso.org/standard/62777.html>)

Standards related to Privacy

The standards related to Information Security Management Systems are further enriched / completed by the ones that have already been issued regarding the Management of Private Information. Some of these standards are:

[ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines](#)

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

(Source: <https://www.iso.org/standard/71670.html>)



BS 10012:2017+A1:2018. Data protection. Specification for a personal information management system

It shows organizations how to implement a Personal Information Management System (PIMS). This will help them reach a good standard of information governance and comply with legal personal data protection requirements.

This standard can be used by any and all organizations holding the personal information of clients and/or staff and wishing to maintain compliance with current regulation and good practice.

As part of an overall information management system, this standard enables organizations to put a Personal Information Management System (PIMS) in place which provides a framework for maintaining and improving compliance with data protection requirements and good practice.

The standard was updated in 2017 to reflect new requirements in the EU's General Data Protection Regulation (GDPR) which came into force on 25 May 2018.

Use of the standard will help organizations avoid compliance breaches, significant fines and reputational damage, as well as reduce the actual cost of recovery following a privacy breach.

(Source:

https://shop.bsigroup.com/ProductDetail/?pid=000000000030378574&_ga=2.156438649.355995019.1578508533-1597060063.1577625444)

EuroPriSe Criteria for the certification of IT products and IT-based services - (v201701)

Material Scope

The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States.

Territorial Scope

Manufacturers and vendors of IT products and providers of IT-based services can apply for a seal even if they are not subject to EU data protection law, but want to prove the compliance of their processing operations with EU law nevertheless. This may cover, but is not limited to the subject matter of Article 46(2)(f) GDPR.

(Source: <https://www.european-privacy-seal.eu/EPS-en/Vision> and EuroPriSe Criteria for the certification of IT products and IT-based services - (v201701))

NIST Special Publication 800-53, Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations.

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters,



structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

(Source: NIST Special Publication 800-53, Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations.)



Known threats and Threat agents

This section will provide an overview regarding common threats, threat agents and attack vectors that could influence the security of information.

To facilitate the further understanding of these topics, the following definitions need to be clarified:

Threats:

A threat is a potential cause of an incident, which may result in harm of systems and organization.

(Definition from ISO/IEC 27005:2018 Information Technology — Security Techniques — Information Security Risk Management)

For the same term, ENISA (Source: "Glossary – ENISA". Enisa.europa.eu. 24 July 2009) also provides the following definition:

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

A threat has the potential to harm amongst others information, processes and systems and therefore organizations. Threats may be of natural or human origin, and could be accidental or deliberate. A threat may arise from within or from outside the organization.

As shown above, there is a vast number of threats. Threats may be deliberate, accidental or environmental (natural) and may result, for example, in damage or loss of essential services, information and others. Threats may be divided into types e.g. Physical damage, Natural events, loss of essential services and others. This grouping of threats can help organizations during Risk Identification (completeness check).

Possible examples of threats are the following:



Fire



Earthquake



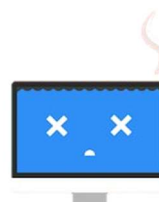
Flood



Theft of media or documents



Software Failure



Hardware Failure



Remote
Spying



Data
Leakage



Loss of
Power Supply

Based on the latest ENISA Threat Landscape Report (2018), the Top Cyber Threats and Trends are the following:

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➡	1. Malware	➡	➡
2. Web Based Attacks	⬆	2. Web Based Attacks	⬆	➡
3. Web Application Attacks	⬆	3. Web Application Attacks	➡	➡
4. Phishing	⬆	4. Phishing	⬆	➡
5. Spam	⬆	5. Denial of Service	⬆	⬆
6. Denial of Service	⬆	6. Spam	➡	⬇
7. Ransomware	⬆	7. Botnets	⬆	⬆
8. Botnets	⬆	8. Data Breaches	⬆	⬆
9. Insider threat	➡	9. Insider Threat	⬇	➡
10. Physical manipulation/ damage/ theft/loss	➡	10. Physical manipulation/ damage/ theft/loss	➡	➡
11. Data Breaches	⬆	11. Information Leakage	⬆	⬆
12. Identity Theft	⬆	12. Identity Theft	⬆	➡
13. Information Leakage	⬆	13. Cryptojacking	⬆	NEW
14. Exploit Kits	⬇	14. Ransomware	⬇	⬇
15. Cyber Espionage	⬆	15. Cyber Espionage	⬇	➡
Legend: Trends: ⬇ Declining, ➡ Stable, ⬆ Increasing Ranking: ⬆ Going up, ➡ Same, ⬇ Going down				

(This table includes a comparison to the values of the 2017 Report, showing also the trend of the relevant Threats).

Threat Source / Agent



A further term related to Threats, is Threat source / Agent:

“Threat source / Agent is used to indicate the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.” (Definition from <https://csrc.nist.gov/glossary/term/Threat-Agent-Source>).

Based on the Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005), the following table contains some of the possible Threat Sources / Agents:

Threat Source	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.



Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.
Nation States*	<p>National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm a nation's interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to a nation's critical infrastructures.</p> <p>The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.</p>
Corporations*	Corporations employ the same techniques and have the same goals as the Nation States described above, with the only difference being that they target other corporations than the critical infrastructure or other information of a country.
Hacktivists*	In Internet activism, hacktivism or hactivism (a portmanteau of hack and activism) is the use of technology to promote a political agenda or a social change.
Script kiddies*	<p>In programming and hacking culture, a script kiddie, skiddie, or skid is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites, such as a web shell. It is generally assumed that most script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities.</p> <p>(Source: Wikipedia)</p>

* these entries were not originally in the Government Accountability Office (GAO) Table, but were added in order to provide a fuller picture of the actors.

In the latest ENISA Threat Landscape Report (2018), the Threat Agents related to the Top CyberThreats are the following:

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:

Primary group for threat: ✓

Secondary group for threat: ✓

Vulnerability

“Vulnerabilities are weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.” (Definition from <https://csrc.nist.gov/glossary/term/vulnerability>).

The relationship between a vulnerability and a threat can be compared to the lock and key one. In this case, threats (as described above) are ever present and existing – the lock analog. What would make a threat materialize for an organization would be the existing of a corresponding vulnerability – the key. If this combination exists then for this organization, this is an existing risk and the organization has to decide on the treatment options – the lock is open.

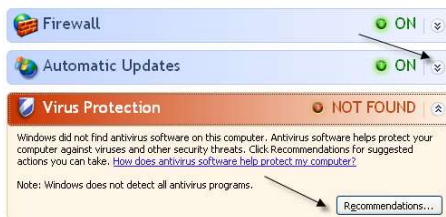
To better understand vulnerabilities the following examples are provided:



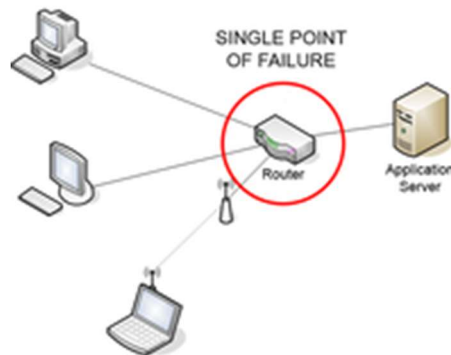
Building having weak foundations



Easy to guess passwords



Having no protection against malware



Having single point(s) of failure

Finally, the following example shows the relationship between threat and vulnerability described above:



In the beginning of April 2014, it was published that a bug exists in a piece of open source software called OpenSSL - which is designed to encrypt communications between a user's computer and a web server, a sort of secret handshake at the beginning of a secure conversation.

This software (OpenSSL), at the time of disclosure, was estimated to be installed in its vulnerable state in 17% (around half a million) of the Internet's secure web servers certified by trusted authorities.

The information security community reached very quickly by publishing patches and issuing warnings and recommendations to operators of vulnerable systems.

(Source: <http://heartbleed.com/>, wikipedia)

In spite of the tremendous publicity and the speed of various interested parties, incidents have been documented as direct results of the exploitation of the Heartbleed bug:



Hackers Exploited Heartbleed Bug to Steal 4.5 Million Patient Records: Report

By Mike Lennon on August 19, 2014



Earlier this week, Community Health Systems, one of the largest hospital operators in the United States, announced that hackers managed to **steal the records** of 4.5 million patients.

FireEye-owned Mandiant, known for investigating high-profile breaches, was hired to investigate the incident and believes the attack was the work of a Chinese advanced persistent threat (APT) group.

While no technical details of the attack had previously been disclosed, information security firm TrustedSec, citing sources familiar with the incident, said on Tuesday that the initial attack vector was through the infamous “**Heartbleed**” vulnerability in OpenSSL, which provided the attackers a way in, eventually resulting in the compromise of patient data.

“This confirmation of the initial attack vector was obtained from a trusted and anonymous source close to the CHS investigation,” TrustedSec wrote in a **blog post**. “Attackers were able to glean user credentials from memory on a CHS Juniper device via the heartbleed vulnerability (which was vulnerable at the time) and use them to login via a VPN.”

While TrustedSec did not share much on the source, the firm is reputable. As background, David Kennedy, TrustedSec's founder and Principal Consultant, formerly worked for the NSA and also served as Chief Security Officer at ATM maker Diebold. He is also founder of the **Derbycon** conference.



(Source: <https://www.securityweek.com/hackers-exploited-heartbleed-bug-steal-45-million-patient-records-report>).

In this example, the threat was Data Leakage from Hackers (Source) by exploiting the fact that the organization in question did not patch (correct) an existing vulnerability.

Attack

“An attack is an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.” (Definition from <https://csrc.nist.gov/glossary/term/attack>).



And an attack vector “is a path or means by which a threat agent can gain access to a computer or network server, abuse weaknesses or vulnerability on assets (including human) in order to achieve a specific outcome”. (Definition from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>).

It has to be understood that an attack always has a purpose, something to be gained for the attacker. Depending on what the purpose of the attack is, the attacker will design the method and implement the attack.

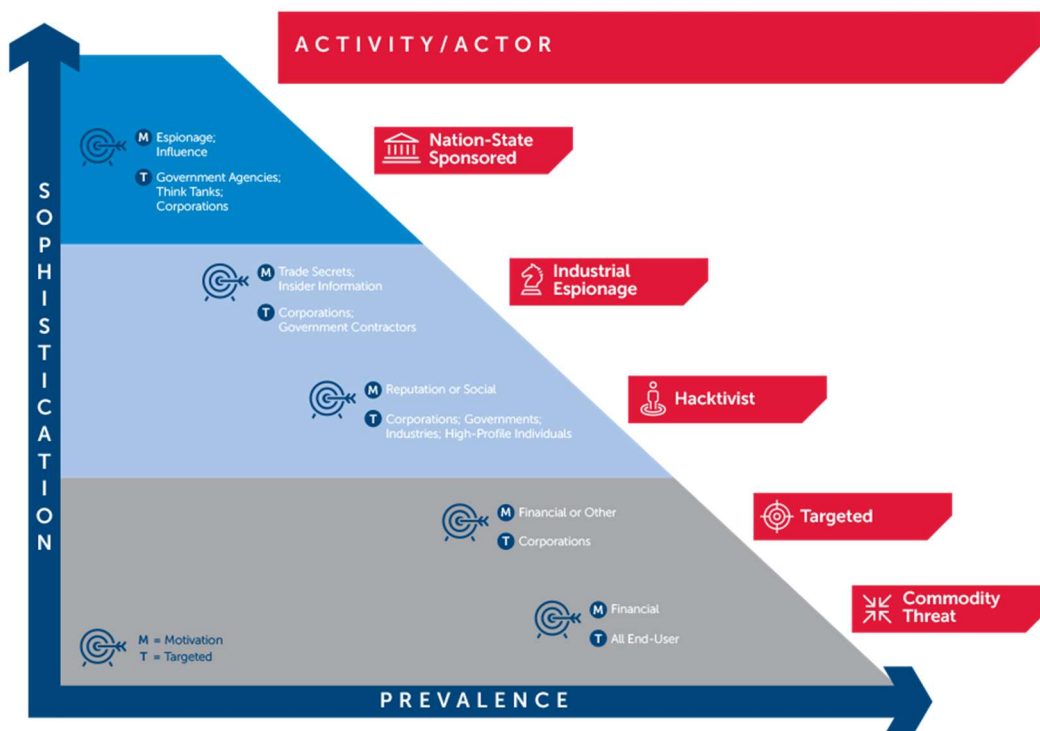
The steps that will be implemented and their sequence is called a “kill chain”.

The following image depicts an external intruder kill chain:



(Source: <https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-EN.pdf>, Panda Security).

The more valuable the target, the more sophisticated (persistent) the attack will be.





(Source: <https://www.secureworks.com/blog/advanced-persistent-threats-apt-a>)

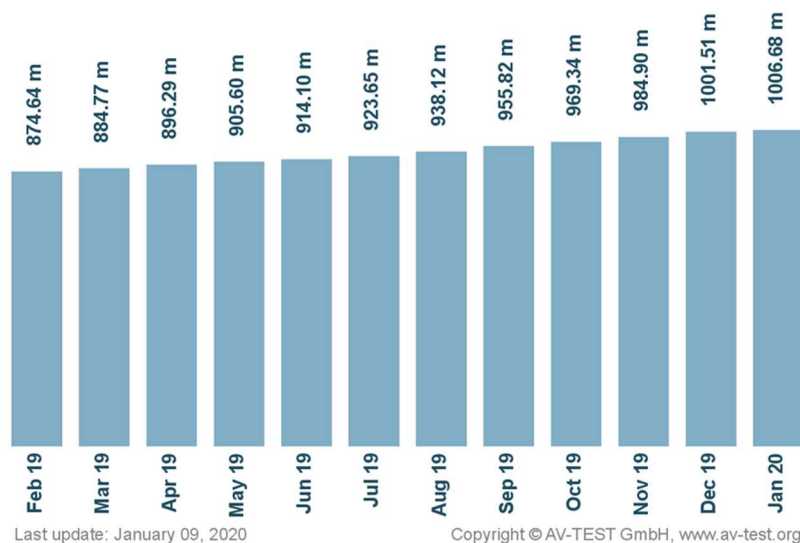
Basic Attack related terminology

Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (Definition from <https://csrc.nist.gov/glossary/term/malware>).

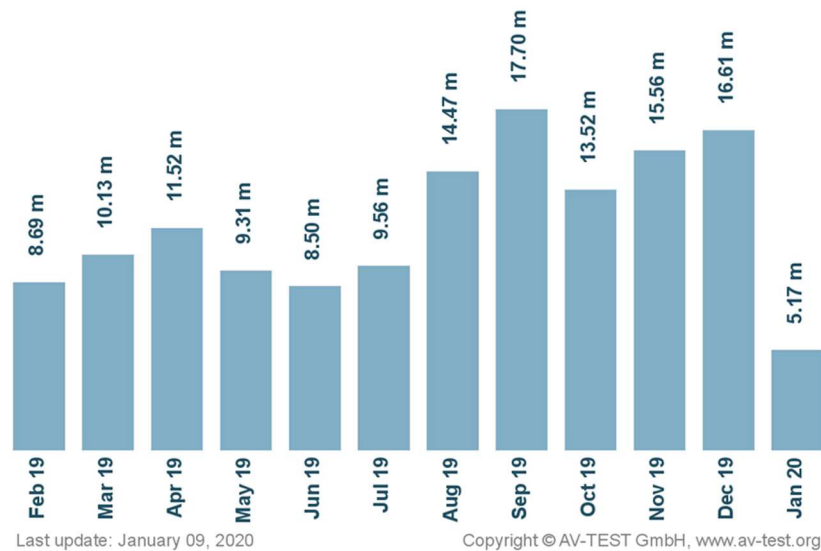
Total Malwares from AV-TEST Institute in the last year

Total malware



(Source: <https://www.av-test.org/en/statistics/malware>)

New Malwares in the last 12 months



(Source: <https://www.av-test.org/en/statistics/malware>)

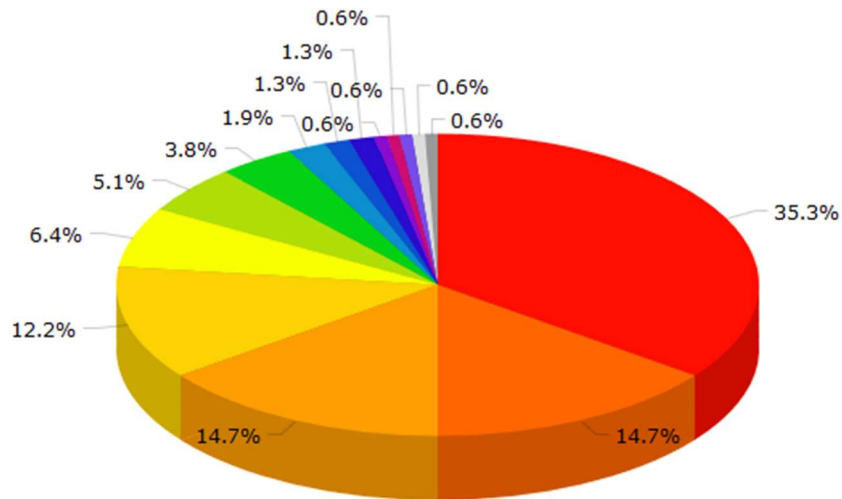
Hackers

Hacker is an unauthorized user who attempts to or gains access to an information system.

(Definition from <https://csrc.nist.gov/Glossary/Term/hacker>).

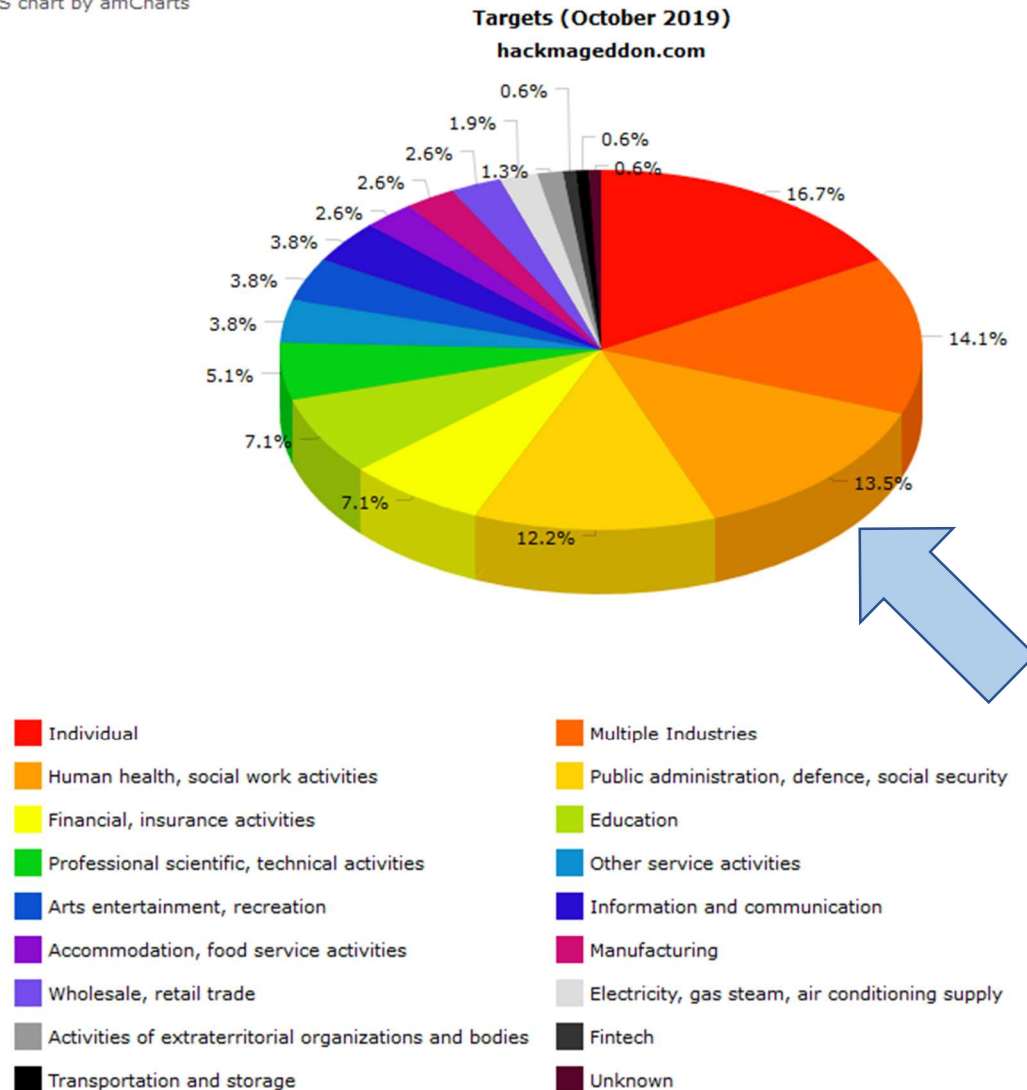
Charts of the techniques that hackers and the targets that they focused. These statistics are from <https://www.hackmageddon.com/>

Attack Techniques (October 2019) hackmageddon.com



- | | | |
|----------------------------|-------------------------------|-----------------------------|
| Malware/PoS Malware | Unknown | Targeted Attack |
| Account Hijacking | Vulnerability | DDoS |
| Malicious Script Injection | BEC | Malicious WordPress plugins |
| Malicious Spam | Fake Social Networks Accounts | Malvertising |
| SQLi | Social Networks Bot | Brute Force |

As you can see in the second chart Healthcare targets are in the third place with a percentage of 13.5%



Cyber extortion

Cyber extortion is an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment. Cyber extortion often takes the form of ransomware and distributed denial-of-service (DDoS) attacks, both of which could paralyze your business. (Source: <https://www.insureon.com/insurance-glossary/cyber-extortion>).

One example is ransomware which is a type of malware and when the attacker gain access to a device or a system, malware locks the screen or encrypts the data stored on the disk. It then presents a ransom payment requirement with detailed payment details.

Now days there are several articles that remind us and warn us that wannacry cyberattack is still here and especially for Healthcare industry. For example the article that was published by

<https://hospicenews.com/> with title 'WannaCry' Ransomware Hits 40% of Health Care Organizations.



 Pixabay

Share



More than 40% of health care organizations have experienced a cyber attack involving the “WannaCry” ransomware cryptoworm within the past six months, according to a [report](#) by the cyber security firm Armis.

Health care organizations, [including hospices](#), continue to be the preferred target of cyber criminals who can glean patient names, insurance information, financial information, addresses, social security numbers and other data that hackers can use for identity theft or other fraudulent activity.

“Health care, manufacturing and retail sectors have high rates of old operating systems in their networks,” the report indicated. “By 2020, Windows 7 will reach its end-of-life, and join many of the earlier Windows versions that do not receive any security updates. It is not a coincidence that these sectors are also the ones affected the most by ransomware like WannaCry, which rely on unpatched devices for their successful operation.”

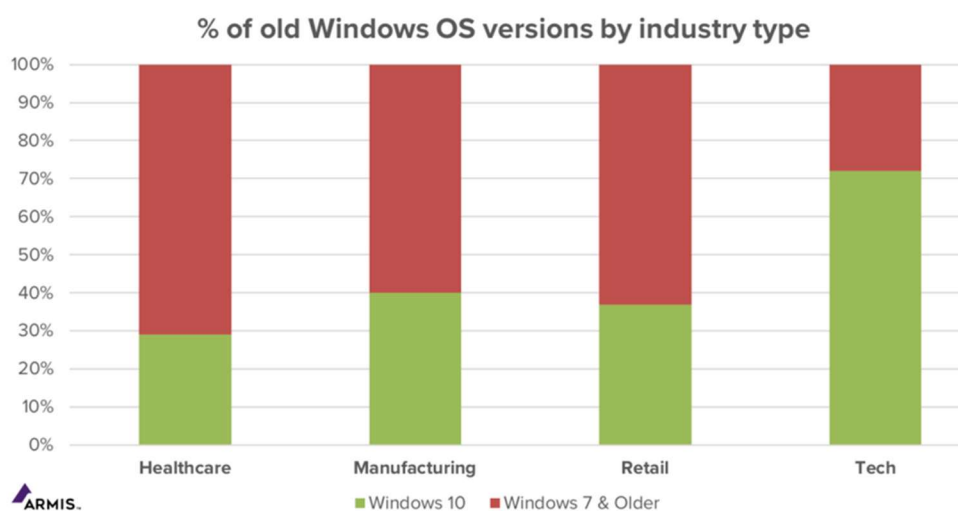
(Source: <https://hospicenews.com/2019/06/17/wannacry-ransomware-hits-40-of-health-care-organizations/>)

As the article mentions, the outdated operating systems is a major issue. <https://www.armis.com> conducted a research with the name **“Two Years In and WannaCry is Still Unmanageable”** and the results confirm all the above.

Active WannaCry Heatmap

After analyzing data from the Armis platform, our research team estimates that as many as 60% of organizations in the manufacturing industry and 40% of healthcare delivery organizations (HDOs) experienced at least one WannaCry attack in the last six months. Organizations in these industries generally have a large number of older or unmanaged devices which are difficult to patch due to operational complexities. As it had when it emerged, WannaCry clearly demonstrates the frightening potential which unpatched vulnerabilities have on such devices.

Moreover, new and similar vulnerabilities are still being found. In fact, just last week [Microsoft disclosed a new wormable vulnerability](#) like the one used by WannaCry. The prevalence of unmanaged devices running old operating systems in organizational networks is surprisingly high, as shown by the Armis data.



Percentage of old Windows OS versions by industry type (Retail, Technology, Healthcare, Manufacturing)

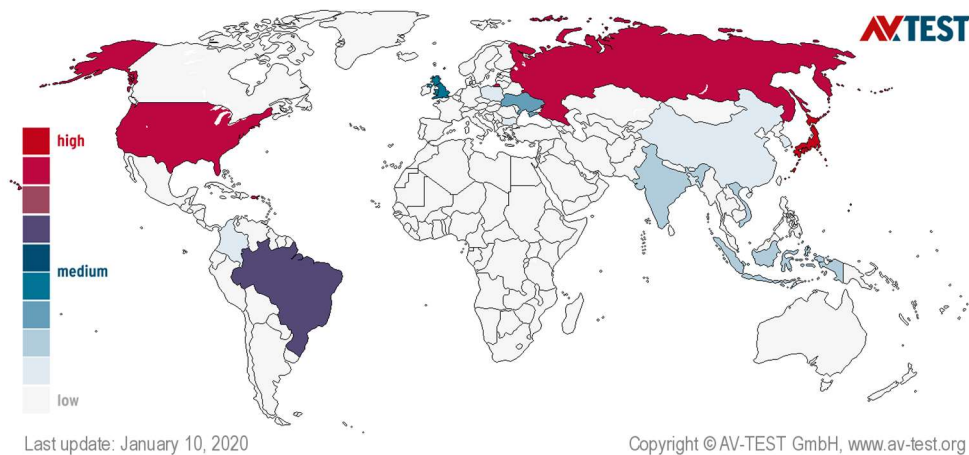
(Source: <https://www.armis.com/resources/iot-security-blog/wannacry/>)

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. Spam—unsolicited email—is often used to deliver spyware and other forms of malware to users. Spam is also frequently used for performing phishing attacks, which are deceptive computer-based means to trick individuals into disclosing sensitive personal information. (Source: NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access).

The following map from <https://www.av-test.org> shows the origin of Spam per country the last 60 days

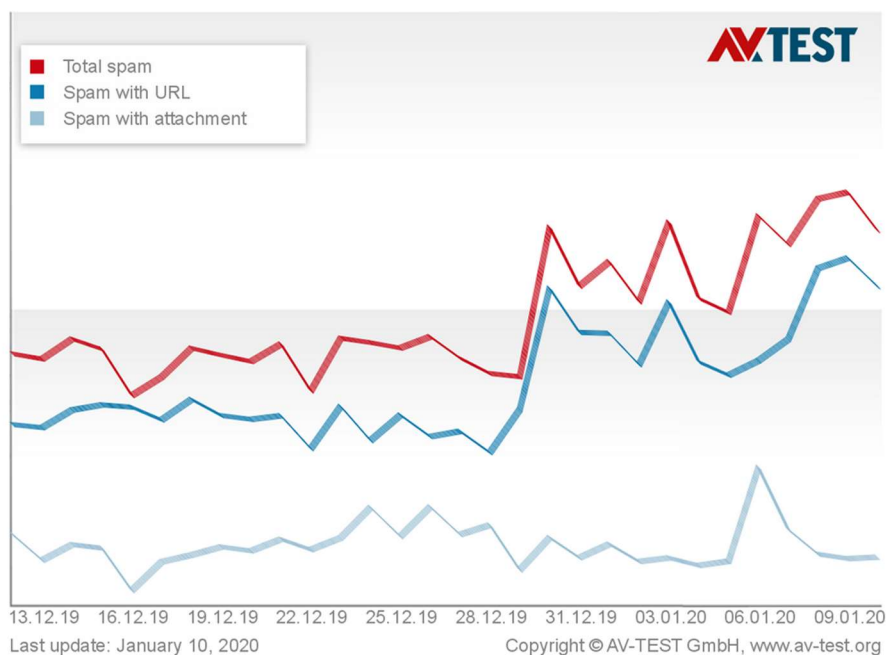
Origin of Spam per Country, last 60 days



(Source: <https://www.av-test.org/en/statistics/spam/>)

The chart below gives the three main spam categories

Spam ratio, last 30 days



(Source: <https://www.av-test.org/en/statistics/spam/>)

Malicious insider

Malicious insiders can be employees, former employees, contractors or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data or



sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.

There are many reasons an insider can be or become malicious including revenge, coercion, ideology, ego or seeking financial gain through intellectual property theft or espionage.

They could:

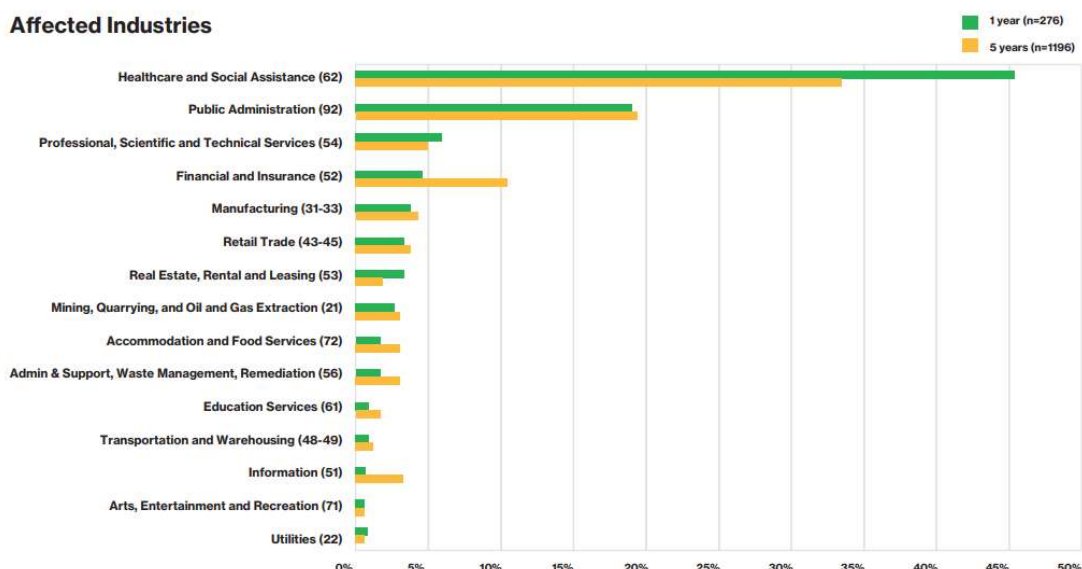
- impact external sites, creating public damage to your brand
- prevent your systems from functioning properly
- steal or sell business trade secrets or intellectual property (IP)
- Install malware for their own purposes.

Cyber adversaries can use employees whose trust they have gained to access your business systems and accounts. Employees could provide information to a malicious insider unknowingly, or mention sensitive details in trust.

(Source: <https://www.cyber.gov.au/threats/malicious-insiders>).

As you can see in the chart below, Healthcare and Social Assistance are in the first place of the affected Industries from insider attacks.

Affected Industries



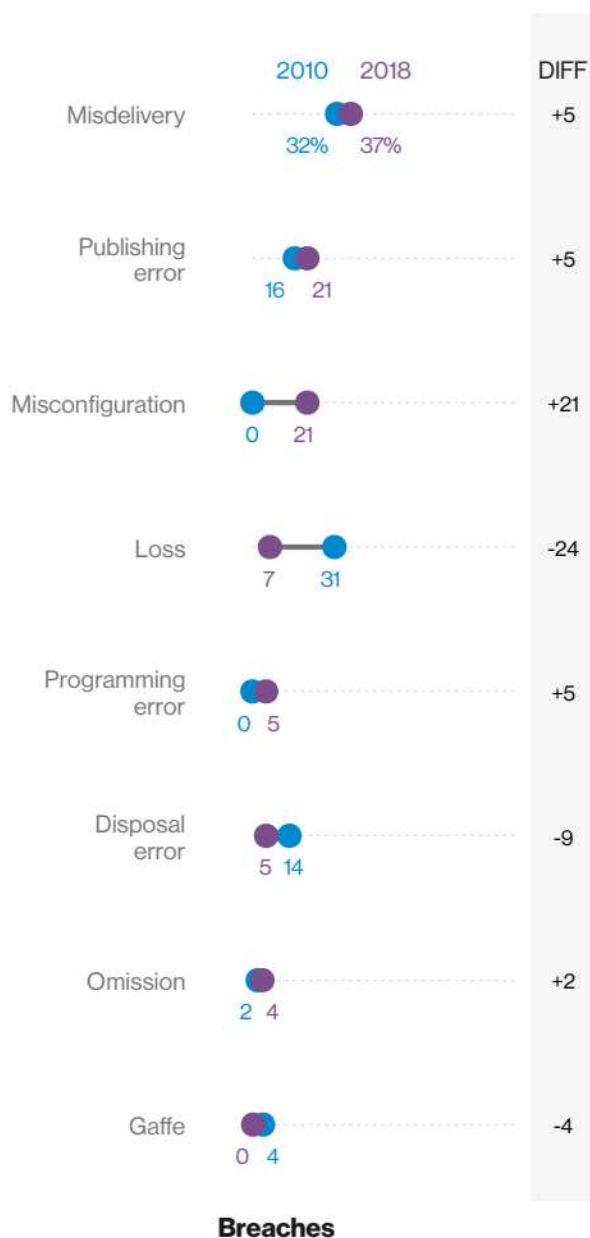
Source: Verizon Insider Threat Report

(Source: <https://www.fairwarning.com/insights/blog/5-types-of-insider-threats-in-healthcare-and-how-to-mitigate-them>, article March 2019)

Error

A final important term is Error. Errors (human or otherwise) is an act or instance that either through ignorance, deficiency, or accident deviates from or fails to achieve what should be done.

Some of the error varieties and their behavior over time are shown in the following figure. The top two error varieties are consistent with previous years performance, with Misconfiguration increasing at the expense of Loss and Disposal Errors. Sending data to the incorrect recipients (either via email or by mailed documents) is still an issue. Similarly, exposing data on a public website (publishing error) or misconfiguring an asset to allow for unwanted guests also remain prevalent.



(Source: Verizon, 2019 Data Breach Investigations)

Trends, statistics and examples

Based on the information from the 2019 Data Breach Investigations Report by Verizon, the healthcare sector is a prime target for attacks.

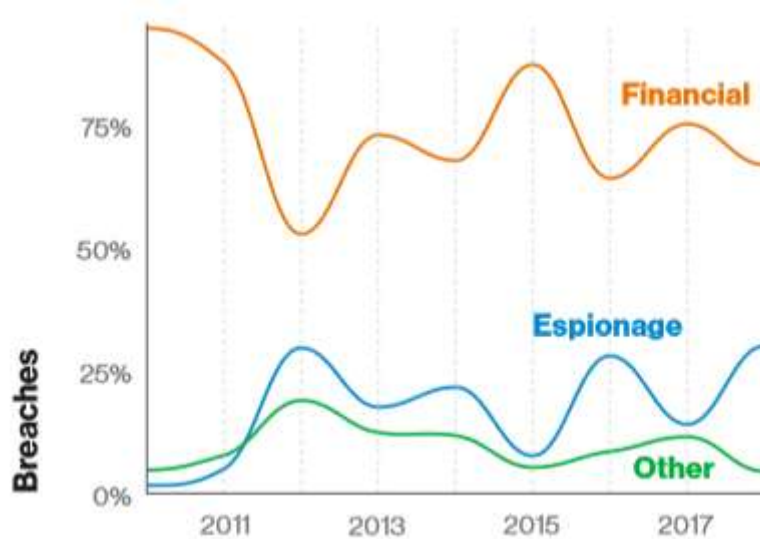
Specifically, as shown in the following figure, 43% of the monitored breaches within the latest report, involved small business victims, 16% involved breaches of Public sector entities, 15% involved breaches of Public sector entities, 15% involving Healthcare Organizations and 10% were breaches of the Financial industry.



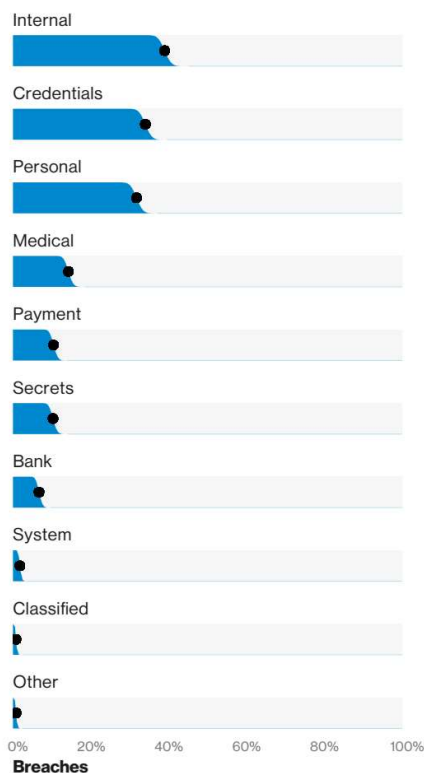
The same report depicts the distribution of breaches based on the location of the threat actors (Internal, External and Partner) over time. As seen in this report, an average value of over 30% of the breaches originate from internal threat actors.



When comparing the motivations behind the breaches, a ratio of 1:3 is observed between Espionage and Financial gain.



Finally, the following figure details the varieties of data that were disclosed as a result of the data breaches that occurred this year. Personal information is once again prevalent. Credentials and Internal are statistically even, and are often both found in the same breach. Credential theft leading to the access of corporate email is a very common example.



(Source: Verizon, 2019 Data Breach Investigations)

Analysis of the Healthcare Industry

The following extract from the Verizon 2019 Data Breach Investigations Report and is included here as further material that the DPO of a Healthcare organization should bare into mind regarding the industry.

Healthcare

Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.

Frequency	466 incidents, 304 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Privilege Misuse and Web Applications represent 81% of incidents within Healthcare
Threat actors	Internal (59%), External (42%), Partner (4%), and Multiple parties (3%) (breaches)
Actor motives	Financial (83%), Fun (6%), Convenience (3%), Grudge (3%), and Espionage (2%) (breaches)
Data compromised	Medical (72%), Personal (34%), Credentials (25%) (breaches)

The doctor can't see you now (that you work for them)

Most people do not enjoy going to the hospital, but once it becomes unavoidable we all need to believe fervently that the good women and men who are providing us care are just this side of perfect. Spoiler alert: they are not. Healthcare is not only fast paced and stressful, it is also a heavily-regulated industry. Those who work in this vertical need to do things right, do things fast, and remain in compliance with legislation such as HIPAA and HITECH (in the US). That in itself is a pretty tall order, but when one combines that with the fact that the most common threat actors in this industry are internal to the organization, it can paint a rather challenging picture.

With internal actors, the main problem is that they have already been granted access to your systems in order to do their jobs. One of the top pairings in Table 5 between actions and assets for Healthcare was privilege abuse (by internal actors) against databases. Effectively monitoring and flagging unusual and/or inappropriate access to data that is not necessary for valid business use or required for patient care is a matter of real concern for this vertical. Across all industries, internal actor breaches have been more difficult to detect, more often taking years to detect than do those breaches involving external actors.

Mailing it in

The Healthcare industry has a multifaceted problem with mail, in both electronic and printed form. The industry is not immune to the same illnesses we see in other verticals such as the very common scenario of phishing emails sent to dupe users into clicking and entering their email credentials on a phony site. The freshly stolen login information is then used to access the user's cloud-based mail account, and any patient data that is chilling in the Inbox, or Sent Items, or other folder for that matter is considered compromised – and its disclosure time.

Misdelivery, sending data to the wrong recipient, is another common threat action variety that plagues the Healthcare industry. It is the most common error type that leads to data breaches as shown in Figure 51. As seen in Table 5 on the next page, documents are a commonly compromised asset. This could be due to errors in mailing paperwork to the patient's home address or by issuance of discharge papers or other medical records to the wrong recipient.

Ransomware "breaches"

Most ransomware incidents are not defined as breaches in this study due to their lack of the required confirmation of data loss. Unfortunately for them, Healthcare organizations are required to disclose ransomware attacks as though they

Things to consider:

Know where your major data stores are, limit necessary access, and track all access attempts. Start with monitoring the users who have a lot of access that might not be necessary to perform their jobs, and make a goal of finding any unnecessary lookups.

Work on improving phishing reporting to more quickly respond to early clickers and prevent late clickers. Think about reward-based motivation if you can – you catch more flies with honey. And you can catch phish with flies. Coincidence?

Know which processes deliver, publish or dispose of personal or medical information and ensure they include checks so that one mistake doesn't equate to one breach.



Table 5
Top pairs of threat action varieties and asset varieties. (n= 304)



Lesson 2: Information Security Basics

Unit 1: What is Information Security

Question 1.:

Which of the following definitions fits better to the term Information Security?

1. Information security ensures the confidentiality, availability and integrity of information.
2. Information security ensures the feasibility, buoyance and integrity of information.
3. Information security ensures the nationality, solidarity and availability of information.
4. Information security ensures the correctness, applicability and iteration of information.

Question 2.:

The following incident was a failure of which of the characteristics of Information Security?

Yahoo! data breaches

From Wikipedia, the free encyclopedia



This article needs to be **updated**. Please update this article to reflect recent events or newly available information. (December 2017)

The Internet service company **Yahoo!** reported two major **data breaches** of user account data to **hackers** during the second half of 2016. The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over 500 million Yahoo! user accounts.^[1] A separate data breach, occurring earlier around August 2013, was reported in December 2016. Initially believed to have affected over 1 billion user accounts,^[2] Yahoo! later affirmed in October 2017 that all 3 billion of its user accounts were impacted.^[3] Both breaches are considered the **largest discovered in the history of the Internet**. Specific details of material taken include names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and **hashed passwords**.^[4] Further, Yahoo! reported that the late 2014 breach likely used **manufactured web cookies** to falsify login credentials, allowing hackers to gain access to any account without a password.^{[5][6][7][8]}

Yahoo! has been criticized for their late disclosure of the breaches and their security measures, and is currently facing several lawsuits as well as investigation by members of the United States Congress. The breaches have impacted **Verizon Communications's** July 2016 plans to acquire Yahoo! for about \$4.8 billion, which resulted in a decrease of \$350 million in the final price on the deal closed in June 2017.

1. Integrity
2. Availability
3. Non-repudiation
4. Confidentiality

Unit 2: Information Security Management System

Question 3.:

What is an Information Security Management System?

1. A collection of IT controls
2. A nice way of implemented Risk Assessment
3. Just another buzz word
4. A best practice in order to achieve and maintain a uniform and predefined level of information security within an organization

Question 4.:

Which of the following is **NOT** a valid reason to implement an effective ISMS?



1. achieve greater assurance that its information assets are adequately protected against threats on a continual basis;
2. maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness;
3. achieve legal and regulatory compliance.
4. gain a discount in a marketing campaign

Unit 3: International Best Practices

Question 5.:

Which of the following standards describe best practices for an Information Security Management System?

1. ISO 27001:2013
2. ISO 27000:2018
3. ISO 27701:2019
4. ISO 27002:2013

Unit 4: Known threats and Threat Agents

Question 6.:

Which of the following best describes the term threat?

1. Something that will happen in the future
2. Bad luck
3. A potential cause of an incident, which may result in harm of systems and organization
4. A weakness of system or a location

Question 7.:

Which of the following are valid threats?

(Select all that apply)





Question 8.:

Which of the following are valid Data Security related threats?

(Select all that apply)

<input checked="" type="checkbox"/> Malware	<input checked="" type="checkbox"/> Spam	<input checked="" type="checkbox"/> Phishing
<input checked="" type="checkbox"/> Botnets	<input type="checkbox"/> Emails	<input type="checkbox"/> Discussions

Question 9.:

Which of the following are valid threat agents?

(Select all that apply)

<input checked="" type="checkbox"/> Criminal groups	<input type="checkbox"/> Neighbors	<input type="checkbox"/> Consumers
<input checked="" type="checkbox"/> Foreign intelligence services	<input type="checkbox"/> Staff dependents	<input checked="" type="checkbox"/> Hackers

Question 10.:

Which of the following depict a vulnerability?



X X X



Question 11.:

Which of the following best describes the term Attack?



1. An attack is an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
2. An attack is the possibility of something bad happening
3. An attack is only something that can happen between different nations
4. An attack is something that can happen to other people.

Question 12.:

Which of the following are NOT Attacks that can affect the security of data?

1. Hacking
2. Social engineering
3. Malware
4. Employee strike

Unit 5: Trends, statistics and examples

Question 13.:

Which of the following statements are TRUE?

(Select all that apply)

1. 43% of the monitored breaches involved small business victims
2. 90% involved breaches of Public sector entities
3. 1% involving Healthcare Organizations and
4. 10% were breaches of the Financial industry.

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 3, unit 1-3

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Risk Management

Definitions

ISO 31000:2018. Risk management — Guidelines, provides amongst others the definitions for the following terms:

Risk

“the effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.”

(Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood. (Source: ISO Guide 73))

Risk management

coordinated activities to direct and control an organization with regard to risk

Consequence

outcome of an event affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

Likelihood

chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

Control

measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

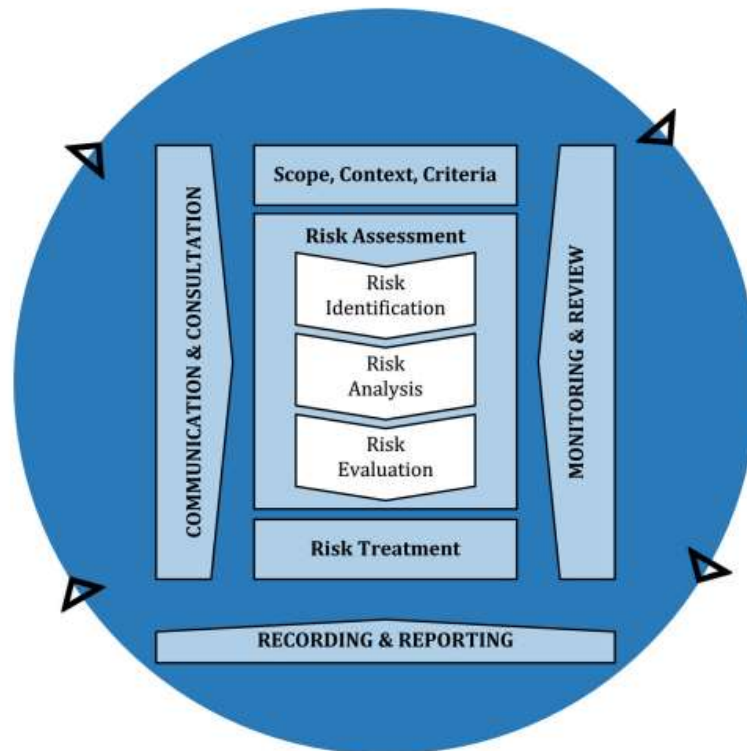
Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

The Risk Management Process

The following figure depicts the various steps that need to be undertaken within the Risk Management Process. Quite often, the Risk Management process is confused with Risk Assessment or Risk Analysis. As shown also in the following figure, risk assessment and Risk Analysis are only parts of the process. An organization should implement an effective Risk Management process in order to be better prepared against potential risks.



(Source: ISO 31000:2018. Risk management — Guidelines)

The following sections will describe the steps that need to be undertaken while implementing the Risk Management process as recommended by ISO 31000:2018.

Scope, Context, Criteria

Before the initiation of the Risk Management Process, it is crucial that the Scope (the extent and boundaries of applicability of the process) be defined. The team involved in the design, implementation and management of the Risk Related activities should be aware regarding the objectives of the project, the assets (information is also an asset) that are under the control of the process and the influencing factors.

The last ones (more commonly referred to as internal and external factors of the context of an organization) can be further analyzed as internal and external. Some indicative factors that belong to each category are depicted below:

Internal	External
----------	----------



The objectives of the organization	The location of the organization
The Policies, Procedures and Guidelines	The current legal and regulatory requirements
The Implemented controls	The contractual obligations to clients
The available resources	The contractual restrictions imposed by Suppliers
The personnel	The competitors
The culture of the organization	The Insurers
The awareness level	The stakeholders
The information that is going to be affected and its value for the organization	

In risk management, the identified Risks have to be assessed and the compared to the organizations risk appetite, in order to decide upon the Risk Treatment option to be employed.

To do this, the following criteria have to be defined:

- Risk Assessment Criteria and
- Risk Acceptance Criteria

Risk Assessment criteria are the parameters that will be used in order to estimate the level of Risk and Risk acceptance criteria are the criteria against which the comparison will be performed in order to identify whether a risk is acceptable or not.

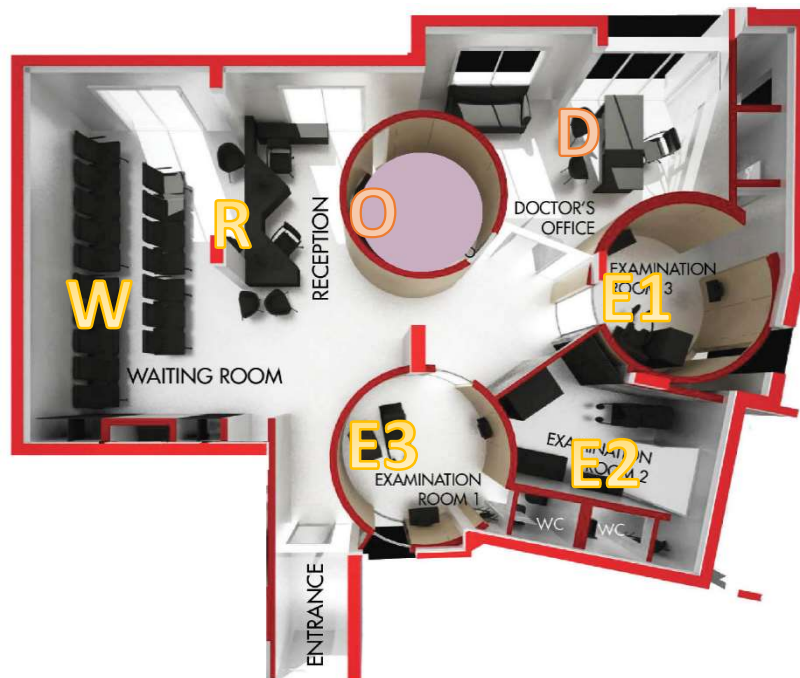
The most typical Risk Assessment Criteria are Impact and Likelihood. For each of these criteria, suitable scales have to be created (or adopted) that will fit the organization. The criteria have to be used consistently throughout the process, in order to produce comparable, reproducible and valid results.

For a better understanding of the Risk Assessment Criteria, the following example is provided:

Scope: The doctor, wishes to access the risks related to the private data of the patients and the employees processed by his office.

Context:

The office is located in the third floor of a modern building in the center of Athens, Greece. The applicable legislation and regulations are: The GDPR and the relevant Greek law for Personal information. More information can be found at www.dpa.gr.



The above overview, presents a small doctor's office. The following information is provided:

Space O: Contains the Computer Server of the office and houses the physical archive of the office.

Space W: Is the waiting room. In the waiting room, patients wait patiently for their turn while enjoying web surfing through the Free Wifi Connection provided by the Office. The Wifi has no password and it is part of the same internet feed that is used by the rest of the office.

Spaces E1, E2, E3: Are the examination rooms. These rooms have specific medical devices installed, all of which connect to the internal network of the office, since they need to send and receive files of examinations and get updated of the machine's firmware.

Space R: Is the reception area. Typically one and in some cases two persons man the reception desk. Their main functions include the management of the appointments, the deciphering of the doctor's notes in order to issue receipts, notices and referrals, and the maintenance of the physical and digital patient files.

Space D: Is the doctor's office. The doctor has a computer with access to the internet, the local server and all the medical equipment.

Objective: The objective and motive for the project, is the fact that the doctor does not want any breach regarding this information and no fine imposed to him by the relevant supervisory authority.

Criteria:

The project team decided to adopt the following criteria:

Risk Assessment: The two basic selected criteria are Likelihood and Impact and the selected scales are depicted below:



Impact (I)

1	2	3	4	5
Non personal information lost.	A few of the personal data of employees have been lost.	Some personal data of the employees and some of the patient personal data are unavailable.	All personal data of the employees have been leaked.	Breach affecting all employee and patient Personal Data. All data have been accessed by unauthorized entities.

Likelihood (L)

1	2	3	4	5
It is unlikely to happen OR Never heard this happening of in the industry	It is to Happen or Never heard this happening of in the industry	It could possibly happen Or Has happened in our organization or more than once per year in the industry	It will probably happen Or Has happened at the location or more than once per year in our organization	It is or has already happened Or Has happened more than once per year at the location

In order to estimate the Risk, a formula has to be used that combines the Risk Assessment criteria. In this case, the formula $R = L \times I$ is used.

The multiplication of the two scales of Likelihood and Impact produces the following table.

Impact→ ↓Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Risk acceptance criteria

The risk acceptance criteria, are set by top management and depict their tolerance regarding risk. The criteria always refer to a combination of the Risk assessment criteria (L, I).



In this case, the management has decided that the Risk Acceptance is 12. This means that top management does not accept risks that:

- a) Will possibly / Or This has happened in our organization / or this has happened more than once per year in the industry (3) – lead to all personal data of the employees being leaked (4) or
- b) Will probably happen / Or This Has happened at the location or more than once per year in our organization (4) - Some personal data of the employees and some of the patient personal data are unavailable (3)

The acceptance criteria can also be depicted in the combined matrix produced above:

Impact→ ↓Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Where Red depicts the unacceptable values of risk and green depicts the acceptable ones.

Risk Assessment

Risk assessment is split to the following three tasks: Risk Identification, Risk Analysis and Risk Evaluation.

Risk Identification

ISO 31000:2018, defines Risk Identification as follows:

“The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.”

In Risk identification the organization will employ any technique suitable for them in order to identify as many Risks as humanly – logically possible.

Please note, that it would be a mistake to identify only the 5 ones that seem more prominent or interesting or easy to deal with. Risk Management is a preventive mechanisms that aims to protect the organization. If it is not properly used, then it can not become a valuable and effective protection tool for the organization.

The outcome of this task is a list of risks.

To continue the example mentioned above, some of the risks that could be identified are contained in the following table. Please keep in mind that this list is indicative and in no way inclusive of all risks:

Threat	Vulnerability	Risk
--------	---------------	------



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

Loss of power supply	Susceptibility to voltage variations	Loss of the availability of the equipment and the related information due to power failure
Abuse of rights	Well-known flaws in the software	Data Leakage because of the exploitation of flaws in the software
Remote Spying	Insecure network architecture	Data leakage by malicious externals because of lack of security in the network architecture
Failure of telecommunication equipment	Single point of failure	Loss of communication availability due to Hardware failure of the main internet modem (Single point of failure)
Error in use	Lack of security awareness	Data Leakage of patient data because of Lack of security awareness
Loss of data	Inadequate or careless use of physical access control to buildings and rooms	Loss of data due to the lack of access control mechanisms in the rooms and office
Fire	Flammable material in the office area.	Destruction of data and equipment due to fire.
Theft of media or documents	Lack of established monitoring mechanisms for security breaches	Theft of media or documents due to lack of relevant monitoring.
Unauthorized access	Poor access control mechanisms to sensitive information	Unauthorized access to patient data due to poor access control mechanisms

Risk Analysis

ISO 31000:2018, defines Risk Analysis as follows:

“The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives. Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.”

The output of the risk analysis step, is a table containing the estimated values of the risk assessment criteria per identified (through the previous step) risk.

To continue the example mentioned above, an estimation was carried out regarding the values of likelihood and impact of the identified risks. This step is called estimation since the values are not precisely calculated (with accuracy) but rather estimated.

The estimation can be based on historical records, the information provided by the manufacturer, industry insights, scientific publication, monitoring implemented by the organization, expert opinion or the opinion of the people involved with the process.

In the case of the example, the values that have been inserted are fictional.

Threat	Vulnerability	Risk	L	I	R
Loss of power supply	Susceptibility to voltage variations	Loss of the availability of the equipment and the related information due to power failure	4	3	12
Abuse of rights	Well-known flaws in the software	Data Leakage because of the exploitation of flaws in the software	3	5	15
Remote Spying	Insecure network architecture	Data leakage by malicious externals because of lack of security in the network architecture	5	5	25
Failure of telecommunication equipment	Single point of failure	Loss of communication availability due to Hardware failure of the main internet modem (Single point of failure)	4	1	4
Error in use	Lack of security awareness	Data Leakage of patient data because of Lack of security awareness	2	5	10
Loss of data	Inadequate or careless use of physical access control to buildings and rooms	Loss of data due to the lack of access control mechanisms in the rooms and office	3	5	15

Fire	Flammable material in the office area.	Destruction of data and equipment due to fire.	2	3	6
Theft of media or documents	Lack of established monitoring mechanisms for security breaches	Theft of media or documents due to lack of relevant monitoring.	2	5	10
Unauthorized access	Poor access control mechanisms to sensitive information	Unauthorized access to patient data due to poor access control mechanisms	3	5	15

Risk Evaluation

ISO 31000:2018, defines Risk Evaluation as follows:

“The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.”

This step encompasses the comparison of the estimated values of risk (based on the previous Risk Analysis step) with the risk acceptance criteria. Any risks that will be identified to be unacceptable, will have to be treated (this is described in the following step – Risk Treatment). All the risks that are deemed acceptable, are the risks that the organization is knowingly willing to take and will not at this time consider them for any further actions.

In the case of the example, as described in the Scope, Context and Criteria section, the risk acceptance criteria is 12. So, the table that was derived in the previous step is transformed as follows

Threat	Vulnerability	Risk	L	I	R	Eval
Loss of power supply	Susceptibility to voltage variations	Loss of the availability of the equipment and the related information due to power failure	4	3	12	Un-acceptable
Abuse of rights	Well-known flaws in the software	Data Leakage because of the exploitation of flaws in the software	3	5	15	Un-acceptable

Remote Spying	Insecure network architecture	Data leakage by malicious externals because of lack of security in the network architecture	5	5	25	Un-acceptable
Failure of telecommunication equipment	Single point of failure	Loss of communication availability due to Hardware failure of the main internet modem (Single point of failure)	4	1	4	Acceptable
Error in use	Lack of security awareness	Data Leakage of patient data because of Lack of security awareness	2	5	10	Acceptable
Loss of data	Inadequate or careless use of physical access control to buildings and rooms	Loss of data due to the lack of access control mechanisms in the rooms and office	3	5	15	Un-acceptable
Fire	Flammable material in the office area.	Destruction of data and equipment due to fire.	2	3	6	Acceptable
Theft of media or documents	Lack of established monitoring mechanisms for security breaches	Theft of media or documents due to lack of relevant monitoring.	2	5	10	Acceptable
Unauthorized access	Poor access control mechanisms to sensitive information	Unauthorized access to patient data due to poor access control mechanisms	3	5	15	Un-acceptable

Risk Treatment

ISO 31000:2018, defines Risk Treatment as follows:

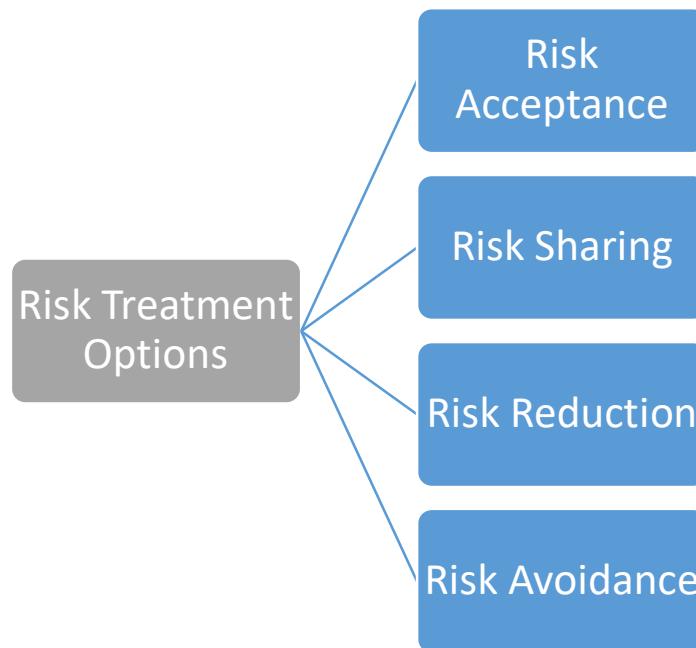
“The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:

— formulating and selecting risk treatment options;

- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable;
- if not acceptable, taking further treatment.”

There are four main risk treatment options:



Risk Acceptance: Although a risk may be above the Risk acceptance criteria, the organization may decide to not implement any actions at this time to modify the risk.

Risk Sharing: This is typically implemented by sharing the risk (or the impacts of the risk should it materialize) with a third party either through insurance or through subcontracting or outsourcing.

Risk Reduction: This option aims to the reduction of any or all of the risk assessment criteria.

Risk Avoidance: This option involved the modification of the way the organization is functioning aiming to remove the risk all together.

In the case of the example, the risks that were unacceptable will undergo the risk treatment step as follows:

Risk	L	I	R	Eval	Treatment Option	Treatment Description
Loss of the availability of the equipment and the related	4	3	12	Un-acceptable	Risk Reduction	Install UPS in all critical equipment

information due to power failure						
Data Leakage because of the exploitation of flaws in the software	3	5	15	Un-acceptable	Risk Reduction	Implement a Patch Management procedure
Data leakage by malicious externals because of lack of security in the network architecture	5	5	25	Un-acceptable	Risk Avoidance	Disconnect the network from the internet
Loss of data due to the lack of access control mechanisms in the rooms and office	3	5	15	Un-acceptable	Risk Acceptance	No measures at this time since the organization is moving to another facility soon
Unauthorized access to patient data due to poor access control mechanisms	3	5	15	Un-acceptable	Risk Reduction	Implement an access control policy

The actions and other information regarding Risk Treatment are documented in a form called Risk Treatment Plan.

The risk treatment plan typically includes the following information:

Risk to be treated | Level of risk before treatment | What will be done | Who will be responsible | Until when this should be done | The results of the risk treatment | The evaluation of the results.

So, an example from the above risks is

Risk	R	Treatment Option	Treatment Description	Responsible	Deadline	Results	Evaluation
Loss of the availability of the equipment and the related information due to power failure	12	Risk Reduction	Install UPS in all critical equipment	IT Manager	1/3/2020	[Expected level of risk: 3*3 =9]	



Recording & Reporting

ISO 31000:2018, defines Risk Recording & Reporting as follows:

“The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the organization;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.”

Communication & Consultation

ISO 31000:2018, defines Risk Communication & Consultation as follows:

“The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.”

Monitoring & Review

ISO 31000:2018, defines Risk Monitoring & Review as follows:

“The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.”

Risk Management, as shown also in the previous paragraphs should be a systematic process, with distinct steps and specific inputs and outputs for each step. These inputs and outputs have to be documented in order to achieve the Risk Management objectives. Moreover, Risk Management is not a task that is undertaken by one individual and remains a secret to the rest. The identified risks have to be communicated to the Top Management and specific decisions have to be taken. In every case, the risk appetite (how risky the organization wants to be) and the residual risks (the risks that remain) should be known and understood by all involved parties.

Finally, it has to be understood that Risk Management is not a process that is implemented once and then forgotten. To make it an effective tool, it should remain current and adapt to the current



situation of the organization. The employees and other interested parties should feed the process with new identified or emerging risks, changes in the organization and its context, events and incidents and any other information needed in order to better protect the organization and its information.



Lesson 3: Risk Management

Unit 1: Definitions

Question 1.:

Which of following best describes the term Risk?

1. the effect of uncertainty on objectives
2. the uncertainty of the environment
3. the impact of an attack
4. the possibility of something happening

Unit 2: The Risk Management Process

Question 2.:

Which of the following are steps of the Risk Management process as described by ISO 31000?

1. Scope, criteria and context
2. Risk Analysis
3. Risk Termination
4. Risk Treatment
5. Risk Consultation
6. Risk measurement

Question 3.:

Which of the following are possible outcomes of the Risk Management process as described by ISO 31000?

1. A list of risks
2. Identified risk owners
3. Risk Treatment plans
4. Attackers
5. Marketing plans
6. Policies

Question 4.:

Which of the following are risk treatment options?

1. Accept the Risk
2. Avoid the Risk
3. Reduce the Risk
4. Ignore the Risk
5. Transfer the Risk
6. Hide the risk

Question 5.:

What is the first step of the risk assessment?

1. Evaluate the risks



2. Identify the risks
3. Report the findings
4. All the above

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 4, unit 1-3

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

IT Security Tools

In this section some of the most common IT Security Tools are presented. The DPO should not be (mandatorily) an expert or a practitioner of IT Security and so this is not the aim of this section – making the DPO an IS Expert. What is deemed important though is that the DPO understands the most common IT Security Tools and what can be achieved by them, so that he may have a better overview of the conditions within the organization.

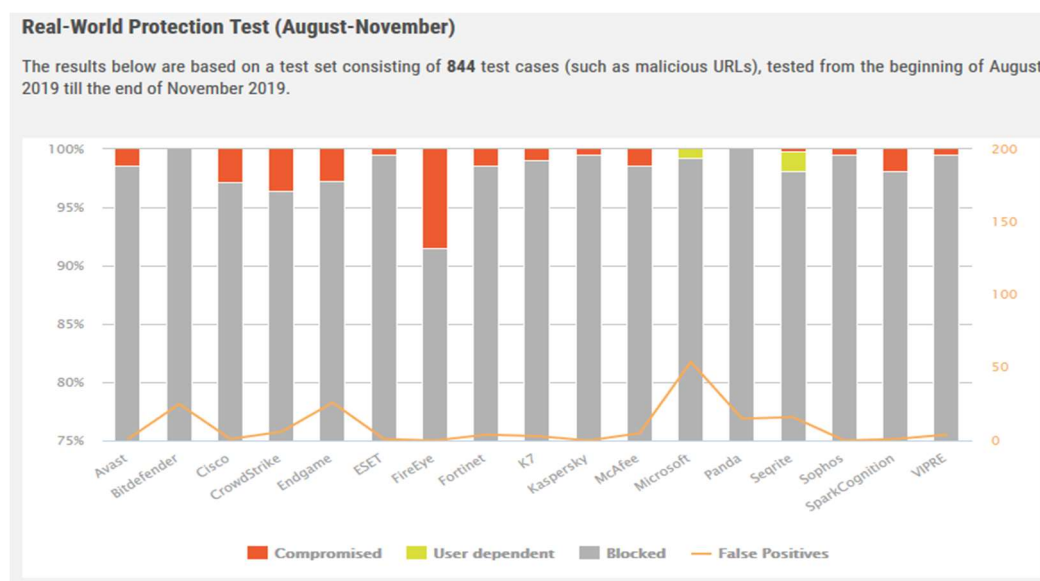
Antivirus

Antivirus software is the most commonly used technical control for malware threat mitigation. There are many brands of antivirus software, with most providing similar protection through the following recommended capabilities:

- Scanning critical host components such as startup files and boot records.
- Watching real-time activities on hosts to check for suspicious activity.
- Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software.
- Scanning files for known malware.
- Identifying common types of malware as well as attacker tools.
- Disinfecting files, which refers to removing malware from within a file, and quarantining files, which means that files containing malware are stored in isolation for future disinfection or examination.

Although antivirus software has become a necessity for malware incident prevention, it is not possible for antivirus software to stop all malware incidents.

There are several comparisons between the antivirus solutions. Find below results from <https://www.av-comparatives.org>



(Source: <https://www.av-comparatives.org/tests/business-security-test-2019-august-november/#malware-protection-test-result>)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2]*	False Alarms
Panda	844	–	–	100%	15
Bitdefender	844	–	–	100%	25
Microsoft	837	7	–	99.6%	45
Kaspersky, Sophos	840	–	4	99.5%	0
ESET	840	–	4	99.5%	1
VIPRE	840	–	4	99.5%	4
K7	836	–	8	99.1%	3
Seqrite	828	14	2	98.9%	16
Avast	832	–	12	98.6%	1
Fortinet	832	–	12	98.6%	4
McAfee	832	–	12	98.6%	5
SparkCognition	828	–	16	98.1%	1
Endgame	821	–	23	97.3%	26
Cisco	820	–	24	97.2%	1
CrowdStrike	814	–	30	96.4%	6
FireEye	772	–	72	91.5%	0

(Source: <https://www.av-comparatives.org/tests/business-security-test-2019-august-november/#malware-protection-test-result>)

Firewall

A firewall software or hardware monitors incoming and outgoing network traffic and decides whether specific traffic needs to be allowed or blocked based on a defined set of security rules that each organization applies in accordance with their security level.

Types of networks:

WAN: The interface which connects the internal network to the Internet

LAN: Is the internal network of the company. All the assets included PCs, Printers, Access Points, Servers etc. are part of the LAN

DMZ (demilitarized zone): Separates the internal network from other untrusted networks, usually the Internet. It is usually used for Web servers, DNS, FTP.

Firewall features

Most of firewalls include extra features such as AV, IPS, Antispam, Content filter, etc.

IDPS: Intrusion detection prevention system is a technology that identifies suspicious activities which detects and also prevents from unwanted requests to the internal network.

Content filter: The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.

VPN (Virtual Private Network): Is a network that uses internet to connect remotely users or regional offices to an internal network.

The following picture, depicts the Gartner Magic Quadrant for firewall brands.



(Source: <https://www.gartner.com/doc/reprints?id=1-1OIMBCY&ct=190919&st=sb>)

SIEM

Security Information and Event Management (SIEM) is a system for monitoring, recording and analysis in real time all the data in an IT infrastructure, allowing the correlation of events and generate reports on the critical functions of the infrastructure systems.

The following image from Esecurityplanet, depicts a comparison between various SIEM vendors according to specific characteristics (e.g. threats blocked, sources ingested, value, performance, management, implementation and others).

SIEM Features Compared

Top SIEM Vendors								
SIEM VENDOR	●●●● BEST ●●● VERY GOOD ●● GOOD ● FAIR							
	THREATS BLOCKED	SOURCES INGESTED	PERFORMANCE	VALUE	IMPLEMENTATION	MANAGEMENT	SUPPORT	SCALABILITY
splunk> ES	●●●●	●●●	●●●	●●●	●●	●●●	●●	●●●
LogRhythm ENTERPRISE	●●●	●●●●	●●●	●●	●●●	●●●	●●●	●●
USM	●●●	●●●	●●●	●●●●	●●●	●●	●●	●●●
MICRO FOCUS ArcSight	●●	●●●	●●●	●●	●●●	●●●●	●●	●●●
MICRO FOCUS Sentinel	●●	●●	●●	●●●	●●●	●●●	●●	●●●
McAfee ESM	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●
Trustwave SIEM	●●●	●●●	●●●	●●●	●●	●●●	●●	●●●●
IBM Radar	●●●	●●●	●●●●	●●●	●●	●●●	●●●	●●●
RSA NetWitness	●●	●●	●●●	●●	●●	●●	●●●	●●●
solarwinds LEM	●●	●●●	●●	●●	●●●●	●●	●●●	●●

SOURCE: eSecurityPlanet.com

(Source: <https://www.esecurityplanet.com/products/top-siem-products.html#features>)

And the following picture, depicts the Gartner Magic Quadrant for SIEM brands.



(Source: Gartner (December 2018), <https://www.51sec.org/2019/01/11/gartner-magic-quadrant-for-siem-products-2016-2015-2014-2013-2012-2011-2010/>)



DLP

Data Loss Prevention (DLP) solutions cover three primary states of information:

- Data at rest refers to stored data. DLP solutions must be able to log where various file types are stored.
- Data in transit refers to data traveling through the network. Deep packet inspection (DPI) is used to analyze the data for sensitive content.
- Data in use refers to data movement at the user workstation level. This includes information sent to printers, thumb drives and the copy-and-paste clipboard.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Although a DLP solution, seems like an ideal solution for managing the privacy of information, one should keep in mind that for an effective DLP implementation, a classification scheme should be in place as well as an effective way of identifying the information and respective level. If an origination does not have a concrete idea regarding what needs to be protected and to what level, then the DLP will not operate effectively. Also, since DLPs use key words, locations or validation algorithms, in an organization that cannot differentiate what is to be controlled based on any of them, a DLP cannot be effectively implemented.

Best Data Loss Prevention Tools

		Free Trial?		Features		Bottom Line
SolarWinds Access Rights Manager		Fully functional, 90-Day	Monitor and manage user access across programs	Use a visual overview to track high-risk access	Minimize the impact of insider threats	This tool offers robust features for managing high-risk user privileges and access for Active Directory, SharePoint, file servers, and more.
SolarWinds Security Event Manager		Fully functional, 90-Day	Event-time correlation of security events	Automated threat remediation	USB device monitoring	This tool utilizes constant log monitoring, alerts, threat intelligence, and automatic responses to protect your sensitive data.
SolarWinds Identity Monitor		Individual email	Employee credential tracking	Researchers monitor the dark web	Track IP address and email breaches	Get peace of mind with a tool that notifies you immediately when certain employee or IP data shows up in online data breaches.
Dynamico DLP		No trial version available	Encryption of all sensitive data	See and control access to data	Stops data theft by monitoring suspicious behaviors on user-installed apps	Appropriate for hybrid environments, it's a scalable choice for enterprises.
SecureTrust DLP		No trial version available	Monitors all web-based attachments and documents	Instant identification of individuals associated with a theft	Offers automatic blocking and encryption for attachments and communications that violate compliance policies	Useful for businesses with minimal DLP experience. Includes 70 pre-set regulation and policy settings.
McAfee Total Protection for DLP		No trial version available	Forensic analysis	Centralized incident management and reporting	Remediate policy violations	This scalable DLP solution for a tech-savvy user ensures that you have the same security policies across your business.
Check Point DLP		Free online demo trial	Very easy to use	Focused on education	Pre-emptive data loss prevention	A program for someone who does not have technological expertise. Focused on educating users about the dangers of data loss and training them to respond immediately.
Verdysys Digital Guardian Endpoint DLP		Free online demo trial	Protects endpoints	Granular control of all data movement	DLP only when you need it	Provides broad coverage across all different types of endpoints with deep visibility into data, user, and system-level events. It works on Mac, Linux, and Windows.
RSA NetWitness Endpoint		Free online demo trial	Continuous endpoint monitoring	Behavioral-based detection	Integrates with many platforms	This tool focuses on monitoring multiple endpoints. RSA does not provide a single tool that will take care of DLP, but the system as a whole is a good way to prevent threats to the network.
Comodo MyDLP		Free 30-Day trial	Single tool	Monitors data in motion, in use, and at rest	Granular policy management	Takes an in-depth, granular approach to monitoring data for DLP. Takes care of what other companies might have several tools do.

(Source: <https://www.dnsstuff.com/data-loss-prevention-software>)



IT Security Controls

In this section some of the most common IT Security Controls are presented. The DPO should not be (mandatorily) an expert or a practitioner of IT Security so this is not the aim of this section. What is deemed important though is that the DPO understands the most common IT Security Controls and what can be achieved by them, so that he may have a better overview of the conditions within the organization. The GDPR only references as examples only the following two controls: encryption and pseudonymisation. This does not mean that only these two exist or that they should be enforced in every case and organization.

Backup

Backups are used to copy files to a second medium such as a disk, tape or the cloud. To ensure better protection and increased resilience backup files should be kept also at an offsite location.

There are three types of backups:

- **Full Backup:** Copies every selected file on the system completely, regardless of recent backup status. Slowest backup method, but fastest for restoring data.
- **Incremental Backup:** Copies all files that have changed since the last backup was made, regardless of whether the last backup was a full or incremental backup. Fastest backup method, but slowest for restoring data.
- **Differential Backup:** Copies only the files that have changed since the last full backup. The file grows until the next full backup is performed.

A backup policy should be established to define the organization's requirements for backup of information, software and systems. The backup policy should define the retention and protection requirements. Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

- a) accurate and complete records of the backup copies and documented restoration procedures should be produced;
- b) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization;
- c) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- d) backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;
- e) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;
- f) in situations where confidentiality is of importance, backups should be protected by means of encryption.



Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

(Source: ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls)

Password Management / Access Control

Access control is the process based on which an entity's (individual, group or system) access to one or more resource such as a location, workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a personal identification number (PIN), card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization. (Definition: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations)

Password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords as much as they can to prevent unauthorized access.

A password management system should:

- a) enforce the use of individual user IDs and passwords to maintain accountability;
- b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- c) enforce a choice of quality passwords;
- d) force users to change their passwords at the first log-on;
- e) enforce regular password changes and as needed;
- f) maintain a record of previously used passwords and prevent re-use;
- g) not display passwords on the screen when being entered;
- h) store password files separately from application system data;
- i) store and transmit passwords in protected form.

(Source: ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls)

Encryption

Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that

restores encrypted data to its original state. (Definition: NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security)

Symmetric encryption: Encryption algorithms using the same secret key for encryption and decryption.

Symmetric Encryption

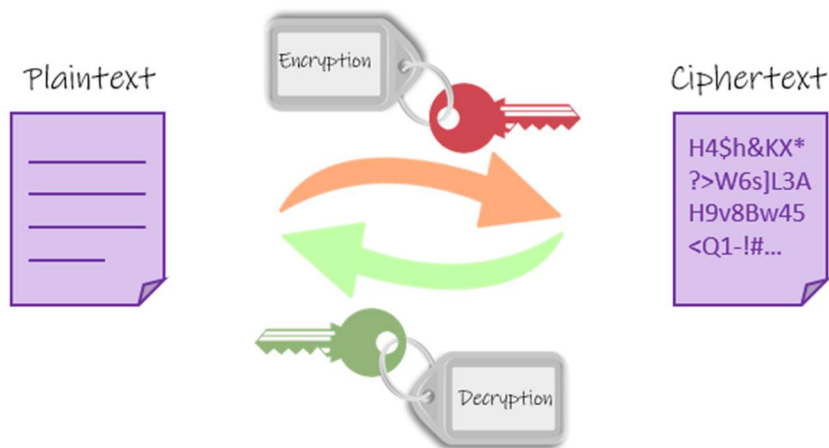


Symmetric Encryption: The same cryptographic key is used both to encrypt and decrypt messages.

(Source: <https://www.101computing.net/symmetric-vs-asymmetric-encryption/>)

Asymmetric encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

Asymmetric Encryption

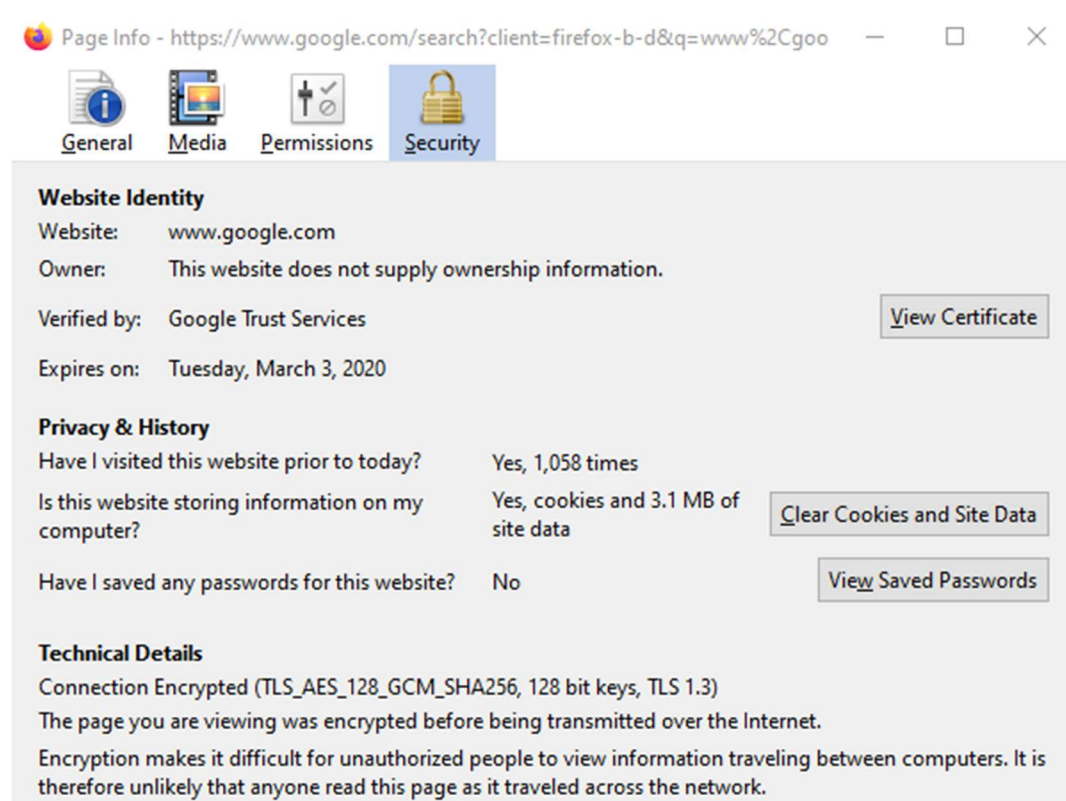
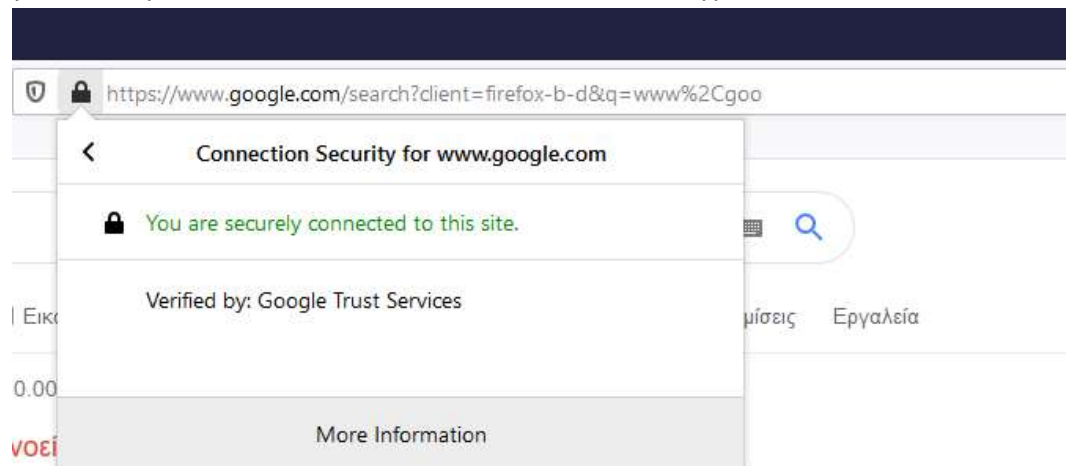


Asymmetric Encryption: A public key is used to encrypt plaintext into ciphertext whereas a private key is used to decrypt a ciphertext.

(Source: <https://www.101computing.net/symmetric-vs-asymmetric-encryption/>)

There are several examples of encryption in our daily life.

Our first example is **HTTPS (Hypertext Transfer Protocol Secure)** that transfers encrypted data through a secure connection. Now days most of web sites are using this protocol and you can check it by your own. Web sites that are using HTTPS have a lock in field that you are typing the URL and if you click it you will have extra information about the encryption.

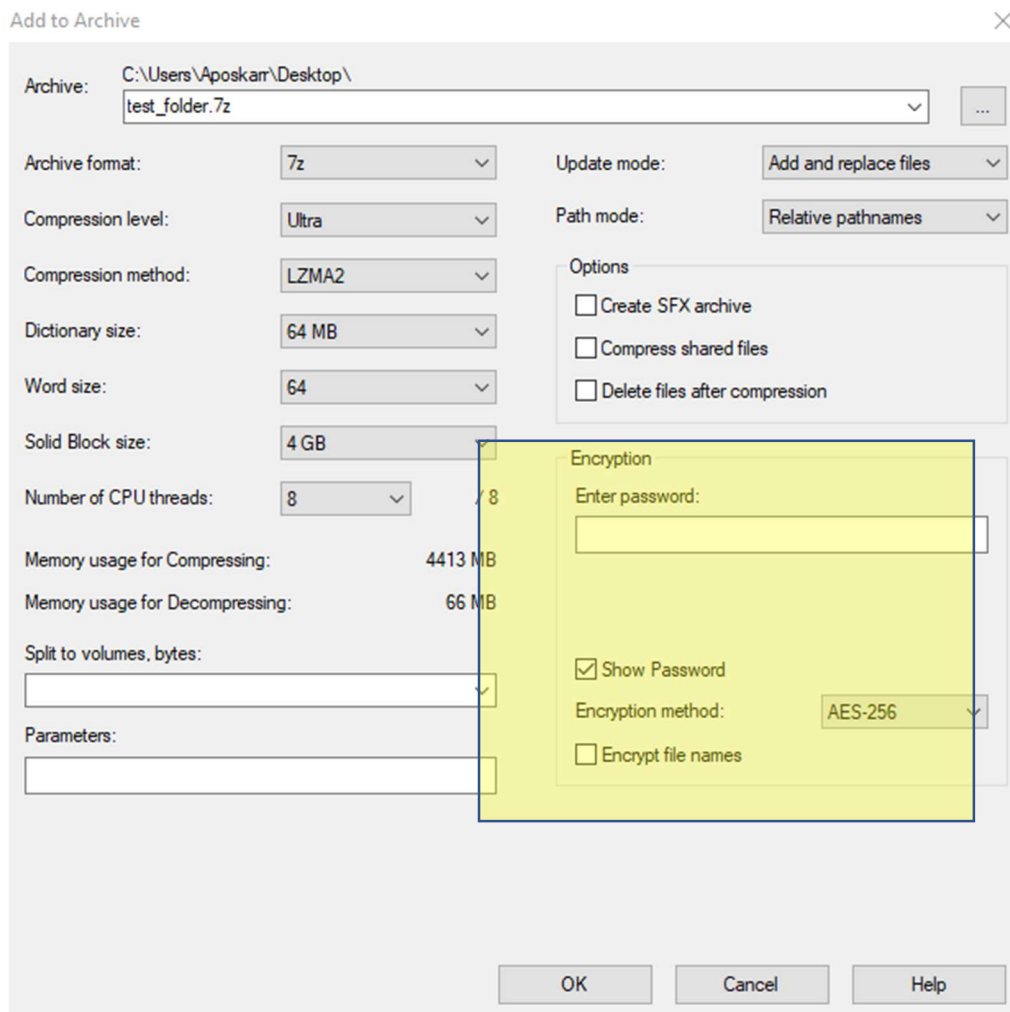


This means that when a user is typing something in this website, the information will be transmitted to the respective server in encrypted format and cannot be read by others.

Another example is the **encryption of files** by adding a password, when we have to send confidential documents through email and we want to be sure that no one else except the receiver will have access to these documents.

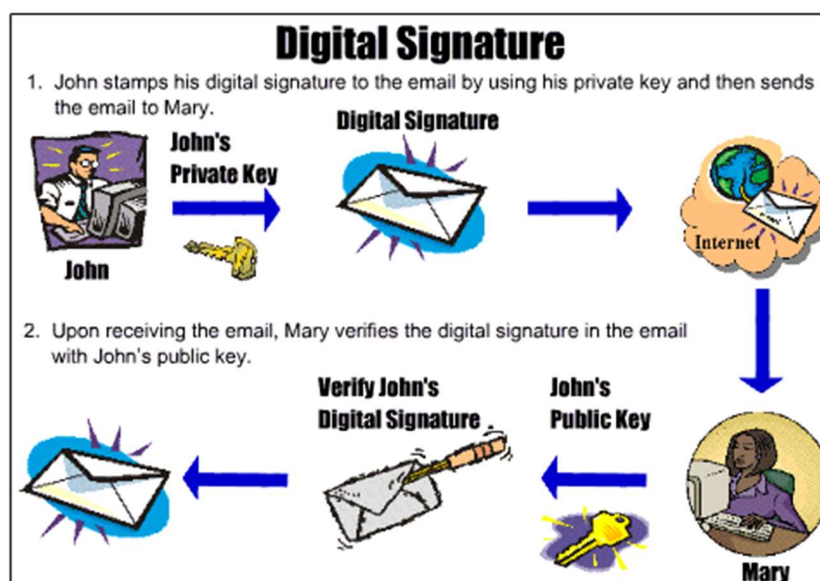


Below, you may see an example of the relevant use of a simple tool (7zip). (Sender needs to send password to receiver through another communication channel).



A final example would be **digital signature** which is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. In emails, the email content itself becomes part of the digital signature. Digital signatures are significantly more secure than other forms of electronic signatures. (Definition: <https://www.us-cert.gov/ncas/tips/ST04-018>).

A digital signature shows beyond doubt that the author of the document / information / etc is who he claims to be.



Taking email as an example, if a digitally signed email has not been tampered with during the course of transmission (integrity), the digital signature will be valid as verified by the recipient. Since the sender is the only person who has access to the corresponding private key, once the digital signature is verified as valid, the recipient can be certain that the email is indeed from the sender (ensuring authenticity); and the sender cannot deny having created and signed the email (non-repudiation).

(Source: https://www.infosec.gov.hk/english/itpro/public_main.html)

Anonymization

Anonymization is a process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party (ISO/TS 25237:2017).

By anonymizing a set of data, the part linked to the identification of a natural person (directly or indirectly) is removed. This makes this set of data non personal as described in the beginning of this document. Since the information is no longer private data, then they fall out of scope of the GDPR.

There are various techniques that could be implemented for anonymizing data sets, and each organization should select the most suitable one based on the context and the contents of the data set.

The fact that the process is irreversible should be taken into account, before an organization performs data anonymization.

Pseudonymization

Pseudonymization is a well-known de-identification process that has gained additional attention following the adoption of GDPR, where it is referenced as both a security and data protection by design mechanism. In addition, in the GDPR context, pseudonymization can motivate the relaxation, to a certain degree, of data controllers' legal obligations if properly applied.

Pseudonymization is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided



g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

- 1) turning off services or capabilities related to the vulnerability;
- 2) adapting or adding access controls, e.g. firewalls, at network borders;
- 3) increased monitoring to detect actual attacks;
- 4) raising awareness of the vulnerability;
- h) an audit log should be kept for all procedures undertaken;

i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

j) systems at high risk should be addressed first;

k) an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;

l) define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

(Source: ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls)

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

(Definition: NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations)

Vulnerability Scanning Tools from OWASP:



Name	Owner	Licence	Platforms
Abbey Scan	MisterScanner	Free	SaaS
Acunetix WVS	Acunetix	Commercial / Free (Limited Capability)	Windows
Application Security on Cloud	IBM	Commercial	SaaS
AppScan	IBM	Commercial	Windows
App Scanner	Trustwave	Commercial	Windows
AppSpider	Rapid7	Commercial	Windows
AppTrana Website Security Scan	AppTrana	Free	SaaS
Arachni	Arachni	Free for most use cases	Most platforms supported
AVDS	Beyond Security	Commercial / Free (Limited Capability)	SaaS
BlueClosure BC Detect	BlueClosure	Commercial, 2 weeks trial	Most platforms supported
BREACHLOCK Dynamic Application Security Testing	BREACHLOCK	Commercial	SaaS
Burp Suite	PortSwigger	Commercial / Free (Limited Capability)	Most platforms supported
Contrast	Contrast Security	Commercial / Free (Full featured for 1 App)	SaaS or On-Premises
Detectify	Detectify	Commercial	SaaS
Digifort- Inspect	Digifort	Commercial	SaaS
edgescan	edgescan	Commercial	SaaS
GamaScan	GamaSec	Commercial	Windows
Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML
Gravtyscan	Defiant, Inc.	Commercial / Free (Limited Capability)	SaaS
Grendel-Scan	David Byrne	Open Source	Windows, Linux and Macintosh
GoLismero	GoLismero Team	GPLv2.0	Windows, Linux and Macintosh
IKare	ITrust	Commercial	N/A
ImmunWeb	High-Tech Bridge	Commercial / Free (Limited Capability)	SaaS
InsightVM		Commercial with Free Trial	SaaS
Intruder	Intruder Ltd.		
Indusface Web Application Scanning	Indusface	Commercial / Free Trial	SaaS
N-Stalker	N-Stalker	Commercial	Windows
Nessus	Tenable	Commercial	Windows
Netsparker	MavituSecurity	Commercial	Windows
Nexpose	Rapid7	Commercial / Free (Limited Capability)	Windows/Linux
Nikto	CIRT	Open Source	Unix/Linux
Probely	Probely	Commercial / Free (Limited Capability)	SaaS
Proxy.app	Websecrify	Commercial	Macintosh
QualysGuard	Qualys	Commercial	N/A

(Source: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools)

Penetration Testing

A penetration test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

There are 3 types of penetration test:

- **White box:** In this type of assessment, the tester is given a lot of information about the system. This will include credentials, architectural diagrams, source code, and any other information. In many cases some rules are applied to firewall and other network devices in order to allow traffic from the tester to the internal network. There is nothing hidden from the tester for this assessment.
- **Gray box:** This type of assessment has many definitions to many people. It is in between black box and white box testing. In this scenario, the tester may receive architectural



diagrams, credentials, demonstrations of the application, communication with the target, and much more. The tester will have the same information as typical user of the system.

- **Black box:** This type of tests closely represent a hacker attempting to gain unauthorized access to a system or IT infrastructure to obtain and exfiltrate data. Black box penetration testing evaluates both the underlying technology as well as the people and processes in place to identify and block real-world attacks. Testers will not have prior knowledge of your organization and architecture.



Lesson 4: IT Security Tools & Controls

Unit 1: IT Security Tools

Question 1.:

Which of the following are capabilities of an Antivirus Solution?

1. Scanning critical host components such as startup files and boot records.
2. Watching real-time activities on hosts to check for suspicious activity.
3. Classifying the files based on importance
4. Scanning files for known malware.

Question 2.:

Which of the following are possible features of a firewall?

1. IPS
2. IDS
3. Antispam
4. Deletion of files

Question 3.:

Which of the following best describes a SIEM?

1. a system for monitoring, recording and analysis in real time all the data in an IT infrastructure, allowing the correlation of events and generate reports on the critical functions of the infrastructure systems
2. a system that monitors incoming and outgoing network traffic and decides whether specific traffic needs to be allowed or blocked based on a defined set of security rules that each organization applies in accordance with their security level.
3. A system that scans critical host components such as startup files and boot records
4. Scans files for known malware.
- 5.

Unit 2: IT Security Controls

Question 4.:

Which of the following are NOT types of Backup?

1. Full
2. Off-site
3. Incremental
4. Definitive

Question 5.:

What does enforcing an access control policy achieve?

1. Everyone gets to access all files
2. Information is accessed on a need to have basis



3. Making the life of the employees difficult
4. Provides valuable information to an attacker

Question 6.:

One of the basic characteristics of anonymization is?

1. The information can not be linked to an identified natural person under any circumstances
2. There is a link between the personal data and the natural person but is known only to a few people
3. The government knows the link between the data and the natural person but not the organization
4. The information is pseudonymized

Question 7.:

Which of the following are NOT types of penetration tests?

1. Black
2. Grey
3. Crystal
4. Red

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 5, unit 1-5

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Data Breaches

Introduction

As part of any attempt to address a breach the DPO should first be able to recognise one. The GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

“destruction” of personal data: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller.

“Damage”: this is where personal data has been altered, corrupted, or is no longer complete.

“loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.

Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

(source: <https://csrc.nist.gov/glossary/term/security-incident> (NIST))

Definitions

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(Source: ENISA overview of cybersecurity and related terminology VERSION 1 SEPTEMBER 2017)

Cyber incident. Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions is called cyber incident. Also we call cyber incident any incident generated by any of cyber space components even if the damage/disruption, dysfunctionality is caused outside the cyber space.

(Source: Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 18/EN WP250rev.01, European Data Protection Board).

So, a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data.

The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst



all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches



Types of personal data breaches

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles:

“Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.

“Integrity breach” - where there is an unauthorised or accidental alteration of personal data.

“Availability breach” - where there is an accidental or unauthorised loss of access¹⁵ to, or destruction of, personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

It is crucial for the DPO to be able to discern the following for each case:

- If an event is a security incident related to private information data breach
- What type of data breach
- What are the consequences of the data breach (since the consequent actions regarding notification are also depending on the impact of the breach [GDPR - Article 33. Notification of a personal data breach to the supervisory authority, * unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, Article 34. Communication of a personal data breach to the data subject * likely to result in a high risk to the rights and freedoms of natural persons])
- What are the actions that need to be performed



Assessment of Impact

ENISA, recommends the following methodology for the assessment of the severity of personal data breached (Source: Recommendations for a methodology of the assessment of severity of personal data breaches - Working Document, v1.0, December 2013)

Criteria

The main criteria taken into account while assessing the severity of a personal data breach are:

- Data Processing Context (DPC): Addresses the type of the breached data, together with a number of factors linked to the overall context of processing.
- Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach.
- Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

Calculation of the severity

Based on the above criteria, the approach of this methodology is the following:

- DPC is at the core of the methodology and evaluates the criticality of a given data set in a specific processing context.
- EI is a correcting factor of the DPC. The overall criticality of a data processing can be reduced depending on the value of EI. In other words, the lower the ease of identification is, the lower gets the overall score. Therefore, the combination of the EI and DPC (multiplication) gives the initial score of the severity (SE) of the data breach.
- CB quantifies specific circumstances of the breach that may be present or not in a particular situation. So, when present, CB can only add to the severity of a specific breach. For this reason the initial score can be further adjusted by the CB. Thus, the final score of the severity assessment can be extracted using the following formula:

$$SE = DPC \times EI + CB$$

In this way, in order for the controller to get the severity result, all three criteria should be scored.

Source: https://edps.europa.eu/sites/edp/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf

After the scoring, and if the conditions mentioned above are met, the DPO is obligated to report the breach to the supervisory authority (more information regarding this topic below).

The methodology described above is one of the available ones. The organization and the DPO will need to select a methodology and implement it systematically.

Other examples of methodologies are:



The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.



From the Information Commissioner's Office (ICO – UK): <https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/>

From the Data Protection Authority of Ireland:
[https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification Practical%20Guidance Oct19.pdf](https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification%20Practical%20Guidance%20Oct19.pdf)



Notification of a Data Breach

The GDPR in Article 33, requires a “Notification of a personal data breach to the supervisory authority” under the following circumstances:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.”

Each supervisory authority has issued a document template regarding the notification of a data breach.

The example of the Austrian Data Protection Agency is provided below. As seen from the below example, there is a variety of information that should be known and recorded by the organization regarding a data breach.

[https://www.dsb.gv.at/documents/22758/1188945/Meldung+von+Verletzungen+des+Schutzes+personenbezogener+Daten+gem%c3%a4%c3%9f+Art.+33+DSGVO+Notification+of+a+personal+data+breach+\(Art.+33+GDPR\)+.pdf/61fc399f-f77f-4b61-b994-e4db7a7656b5](https://www.dsb.gv.at/documents/22758/1188945/Meldung+von+Verletzungen+des+Schutzes+personenbezogener+Daten+gem%c3%a4%c3%9f+Art.+33+DSGVO+Notification+of+a+personal+data+breach+(Art.+33+GDPR)+.pdf/61fc399f-f77f-4b61-b994-e4db7a7656b5)



Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO

Notification of a personal data breach (Art. 33 GDPR)

Stand: Juli 2019 / Last changed: July 2019

Verantwortlicher / Controller:

Name / Name:

Anschrift / Postal address:

E-Mail-Adresse / Email address:

Datenschutzbeauftragter / Data protection officer:

Name / Name:

Anschrift (sofern nicht identisch mit der des Verantwortlichen) / Postal address (unless identical to that of the controller):

E-Mail-Adresse (sofern nicht identisch mit der des Verantwortlichen) / Email address (unless identical to that of the controller):

Hiermit melden wir folgende Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO / We hereby notify the following data breach of personal data pursuant to Art 33 GDPR:

Unverbindliches Formular der österreichischen Datenschutzbehörde • www.dsb.gv.at
Informationen gemäß Art. 13 und 14 DSGVO www.dsb.gv.at/datenschutz



1. Beschreibung der Verletzung des Schutzes personenbezogener Daten / *Description of the personal data breach:*

2. Es handelt sich um folgende Art der Verletzung des Schutzes personenbezogener Daten / *The following type of personal data breach took place:*

- ☐ Verletzung der Vertraulichkeit (Daten wurden gestohlen oder kopiert) / *Breach of confidentiality (data were stolen or copied)*
- ☐ Verletzung der Integrität (Daten wurden unautorisiert geändert) / *Breach of integrity (data were changed without authorisation)*
- ☐ Verletzung der Verfügbarkeit (Daten wurden gelöscht oder sind aus anderen Gründen nicht mehr verfügbar) / *Breach of availability (data were erased or are no longer accessible for another reason)*

3. Kategorien der betroffenen Personen (Kunden, Mitarbeiter, Patienten, Kinder etc.) / *Categories of the affected data subjects (customers, employees, patients, children, etc.):*

Unverbindliches Formular der österreichischen Datenschutzbehörde • www.dsb.gv.at
Informationen gemäß Art. 13 und 14 DSGVO www.dsb.gv.at/datenschutz

4. Angabe der ungefähren Zahl der betroffenen Personen / *Approximate number of data subjects:*

5. Angabe der betroffenen Kategorien (erworbene Produkte, Gesundheitsdaten, Bankdaten, politische Meinungen etc.) und der ungefähren Zahl der betroffenen personenbezogenen Datensätze / *Categories of data (purchased products, health data, banking data, political opinion) and the approximate number of data records involved:*

6. Zeitpunkt der Verletzung / *Time the breach took place:*

7. Zeitpunkt, an dem die Verletzung bekannt wurde / *Time the breach became known:*

8. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten für die betroffenen Personen (Bloßstellung, Diskriminierung, finanzieller Verlust, Haftung gegenüber Kunden, Identitätsdiebstahl) / *Description of the most likely consequences of the data breach for the data subjects (exposure, discrimination, financial loss, liability towards customers, identity theft):*

Unverbindliches Formular der österreichischen Datenschutzbehörde • www.dsb.gv.at
Informationen gemäß Art. 13 und 14 DSGVO www.dsb.gv.at/datenschutz

9. Folgende Maßnahmen wurden zur Behebung der Verletzung des Schutzes personenbezogener Daten ergriffen / *The following measures have been taken to address the breach of personal data:*

10. Folgende Maßnahmen wurden zur Abmilderung der möglichen nachteiligen Auswirkungen ergriffen / *The following measures have been taken to mitigate the possible adverse effects:*

11. (Optional)

☐ Es ist uns nicht möglich, die obengenannte Informationen derzeit bereitzustellen. Die Informationen werden ohne unangemessene weitere Verzögerung zur Verfügung gestellt (Art. 33 Abs. 4 DSGVO) / *We cannot provide the information at this time. The information will be provided in phases without undue further delay (Art. 33 para. 4 GDPR).*

12. Besondere Angaben (bei Bedarf) / Special details (as required):

- ☐ **12.1** Falls zwischen dem Zeitpunkt seit dem die Verletzung bekannt ist, und dem Zeitpunkt der Meldung mehr als 72 Stunden verstrichen sind, geben wir folgende Begründung für die Verzögerung / *If the notification was not made within 72 hours since the data breach became known, we give the following reasons for the delay:*

- ☐ **12.2** Die Daten werden von uns und einem anderen Verantwortlichen gemeinsam verarbeitet (Art. 26 DSGVO) / *We process the data jointly with another controller (Art. 26 GDPR):*

Unverbindliches Formular der österreichischen Datenschutzbehörde • www.dsb.gv.at
Informationen gemäß Art. 13 und 14 DSGVO www.dsb.gv.at/datenschutz

- ☐ **12.3** Die Daten werden von einem Auftragsverarbeiter verarbeitet (Art. 28 DSGVO) / *The data are processed by a processor (Art. 28 GDPR):*

Name / *Name:*

Anschrift / *Postal address:*

E-Mail-Adresse / *Email address:*

- ☐ **12.4** Es gibt eine weitere Anlaufstelle für Informationen:

Name / *Name:*

Anschrift / *Postal address:*

[ENISA Breach Notification Tool](#)

ENISA, in co-operation with the Office of the Federal Commissioner for Data Protection and Freedom of Information of Germany (German DPA), developed a tool for the notification of personal data breaches.



In particular, the purpose of the tool is to provide for the online completion and submission of a personal data breach notification by the data controller to the competent authority (DPA/NRA). It covers all types of personal data breaches and all types of business sectors, public or private.

Based on the input of the notification, the tool also provides to the competent authority an assessment of the severity of the breach. The assessment is based on the relevant Personal Data Breach Severity Assessment Methodology developed by ENISA in co-operation with the DPAs of Greece and Germany.

https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/data-breach-notification-tool/folder_contents



Lesson 5: Data Breaches

Unit 1: Introduction

Unit 2: Definitions

Question 1.:

Which of the following definitions corresponds to the term Breach?

1. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
2. personal data has been altered, corrupted, or is no longer complete
3. the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
4. data no longer exists, or no longer exists in a form that is of any use to the controller

Question 2.:

_____ of personal data, is where the data no longer exists, or no longer exists in a form that is of any use to the controller.

1. Corruption
2. Destruction
3. Construction
4. Disruption

Unit 3: Types of personal data breaches

Question 3.:

Map each of the type of breaches to their correct description?

"Confidentiality breach"	where there is an unauthorised or accidental alteration of personal data.
"Integrity breach"	where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
"Availability breach"	where there is an unauthorised or accidental disclosure of, or access to, personal data.

Unit 4: Assessment of impact

Unit 5: Notification of a Data Breach

Question 4.:

Which of the following is correct based on GDPR?



1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless *the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*
2. In the case of a personal data breach, the processor shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless *the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*
3. In the case of a personal data breach, the controller shall after 72 hours from the breach, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless *the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*
4. In the case of a personal data breach, the controller shall without undue delay and, where feasible, notify the data subjects regarding the breach

Question 5.:

In the context of a hospital, critical medical data about patients are unavailable, for several hours already. Which should be the actions of the DPO regarding notification?

1. this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled, so the competent authority should be notified
2. there is no need to notify anyone, since all of the patients already know this
3. this will probably be fixed before the 72 hours window so no actions need to be taken
4. the customers of the hospital have to be notified within 72 hours

Module 2: IT tools and methodologies applied to data protection

Chrysoula Psyllaki

Lesson 6, unit 1-6

Copyright © GDPR4H project

This deliverable is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Other tools for the DPO

There is a vast number of resources where one can obtain information relating to the current state of Attacks, Information Security Incidents and Private Data Breaches.

In this Section, some of these sources are presented. The DPO, is not obligated to know by heart any of this information but should rather have a basic understanding of the landscape, the trends regarding attacks and threats as well as other resources and capabilities that could be used if needed.

The recourses that could prove useful for the DPO fall into the following categories:

Official websites of the EDPB and the relevant authorities

The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR related matters and without the right to vote and being elected as chair or deputy chairs. The EDPB is established by the General Data Protection Regulation (GDPR), and is based in Brussels. The European Commission and -with regard to the GDPR related matters- the EFTA Surveillance Authority have the right to participate in the activities and meetings of the Board without voting right.

(Source: https://edpb.europa.eu/edpb_en)

The DPO can be informed through this website regarding the following:

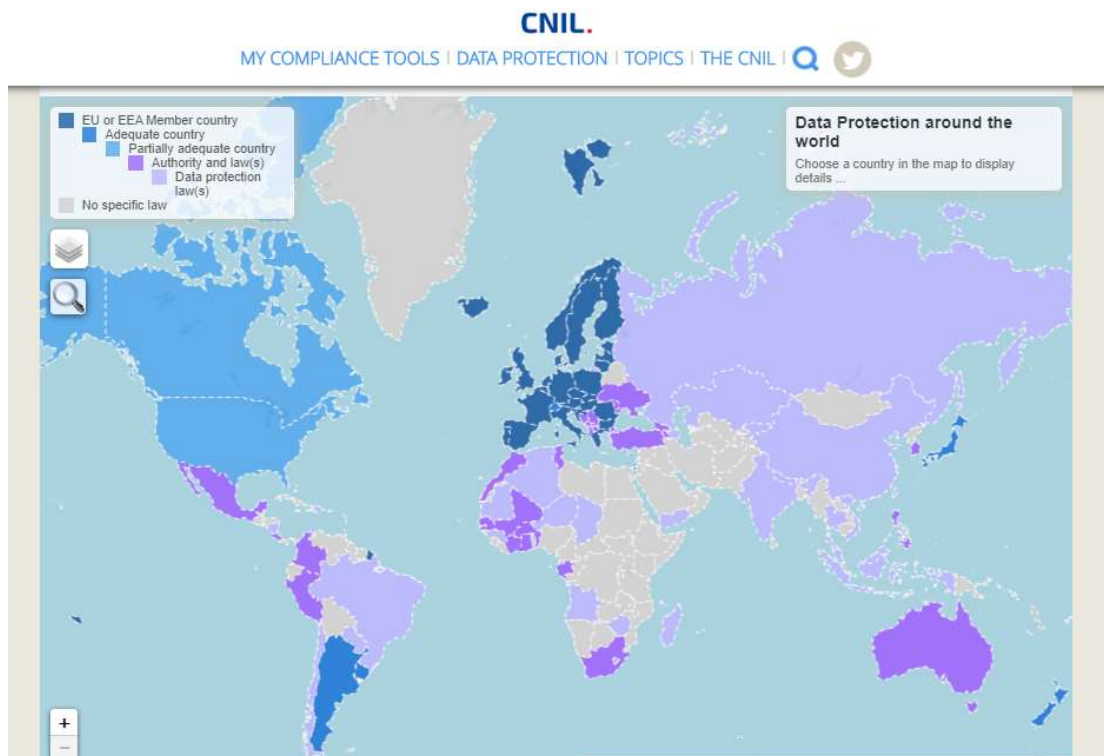
- GDPR: Guidelines, Recommendations, Best Practices
- Police & Justice: Guidelines, Recommendations, Best Practices
- Consistency Findings
- Opinions
- EDPB/EDPS Joint Opinions
- Binding Decisions
- Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism
- Letters
- Public Consultations
- Accountability Tools
- Register for Codes of Conduct, amendments and extensions
- Register of certification mechanisms, seals and marks
- Register of approved binding corporate rules



The supervisory authorities

Each country has one supervisory authority. Each DPO should systematically consult the website of its supervisory authority, in order to see news, decisions and other information. Moreover, the DPO may need to consult other supervisory authorities' websites, especially when involved in international transfer of personal data.

The CNIL (the French DPA) has a page in its website, with links to supervisory authorities across the globe.



<https://www.cnil.fr/en/data-protection-around-the-world>



Reports on current Threat Landscape

The following section contains some of the available reports on this subject. The list is by no means inclusive or complete. If more specific information is required the DPO should be able to search for the relevant information by himself. (The purpose of this list is not commercial but informational and the ownership of these publications belongs to their owner).

ENISA:

As referenced also above, ENISA publishes a yearly Threat Landscape Report that provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. Hundreds of reports from security industry, networks of excellence, standardisation bodies and other independent institutes have been analysed.

(Source: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape>)

Symantec:

The 2019 Internet Security Threat Report takes a deep dive into the latest trends in cyber security attacks, including ransomware, formjacking, and cloud security.

(Source: <https://www.symantec.com/security-center/threat-report>)

PWC:

For 20 years, leaders have turned to PwC's Global State of Information Security® Survey (GSISS) as a trusted resource to navigate the cyber risk landscape. Over time, that landscape has evolved to be less about information security and more about managing digital risk.

As cybersecurity, privacy and data ethics become increasingly intertwined, organizations need a central place to turn for actionable advice. So PwC has developed Digital Trusts Insights, a new platform that explores how to build confidence in the readiness of people, processes and technologies to meet tomorrow's challenges.

(Source: <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html>)

ORACLE and KPMG:

Public cloud-hosted and -delivered services have become the centers of gravity for many organizations' information technology infrastructures. Cloud applications and platform services have enabled businesses to move faster than ever, intensifying organizational dependence on the availability, integrity, and security of those services. Last year's Oracle and KPMG Cloud Threat Report explored market research that revealed how organizations are struggling to keep pace with the speed and scale at which their businesses are using cloud services, creating a cloud security readiness gap. A year later, it is clear that the business-critical nature of cloud services has substantially raised the stakes for securing public cloud assets. IT organizations are operating with a strategic imperative to address a myriad of both old and new cybersecurity challenges, highlighting



the need to retool the foundational elements of a cybersecurity program to bring the cloud into scope.

(Source: <https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf>)

KPMG - Cyber Trends Index:

One quick look at the Cyber Trends Index gives a real-time overview of buzzing news, threats and incidents from around the world.

The latest news ticker gives real-time highlights and directly links to news articles regarding information security incidents, developments and threats from around the world.

Trends and threats as two separate views, where one focuses on new developments, and the other focuses on events hitting the industry.

A comprehensive trend timeline to see the historic development of the threats, incidents and trends, allowing you to see the news that has been trending over time.

Trends activity, allowing you to see what caused peaks in trends or threats.

(Source: <https://cyber.kpmg.com/#threats/day/group:vzgomtbdhqzqnfsnkcrxn0rbojkgyvcd>)

Verizon:

The 2019 Data Breach Investigations Report is built upon analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches. We will take a look at how results are changing (or not) over the years as well as digging into the overall threat landscape and the actors, actions, and assets that are present in breaches. Windows into the most common pairs of threat actions and affected assets also are provided. This affords the reader with yet another means to analyze breaches and to find commonalities above and beyond the incident classification patterns that you may already be acquainted with.

(Source: <https://enterprise.verizon.com/resources/reports/dbir/>)

Reports on Imposed Fines

EDPB

The European Data Protection Board maintains a “Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism” at:

https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.



Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism

Type ▾
Member states ▾
2019 ▾
Topics ▾
APPLY FILTERS
RESET

Description	Type	Member states	Date ▾	Topics	Document	Opinion / Binding decision References
DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR	SA	Denmark	10 December 2019	Controller, Processor	DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR	Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)
French SAs list of the kind of processing operations exempt from the requirement for a Data Protection Impact Assessment under Art 35(5) of the General Data Protection Regulation (EU) 2016/679 (GDPR)	SA	France	12 September 2019	Data Protection Impact Assessment (DPIA), Opinions of the EDPB	France DPIA whitelist	Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)
Iceland SAs list of the kind of processing operations which are subject to the requirement for a Data Protection Impact Assessment under Article 35(4) of the General Data Protection Regulation (EU) 2016/679 (GDPR)	SA	Iceland	29 August 2019	Data Protection Impact Assessment (DPIA), Opinions of	Iceland DPIA List	Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

The consistency mechanism is used to promote consistent application of the GDPR by European supervisory authorities:

- **Opinions:** Opinions are issued on any matter of general application of the GDPR, or any issue having an effect in more than one member state. In addition, opinions are issued on some decisions made by European supervisory authorities, which have cross-border effects.
- **Binding decisions:** The GDPR creates a dispute resolution system, allowing for the EDPB to make binding decisions, where different supervisory authorities take different views or a national authority does not follow the opinion of the EDPB on a draft decision subject to consultation. The EDPB's binding decisions should be respected by national supervisory authorities when making their decisions.

Enforcement Tracker

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete.



GDPR Enforcement Tracker

tracked by **C/M'S'**
Law, Tax

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and penalties](#).

Show **10** entries

Search:

Country	Authority	Date	Fine [€]	Controller/Processor	Quoted Art.	Type	Infos
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>			<input type="text" value="Filter"/>		<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
UNITED KINGDOM	Information Commissioner (ICO)	2019-12-20	320,000	Doorstep Dispensaree Ltd. (Pharmacy)	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ROMANIA	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	2019-12-18	2,000	Telekom Romania Mobile Communications SA	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
BELGIUM	Belgian Data Protection Authority (APD)	2019-12-17	2,000	Nursing Care Organisation	Art. 12 GDPR, Art. 15 GDPR, Art. 17	Insufficient fulfilment of data subjects rights	link

(Source: <https://www.enforcementtracker.com/>)



Tools to check if information has been leaked

Have I Been Pwned?

One of the primary purposes of this site based on its creator is:

“firstly, it obviously provides a service to the public. Data breaches are rampant and many people don't appreciate the scale or frequency with which they occur. By aggregating the data here I hope that it not only helps victims learn of compromises of their accounts, but also highlights the severity of the risks of online attacks on today's internet.” And

<https://haveibeenpwned.com/>

This website hosts a list of sites which have had their information stolen over recent years. Anyone can check by scrolling through the list of websites there and also by inserting their email address in order to check whether it has been compromised.

Breach Alarm

“BreachAlarm is a service that allows you to check anonymously if your password has been posted online, and sign up for email notifications about future password hacks that affect you.

We comb the depths of the Internet to find stolen password lists that have been hacked, leaked or compromised, and we spot the email addresses of the users those passwords belong to. We keep a database of those email addresses so that you can check easily whether your email address and password have been included in any of these breaches.”

<https://breachalarm.com/>

DeHashed

“DeHashed is a hacked-database search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on database breaches and account leaks. Protect yourself before it's too late, don't wait until you're hacked.

Our advanced systems allow you to search for I.P. Addresses, Emails, Usernames, Names, Phone Numbers, VIN Numbers, Addresses; and what makes us even more unique, we allow you to reverse search Passwords, Hashes, and more!”

<https://www.dehashed.com/>



Lesson 6: Other tools for the DPO

Unit 1: Official websites of the EDPB and the relevant authorities

Question 1.:

What information would you would NOT expect to find in the EDPB website?

1. The fines imposed by the national competent authority
2. Guidelines regarding the processing of personal data
3. The approved codes of conduct and certification schemes
4. Templates for the implementation of GDPR compliance in an organization

Unit 2: Reports on current Threat Landscape

Unit 3: Reports on Imposed Fines

Question 2.:

Why monitoring the imposed fines would be beneficial for a DPO?

1. To rejoice in the misfortune of others
2. To understand the rationale of the decisions of the competent authorities and the measure of the impact
3. To gain insider information on other organizations
4. To use it as a competitive advantage

Unit 4: Tools to check if information has been leaked

Question 1:

Which of the followings are special categories of personal data?

1. Political opinions
2. Biometric data for the purpose of uniquely identifying a natural person
3. ID number
4. All the above

Question 2:

In an organization, who sets the risk acceptance criteria?

1. Information Security Officer
2. Top Management
3. IT Manager
4. Is not needed to set risk acceptance criteria

Question 3:

Which of the following antivirus solutions are not secure?



1. An unlicensed antivirus solution
2. An antivirus solution that is fully activated with a crack software
3. A full licensed antivirus solution
4. A freeware antivirus solution

Question 4:

A _____ is an unauthorized user who attempts to or gains access to an information system.

1. Malicious insider
2. Hacker
3. Joker
4. Student

Question 5:

Which of the following is an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment?

1. Cyber espionage
2. Cyber bullying
3. Cyber extortion
4. Cyber pollution

Question 6:

Would the loss of a securely encrypted mobile device, utilized by the controller and its staff require notification to the supervisory authority? (The encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker.).

1. Yes, because the mobile device contains personal data.
2. No, because the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question.

Question 7:

In _____ encryption, encryption algorithms use the same secret key for encryption and decryption.

1. Asymmetric
2. Symmetric
3. RSA
4. Public

Question 8:

Which of the following activities can be monitored by a DLP?

1. Printing documents



2. Network activities
3. Use of removable media
4. All the above

Question 9:

If you believe that your account has been compromised, to whom you have to report the incident?

1. Colleague
2. Nobody
3. Your manager
4. To the person or department especially designed for this role (e.g. IT Department, Security Management etc)

Question 10:

In order to have a strong password what kind of characters should we use?

1. Letters and Numbers
2. Special Characters (e.g. @\$%^)
3. Lower and Upper characters
4. All the above